UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK

Matthew Fero; Roger A. Carroll, D.D.S.; Andres Curbelo; Cindy Harden; Cathryn Kwit; Robert Kwit; Harold Jackling; Nina Mottern; Barbara Palmer; Carole Preston; James J. Smith, Jr.; Sharon C. Smith; Edward Trumble; Dwayne Church; Don Korn; Therese Boomershine; Carlos Martinho; Thomas Albrecht; and Brenda Caltagarone, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

Excellus Health Plan Inc., Lifetime Healthcare, Inc., Lifetime Benefit Solutions, Inc., Genesee Region Home Care Association, Inc. d/b/a Lifetime Care, Genesee Valley Group Health Association d/b/a Lifetime Health Medical Group, MedAmerica, Inc., Univera Healthcare, and Blue Cross and Blue Shield Association,

Defendants.

Case No. 6:15-cv-06569

SECOND AMENDED CONSOLIDATED MASTER COMPLAINT

DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

Plaintiffs identified below (collectively, "Plaintiffs" or "Class Members"), individually and on behalf of the putative Classes of similarly situated persons defined herein, file this Amended Consolidated Master Complaint pursuant to the Court's Decision and Order dated January 25, 2016, (Dkt. 80), as modified by the Orders of Court dated February 16, 2016, (Dkt. 83), February 23, 2017 (Dkt. 140), and January 19, 2018 (Dkt. 181). Plaintiffs file suit against Excellus Health Plan, Inc., Lifetime Healthcare, Inc., Lifetime Benefit Solutions, Inc., Genesee Region Home Care Association, Inc. d/b/a Lifetime Care, Genesee Valley Group Health Association d/b/a Lifetime Health Medical Group, MedAmerica, Inc., Univera Healthcare, and Blue Cross and Blue Shield Association (collectively, "Defendants").

INTRODUCTION

1. Beginning on or before December 23, 2013, hackers infiltrated Defendants' cybersecurity systems, acquired high-level access to Defendants' computer networks (referenced, collectively, as the "Excellus Networks"), and gained access to the personal information and protected health information of approximately 10 million individuals. For at least the next nine months, these intruders operated in the Excellus Networks with impunity.

2. Prompted by several other high profile data breach events, Defendants retained a cybersecurity and forensics analysis company called Mandiant to conduct a scan of their systems. On August 5, 2015, shortly after it began its scans, Mandiant reported that the Excellus Networks been breached in an extended intrusion. Although Mandiant did not identify when the hackers first accessed the Excellus Networks, it identified unauthorized activity as early as December 2013. In the 600 days that elapsed between the

initial breach and its belated discovery, hackers were able to gain access to an array of sensitive and confidential Personal Information, which included Personally Identifiable Information, or "PII," as well as Protected Health Information, or "PHI." This Personal Information was entrusted to Defendants and stored in the Excellus Networks

3. The Personal Information exfiltrated by the attackers in the Excellus data breach includes names, dates of birth, social security numbers, mailing addresses, telephone numbers, member identification, financial information, credit card numbers, and medical claims information belonging to millions of adults and minor children. Some of this Personal Information dates back to the 1980s and is over thirty years old.

4. The Personal Information that was exfiltrated pertains to individuals: (a) who have been enrolled in health plans with Defendants Excellus Health Plan, Inc. ("Excellus"); (b) whose medical claims were processed by Excellus under a series of agreements with Defendant Blue Cross and Blue Shield Association ("BCBSA") and its licensees; (c) who have been customers of several affiliates of Defendant Lifetime Healthcare, Inc. ("Lifetime"), including Defendants Lifetime Benefit Solutions, Inc. ("Lifetime Benefit"), Genesee Region Home Care Association, Inc. d/b/a Lifetime Care ("Lifetime Care"), Genesee Valley Group Health Association d/b/a Lifetime Health Medical Group ("Lifetime Health Medical"), MedAmerica Inc. ("MedAmerica"), and Univera Healthcare ("Univera"); and (d) who are health care providers that treated the individuals listed above.

5. On September 9, 2015, Excellus and its parent company, Lifetime, publicly acknowledged the data breach and that Personal Information of over 10 million individuals was compromised. This data breach is the direct result of Defendants' failure to implement

cybersecurity measures commensurate with the duties they undertook by storing vast quantities of highly sensitive Personal Information.

6. Indeed, Defendants knew that the Personal Information they stored was both valuable and vulnerable to cyber attackers. The data collected and stored by healthcare providers and health insurance companies like Defendants are among the most highly sensitive personally identifiable information. Healthcare and health insurance companies, in turn, bear the crucial responsibility to protect this data from compromise and theft.

7. What is more, the threat of compromise is significant. Government agencies and cybersecurity experts have warned of persistent threats targeting the healthcare industry. The risk of cyberattack in the healthcare industry is known and undeniable; it is imperative that healthcare and health insurance companies assume a corresponding duty to guard against this known risk and thwart preventable attacks.

8. Because the risk of loss or theft is so significant, entities that finance and deliver healthcare services are required to protect their customers' PII and PHI by adopting and implementing data security regulations and standards, including those set forth under the Health Insurance Portability and Accountability Act ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act ("HITECH Act"), applicable state law, including New York State law, and common law.

9. Not only did Defendants understand their duty of care, each Defendant made repeated promises and representations that it was protecting its customers' sensitive information. Defendants expressly and impliedly promised to provide protections to their customers—including in Defendants' customer agreements and privacy policies and on

Defendants' websites—in exchange for payments and other consideration. As set forth in detail below, Defendants' promises were hollow.

10. Any company with reasonable data security practices and procedures, for example, would implement adequate monitoring protocols sufficient to detect a data security breach, particularly an intrusion as long lasting and wide-ranging as this one, at the time of or in close proximity to the initial intrusion. Implementation of reasonable monitoring protocols is of even greater import where, as here, Defendants were storing valuable Personal Information that was a known target of cyber attackers. The Excellus Networks were breached on or before December 2013, however, and Defendants' monitoring protocols were so poor that they failed to detect the breach until August 2015, when they hired an outside company to scan their systems.

11. Based on a 2016 report on data breaches, developed from analyzing over 300 incidents in 2015, the time that it took Defendants to detect this breach was ten times as long as the usual response time for this type of breach. This report summarizes past data breach incidents and the breached entity's discovery of the intrusion as follows:

> The time from when an incident first began until it was detected ranged from 0 to over 400 days. The overall average time to detect was 69 days and the median was 15 days. For the subset of matters involving an unauthorized person who gained access to a network, the average time to detect was 106 days and the median was 55 days.[1]

12. Victims of the Excellus data breach have suffered harm repeatedly since their Personal Information was compromised. As detailed below, false tax returns have

[1] BakerHostetler, Is Your Organization Compromise Ready?, 2016 Data Security Incident Response Report at 8 (2016), http://bakerlaw.com/files/uploads/Documents/Privacy/2016-Data-Security-Incident-Response-Report.pdf.

been filed in Class Members' names and some Members have yet to receive their refunds; Class Members' bank account and investment account information has been accessed via the Internal Revenue Service's portal; Class Members have experienced credit card and debit card fraud, as well as social security fraud and US Postal Service fraud; they have spent hours completing police reports, reporting identity theft and fraud to the Federal Trade Commission (FTC); freezing their credit, and monitoring credit reports. Many Class Members have enrolled in a credit monitoring service offered by a non-party credit monitoring provider, Kroll, Inc. ("Kroll"). Still others are paying monthly or annual fees for additional identity theft and credit monitoring services or insurance. Parents of minor victims have been left to fend for themselves, as Defendants have failed even to offer advice or guidance on how to protect children from identity theft. On top of this, the personal and medical information of these minor victims has been compromised. For all Class Members, fear and anxiety of identity theft or fraud is the new norm.

13. In short, Defendants breached their duty to protect and safeguard Class Members' personal, health, and financial information and to take reasonable steps to contain the damage caused where any such information was compromised. Through no fault of their own, Class Members have suffered financial and emotional injury and must now attempt to safeguard themselves and their families from unknown but certainly impending future crimes. For the reasons set forth below, Plaintiffs and Class Members request damages to compensate them for current and future losses, as well as injunctive relief to provide safeguards against another failure of Defendants' cybersecurity systems. In addition, Plaintiffs and Class Members seek credit monitoring services uniquely tailored to protect the interests of the minor victims of this data breach, as well as retention of a

service to assist the elderly and infirm victims of this breach, including those who reside in nursing homes and assisted living facilities, to monitor their credit and proactively guard against future identity theft and fraud.

JURISDICTION AND VENUE

14. Jurisdiction is proper in this Court pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because (i) there are more than 100 Class Members, (ii) the aggregate amount in controversy exceeds $5,000,000 exclusive of costs and interests, and (iii) some Plaintiffs and Class Members are citizens of states different from Defendants' home states.

15. This Court has personal jurisdiction over Defendants Excellus, Lifetime, Lifetime Care, Lifetime Health Medical, MedAmerica, and Univera because each of these entities maintain a principal place of business in this judicial district and regularly conduct business in New York. This Court has personal jurisdiction over Defendant Lifetime Benefit and BCBSA because each Defendant regularly conducts business in this district and New York State.

16. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because several Defendants, including Excellus and Lifetime, reside in this district and regularly conduct business in this district, a substantial part of the events or omissions giving rise to these claims occurred in this district, and Defendants have caused harm to Class Members residing in this district.

PARTIES

Plaintiffs

New York

17. Plaintiff Matthew Fero is a citizen of the State of New York and resides in the Town of Brighton. At all times relevant hereto, Mr. Fero was enrolled in an Excellus policy and paid premiums on a regular basis. Excellus collected and received Mr. Fero's PII and PHI, which it maintained in the Excellus Networks. In the fall of 2015, Mr. Fero received a letter from Excellus informing him that his PII and PHI, as well as the PII and PHI of his wife and two minor children, may have been compromised as a result of the data breach. Following his notification of the breach, Mr. Fero enrolled in the two-year credit monitoring service offered through Kroll. Mr. Fero also enrolled his wife in Kroll's credit monitoring service, but pursuant to Kroll's instructions, he was not able to enroll either of his minor children in the monitoring program. In or around March of 2017, Sylint Group conducted a DarkNet search and located Mr. Fero's PII for sale in the same data set where plaintiffs Boomershine and Church's PII was also for sale. Mr. Fero has no connection to plaintiffs Boomershine or Church, who reside in Indiana and California respectively, other than that their PII was stored in the Excellus Network. As a result of the data breach and the theft of his PII and PHI, the Personal Information of Mr. Fero and his family has been compromised, and he has spent time attempting to ensure that his family is protected from future acts of identity theft or fraud stemming from this data breach.

18. Plaintiff Dr. Roger A. Carroll is a citizen of the State of New York and resides in the City of Rochester. Dr. Carroll is a New York State licensed Doctor of Dental Surgery. At all times relevant hereto, Dr. Carroll had a provider contract with Excellus.

Pursuant to that contract, Excellus collected and received Dr. Carroll's PII. On or about September 30, 2015, Dr. Carroll was contacted by the fraud department of CareCredit, a health care financing company, and told that an individual was attempting to establish credit at a new dental practice in Brooklyn, New York, using Dr. Carroll's PII, including his social security number, date of birth, and professional qualifications. Upon information and belief, this individual allegedly created a fictitious email address for a practice in Dr. Carroll's name in Brooklyn, New York, and was attempting to fraudulently billed CareCredit for fictitious dental services using Dr. Carroll's identity. Upon further information and belief, using Dr. Carroll's PII, the individual also submitted a fictitious utility bill and IRS form to support the fraudulent dental provider identity. In the fall of 2015, Dr. Carroll received a letter from Excellus informing him that his PII and PHI may have been compromised as a result of the data breach. Following his notification of the breach, Dr. Carroll enrolled in the two-year credit monitoring service offered through Kroll and froze his credit with all three credit agencies. As a result of the breach and the theft of his PII and PHI, Dr. Carroll's PII has been compromised, his identity has been stolen, and he has spent hours remediating the financial fraud and identity theft. It is highly likely that he will be required to spend additional time protecting himself from certainly impending incidents of future identity theft and fraud.

19. Plaintiff Andres Curbelo is a citizen of the State of New York and resides in the Town of Henrietta. At all times relevant hereto, Mr. Curbelo was a longtime patient at Marion B. Folsom Health Center, a Lifetime Health Medical group facility in Rochester, New York. Lifetime Health Medical collected and received Mr. Curbelo's PII and PHI, which Excellus maintained in the Excellus Networks. On February 22, 2016, Mr. Curbelo

received a 5071C letter from the Internal Revenue Service (IRS) advising him that the IRS received a federal income tax return bearing his name and social security number for tax year 2015, and requesting further verification. Mr. Curbelo completed a Form 14039 Identity Theft Affidavit. In March 2016, he received another letter from the IRS confirming that he had been the victim of identity theft and providing instructions to obtain an identity theft protection personal identification number. Mr. Curbelo also notified the New York State Department of Taxation and Finance that he was the victim of identity theft and tax fraud and he completed a DTF-275 Identity Theft Declaration form with the State. To date, Mr. Curbelo has spent numerous hours on the telephone and completing paperwork necessary to address this fraud, and his efforts are ongoing. In the fall of 2015, Mr. Curbelo received a letter from Lifetime and an email from Lifetime Health Medical eNews informing him that his PII and PHI may have been compromised as a result of the data breach. Following his notification of the breach, Mr. Curbelo enrolled in the two-year credit monitoring service offered through Kroll and ordered copies of his credit reports to monitor his credit. He also filed an identity theft complaint with the Federal Trade Commission (FTC) and an identity theft report with the Monroe County Sheriff's Office. In addition, he went to his bank and placed a fraud alert on his account, and changed his telephone banking privileges. As a result of the data breach and the theft of his PII and PHI, Mr. Curbelo's Personal Information has been compromised, he has spent numerous hours attempting to remediate the tax fraud that he experienced, and it took longer for him to file his 2015 federal and New York State income tax returns, thereby denying him access, as of the date of this filing, to his 2015 federal tax return.

20. Plaintiff Cindy Harden is a citizen of the State of New York and resides in the Town of Ontario. At all times relevant hereto, Mrs. Harden was enrolled in an Excellus policy and paid premiums on a regular basis. In addition, Mrs. Harden's employee benefits were administered through Lifetime Benefit Solutions, Inc. Excellus and Lifetime Benefit Solutions, Inc. collected and received Mrs. Harden's PII and PHI, which it maintained in the Excellus Networks. In June 2014, Mrs. Harden received a letter from the IRS dated May 30, 2014 advising her that someone attempted to file federal tax returns in the name of Mrs. Harden and her husband using their social security numbers. In the fall of 2015, Mrs. Harden received a letter from both Excellus and Lifetime informing her that her PII and PHI, as well as the PII and PHI of her husband, may have been compromised as a result of the data breach. Accordingly, as a result of the data breach and the theft of her PII and PHI, Mrs. Harden's Personal Information has been compromised, and she has spent at least ten hours attempting to protect herself and her family from identity theft and fraud. In this vein, Mrs. Harden has purchased a subscription to LifeLock Ultimate, a credit monitoring service, placed fraud alerts and a credit freeze on her credit with each of the three major reporting bureaus, and requested copies of her credit report from each of the three major reporting bureaus. In addition, access to her 2013 federal income tax return was delayed by several months due to the breach. Mrs. Harden continues to regularly order copies of her credit reports and monitors them for any suspicious activity. She also filed an identity theft report with the New York State Police and has filed or intends to file an identity theft report with the FTC.

21. Plaintiff Cathryn Kwit is a citizen of the State of New York and resides in the Town Irondequoit. At all times relevant hereto, Mrs. Kwit was enrolled in an Excellus

policy and paid premiums on a regular basis. Excellus collected and received Mrs. Kwit's PII and PHI, which it maintained in the Excellus Networks. In the fall of 2015, Mrs. Kwit received a letter from both Excellus and Lifetime informing her that her PII and PHI may have been compromised as a result of the data breach. In September 2015, Mrs. Kwit received a notification from the United States Post Office indicating that someone fraudulently changed her mailing address from her current mailing address to her mailing address of 14 years earlier. In October 2015, Mrs. Kwit learned that someone fraudulently opened a GO Bank checking account with an associated debit card in her name in California. On October 19, 2015, Mrs. Kwit received a letter from the Social Security Administration advising her that someone had fraudulently changed her direct deposit information for her Social Security Retirement benefits so that her benefits would be deposited to the fraudulent GO Bank checking account. In addition, someone created a fraudulent Social Security online account to facilitate the change of direct deposit information. Mrs. Kwit also received two "phishing" telephone calls in 2015 on her unlisted home telephone number. The phishing calls offered to repair her Windows computer system if she would log on online with the caller. She hung up and reported the first call to the Irondequoit Police Department. As a result of the data breach and the theft of her PII and PHI, Mrs. Kwit has spent at least fifteen hours attempting to protect herself from identity theft and fraud. In this vein, Mrs. Kwit was present when her husband, Plaintiff Robert Kwit, contacted the U.S. Postal Service and U.S. Postal Inspector to correct the fraudulent address change. She visited the Social Security Administration to correct the fraudulent change of direct deposition information. She enrolled herself and her husband in the two-year credit monitoring service offered through Kroll. She has

purchased "ProtectMyID" credit monitoring and placed fraud alerts with each of the three major reporting bureaus. She alerted her pension company, the New York State Teachers Retirement System, of the fraud. Mrs. Kwit also went to her bank to alert it to the fraud. In addition, Mrs. Kwit, along with her husband, filed an identity theft report with the Irondequoit Police Department. She also filed complaints on behalf of herself and Mr. Kwit against GO Bank with the Federal Deposit Insurance Corporation and the Federal Reserve Bank of San Francisco. She also filed an identity theft complaint with the FTC. In addition, Mrs. Kwit contacted Doyle Security company to investigate a home security system to further protect her family.

22. Plaintiff Robert Kwit is a citizen of the State of New York and resides in the Town of Irondequoit. At all times relevant hereto, Mr. Kwit was enrolled in an Excellus policy and paid premiums on a regular basis. Excellus collected and received Mr. Kwit's PII and PHI, which it maintained in the Excellus Networks. In the fall of 2015, Mr. Kwit received a letter from both Excellus and Lifetime informing him that his PII and PHI may have been compromised as a result of the data breach. In September 2015, Mr. Kwit received a notification from the United States Post Office indicating that someone fraudulently changed his mailing address from his current mailing address to his mailing address of 14 years earlier. In October 2015, he learned someone fraudulently opened a GO Bank checking account in his name in California. On October 22, 2015, Mr. Kwit received a letter from the Social Security Administration advising him that someone had fraudulently changed his direct deposit information for his Social Security Retirement benefits so that his benefit payments would be directed to the fraudulent GO Bank checking account. In addition, someone created a fraudulent Social Security online account to

facilitate that change of direct deposit information. As a result of the data breach and the theft of his PII and PHI, Mr. Kwit has spent at least twenty hours attempting to protect himself from identity theft and fraud. In this vein, Mr. Kwit contacted the U.S. Postal Service and U.S. Postal Inspector to correct the fraudulent address change. Mr. Kwit visited the Social Security Administration to correct the fraudulent change of direct deposit information. He also purchased "ProtectMyID" credit monitoring and placed fraud alerts with each of the three major reporting bureaus. Mr. Kwit also went to his bank to alert it to the fraud, and he contacted his credit card companies to alert them to the fraud. In addition, Mr. Kwit has filed identity theft reports with the IRS, the New York State Department of Taxation and Finance, the Irondequoit Police Department, and the FTC, and he also contacted the New York State Attorney General's Office regarding the breach.

23. Plaintiff Harold Jackling is a citizen of the State of New York and resides in the Town of Pittsford. At all times relevant hereto, Mr. Jackling was enrolled in an Excellus policy and paid premiums on a regular basis. Excellus collected and received Mr. Jackling's PII and PHI, which it maintained in the Excellus Networks. In the fall of 2015, Mr. Jackling received a letter from Excellus informing him that his PII and PHI may have been compromised as a result of the data breach. He enrolled in the two-year credit monitoring service offered through Kroll. In March 2017, Mr. Jackling discovered that someone fraudulently used his Best Buy Citibank Visa Card in New York City to purchase a camera and then exchanged the camera at a different Best Buy store in Brooklyn, New York for a gift card. In April 2017, he discovered someone fraudulently used his newly replaced Best Buy Citibank Visa Card in Brooklyn, New York, to purchase a camera and then exchanged it at a different Best Buy store in New York City for a gift card. Both of

these charges were ultimately reversed, and Best Buy issued him a new credit card. Mr. Jackling reported the fraud to the Monroe County Sheriff's Department. He also ordered and reviewed carefully copies of his credit reports from all three major credit reporting bureaus, and placed a 90-day fraud report with them. Then in April 2017, someone attempted to use his Loews credit card for a fraudulent purchase, but the charge was declined before it went through. In May 2017, someone tried to open a credit card account at Target, which account application was denied by Target. Also in May 2017, someone attempted to open a credit card account at Kohl's, which account application was denied by Kohl's. Mr. Jackling reported these new frauds to the same Sheriff's Officer who took the first report. He placed 7-year fraud alerts with each of the three major reporting bureaus. In addition, Mr. Jackling filed an identity theft complaint with the FTC, and filled out requested paperwork and reports related to the fraud from the retail stores. In November 2017, Mr. Jackling purchased LifeLock Ultimate Plus Plan for $30/month credit monitoring. As a result of the breach and the theft of his PII and PHI, Mr. Jackling's Personal Information has been compromised, and he has spent at least 200 to 250 hours attempting to remediate the fraud that he experienced, and attempting to protect himself and his family from future acts of identity theft and fraud. He continues to check his financial accounts and his LifeLock account approximately five times a week 30 minutes a day for any fraudulent charges, and will continue to do so in the future.

24. Plaintiff Nina Mottern is a citizen of the State of New York and resides in the Town of East Rochester. At all times relevant hereto, Mrs. Mottern was enrolled in an Excellus policy, which she carried through the Federal Health Benefit Plan. Excellus collected and received Mrs. Mottern's PII and PHI, which it maintained in the Excellus

Networks. In February 2014, Mrs. Mottern became aware that fraudulent charges had been attributed to her American Express credit card. In the fall of 2015, Mrs. Mottern received a letter from both Excellus and Lifetime informing her that her PII and PHI, as well as the PII and PHI of her husband, may have been compromised as a result of the data breach. Following her notification of the breach, Mrs. Mottern was enrolled in the two-year credit monitoring service offered through Kroll, had fraud alerts placed on her credit cards, and purchased "My Eyes Only," a password maintenance service. As a result of the data breach and the theft of her PII and PHI, Mrs. Mottern's Personal Information has been compromised and she has spent time attempting to protect herself and her family from future incidents of identity theft or fraud. Indeed, each time she receives a credit alert, Mrs. Mottern is filled with anxiety.

25. Plaintiff Barbara Palmer is a citizen of the State of New York and resides in the Town of Parma. At all times relevant hereto, Mrs. Palmer was enrolled in an Excellus policy and paid premiums on a regular basis. Excellus collected and received Mrs. Palmer's PII and PHI, which it maintained in the Excellus Networks. In the fall of 2015, Mrs. Palmer received a letter from Excellus informing her that her PII and PHI, as well as the PII and PHI of her husband, may have been compromised as a result of the data breach. In September 2015, the Internal Revenue Service sent Mrs. Palmer a notification indicating that the IRS learned that her social security number was used in an attempt to obtain a transcript of her tax account through the IRS's Get Transcript application on IRS.gov. One month prior to this notification, the Internal Revenue Service sent Mrs. Palmer's husband a notification indicating that it had learned that criminal actors used his personal information to view the Palmers' tax information, including their checking, savings and

retirement account information, through the IRS's Get Transcript application on IRS.gov. The IRS indicated that Mrs. Palmer's personal information was "obtained from a source outside the IRS." Mrs. Palmer and her husband were assigned a special identity protection personal identification number with which to complete their 2016 federal tax returns. In addition, in January 2014, Mrs. Palmer discovered that thirteen fraudulent charges were charged to her Visa credit card totaling in excess of $900. As a result, she was deprived of access to her Visa credit card for approximately twelve days when she was on vacation in Florida. All of Mrs. Palmer's attempts to remediate this instance of credit card fraud were undertaken during her vacation. In May 2015, Mrs. Palmer's Visa was the subject of seven more fraudulent charges. Following her notification of the breach, Mrs. Palmer enrolled in the two-year credit monitoring service offered through Kroll, placed fraud alerts on her credit cards, and initiated a credit freeze with each of the three major credit reporting bureaus. She also filed a report with the Federal Trade Commission and the Greece Police Department. As a result of the data breach and the theft of her PII and PHI, Mrs. Palmer's Personal Information has been compromised, and she has spent at least fifteen hours attempting to protect herself from tax fraud and remediate the credit card fraud, as well as to prevent future incidents of identity theft or fraud. She no longer charges items at restaurants or the gas station, instead opting to pay with cash.

26. Plaintiff Carole Preston is a citizen of the State of New York and resides in the Village of McGraw. At all times relevant hereto, Mrs. Preston was enrolled in an Excellus policy and paid premiums on a regular basis. Excellus collected and received Mrs. Preston's PII and PHI, which it maintained in the Excellus Networks. In the fall of 2015, Mrs. Preston received a notice from her credit card company informing her of four

suspicious credit card charges totaling approximately $1,000. These charges were ultimately reversed. The day before Mrs. Preston received this notice, her husband, who is also enrolled in an Excellus policy, received notice from his credit card company of approximately $200 in suspicious purchases charged to his credit card. Mr. Preston's financial institution reversed these charges as well. Two days after Mrs. Preston's financial institution notified her of the fraudulent charges to her account, she received a letter from Excellus informing her that her PII and PHI may have been compromised as a result of the data breach. Mrs. Preston also received a letter notifying him of the breach. As a result of the data breach and the theft of her PII and PHI, Mrs. Preston's Personal Information has been compromised, and she has spent time remediating the financial fraud that she and her husband experienced, and it is likely that she will be required to spend additional time protecting herself from future incidents of identity theft and fraud.

27. Plaintiff James J. Smith, Jr. is a citizen of the State of New York and resides in the Town of Fairport. At all times relevant hereto, Mr. Smith was enrolled in an Excellus policy and paid premiums on a regular basis. Excellus collected and received Mr. Smith's PII and PHI, which it maintained in the Excellus Networks. From March 2014 through March 2016, Mr. Smith had periodic fraudulent charges appear on his Marriott Rewards Visa credit card. These charges were all reversed. In April and May 2015, Mr. Smith learned that someone using his PII fraudulently opened or attempted to open in his name nine different credit accounts with various credit companies. In September 2015, Mr. Smith learned that someone using his PII fraudulently opened or attempted to open in his name approximately twelve different credit accounts with various credit companies. These incidents of fraud spurred Mr. Smith to begin closely monitoring his credit reports and to

place credit freezes with each of the three major credit reporting bureaus. In the fall of 2015, Mr. Smith received letters from Excellus and Lifetime informing him that his PII and PHI may have been compromised as a result of the data breach. Following his notification of the breach, Mr. Smith enrolled in the two-year credit monitoring service offered through Kroll, placed fraud alerts with three of the major credit reporting bureaus, froze his credit and ordered copies of his credit report. He also filed an identity theft report with the Monroe County Sheriff's Office and the FTC. Mr. Smith now monitors his checking and credit card accounts daily for any fraudulent activity. As a result of the data breach and the theft of his PII and PHI, Mr. Smith's Personal Information has been compromised, and he has spent at least 120 hours attempting to remediate the fraud that he experienced and to monitor his accounts for any further fraud, and this time increases daily. It is highly likely that he will be required to spend additional time protecting himself from future incidents of identity theft and fraud, given what he has experienced over the past year.

28. Plaintiff Sharon Smith is a citizen of the State of New York and resides in the Town of Fairport. At all times relevant hereto, Mrs. Smith was enrolled in an Excellus policy and paid premiums on a regular basis. Excellus collected and received Mrs. Smith's PII and PHI, which it maintained in the Excellus Networks. From March 2014 through March 2016, Mrs. Smith had periodic fraudulent charges appear on her Marriott Rewards Visa credit card. These charges were all reversed. In August 2015, a fraudulent charge appeared on her Citizens Bank Debit Card to purchase goods or services through PayPal. In August and September 2015, fraudulent charges appeared on her Xceed Financial credit card. Also in September 2015, Mrs. Smith learned that someone using her PII fraudulently

opened or attempted to open in her name approximately six different credit accounts with various credit companies. These incidents of fraud spurred Mrs. Smith to begin closely monitoring her credit reports and to place credit freezes with each of the three major credit reporting bureaus. In addition, February, March and April of 2016, Mrs. Smith received numerous different phishing emails seeking her personal and financial information. In the fall of 2015, Mrs. Smith received letters from Excellus and Lifetime informing her that her PII and PHI may have been compromised as a result of the data breach. Following her notification of the breach, Mrs. Smith enrolled in the two-year credit monitoring service offered through Kroll, placed new fraud alerts with three of the major credit reporting bureaus, and ordered fresh copies of her credit report. She also filed an identity theft report with the Monroe County Sheriff's Office and the FTC. Mrs. Smith now checks her two credit card accounts daily for any fraudulent activity. As a result of the data breach and the theft of her PII and PHI, Mrs. Smith's Personal Information has been compromised, and she has spent at least 145 hours attempting to remediate the fraud that she experienced and monitor her accounts for any further fraud, and this time increases daily. It is likely that she will be required to spend additional time protecting herself from future incidents of identity theft and fraud, given what she has experienced over the past year.

29. Plaintiff Edward Trumble is a citizen of the State of New York and resides in the Town of Webster. At all times relevant hereto, Mr. Trumble was enrolled in an Excellus policy and paid premiums on a regular basis. Excellus collected and received Mr. Trumble's PII and PHI, which it maintained in the Excellus Networks. On or about April 8, 2015, Mr. Trumble attempted to e-file his federal income taxes along with his tax preparer. On or about April 9, 2015, Mr. Trumble learned that someone had already filed

fraudulent federal income tax returns using his name and social security number. He thereafter made several visits to his local IRS office to report and correct the fraud, and to file a traditional paper income tax return and confirm his identity. In the fall of 2015, Mr. Trumble received a letter from Excellus informing him that his PII and PHI may have been compromised as a result of the data breach. Following his notification of the breach, Mr. Trumble enrolled in the two-year credit monitoring service offered through Kroll, placed fraud alerts with two of the major credit reporting bureaus, and ordered copies of his credit report. Mr. Trumble also filed identity theft reports with the Webster Police Department and the FTC. As a result of the data breach and the theft of his PII and PHI, Mr. Trumble's Personal Information has been compromised, and he has spent approximately twelve hours attempting to remediate the tax fraud that he experienced, as well as to protect himself from future incidents of identity theft or fraud. In addition, Mr. Trumble did not receive his 2014 federal tax refund until on or around August 2015 because of the fraud.

California

30. Plaintiff Dwayne Church is a citizen of the State of California and resides in the City of San Diego. In the early 1980s, and while he was under the age of 19, Mr. Church's mother purchased an insurance policy through Excellus and named Mr. Church as an insured under the policy. Excellus collected and received Mr. Church's PII and PHI, which it maintained in the Excellus Networks. In the fall of 2015, Mr. Church received a letter from Excellus informing him that his PII and PHI may have been compromised in the breach. Following his notification of the breach, Mr. Church enrolled in the two-year credit monitoring service offered through Kroll and ordered a copy of his most recent credit report. In or around March of 2017, Sylint Group conducted a DarkNet search and located

Mr. Church's PII for sale in the same data set where plaintiffs Boomershine and Fero's PII was also for sale. Mr. Church has no connection to plaintiffs Boomershine or Fero, who reside in Indiana and New York respectively, other than that their PII was stored in the Excellus Network. As a result of the data breach and the theft of his PII and PHI, Mr. Church's Personal Information has been compromised, and he has been forced to spend time attempting to protect himself from future incidents of identity theft and fraud.

Florida

31. Plaintiff Don Korn is a citizen of the State of Florida and resides in the City of Sanibel. At all times relevant hereto, Mr. Korn was enrolled in an Excellus policy. Mr. Korn paid his premiums on a regular basis until 2012; his policy premiums have been paid by Medicare since 2012. Excellus collected and received Mr. Korn's PII and PHI, which it maintained in the Excellus Networks. In 2015, Mr. Korn learned that someone had attempted to procure credit cards with two different banking entities using Mr. Korn's personal information. In response to this incident, Mr. Korn placed 90-day fraud alerts on his credit reports with each of the three major credit reporting bureaus. Further, although he prevented the credit cards from being issued in his name, Mr. Korn spent several hours to remediate the situation and freeze his credit. In the fall of 2015, Mr. Korn received a letter from Excellus informing him that his PII and PHI, as well the PII and PHI of his wife, may have been compromised in the data breach. Following his notification of the breach, Mr. Korn enrolled in the two-year credit monitoring service offered through Kroll and placed fraud alerts on his credit cards. In addition, Mr. Korn filed an identity theft report with the Sanibel Police Department and the FTC. As a result of the data breach, Mr. Korn and his wife's Personal Information has been compromised, and he has spent several hours

attempting to remediate the financial fraud caused by the breach and to protect himself and his wife from future incidents of identity theft and fraud.

Indiana

32. Plaintiff Therese Boomershine is a citizen of the State of Indiana and resides in the Town of Roanoke. Lifetime collected and received Ms. Boomershine's PII and PHI, which it maintained in the Excellus Networks. In the fall of 2015, Ms. Boomershine received a letter from The Lifetime Healthcare Companies informing her that her PII and PHI may have been compromised in the data breach. Following her notification of the breach, Ms. Boomershine enrolled in the two-year credit monitoring service offered through Kroll, took steps to implement credit freezes with the three major reporting bureaus, and ordered copies of her most recent credit report. In addition, she filed a police report with the Roanoke Police Department and an identity theft report with the Federal Trade Commission. Ms. Boomershine also obtained an additional credit monitoring service called Credit Karma. In or around March of 2017, Sylint Group conducted a DarkNet search and located Ms. Boomershine's PII for sale in the same data set where plaintiffs Fero and Church's PII was also for sale. Ms. Boomershine has no connection to plaintiffs Fero or Church, who reside in New York and California respectively, other than that their PII was stored in the Excellus Network. As a result of the breach, Ms. Boomershine's Personal Information has been compromised, and she has spent significant time attempting to protect herself from identity theft and fraud.

New Jersey

33. Plaintiff Carlos Martinho is a citizen of the State of New Jersey and resides in the Township of Lakewood. Mr. Martinho's spouse was enrolled in an Excellus policy,

under which Mr. Martinho was a named beneficiary. Mr. Martinho and his spouse jointly paid the policy premiums. Excellus collected and received Mr. Martinho's PII and PHI, which it maintained in the Excellus Networks. In the fall of 2015, Mr. Martinho received a letter from Excellus informing him that his PII and PHI may have been compromised in the data breach. His wife and his two children received letters as well. Following his notification of the breach, Mr. Martinho attempted to enroll in the free credit monitoring service offered through Kroll, but had difficulty with its webpage while signing up and was unable to complete the process because the sign-up process was not functioning. Thus, he enrolled in a credit monitoring service called Credit Karma and ordered the most recent copy of his credit report. On February 26, 2016, Mr. Martinho was notified via text message by Chase Bank that a suspicious purchase had been charged to his credit card at a home furnishing store in the amount of $100.91. Mr. Martinho immediately contacted Chase, learned that the purchase was made in California, and notified Chase that it was fraudulent. He also placed a freeze on his credit with the three major credit reporting bureaus and filed an identity theft complaint with the FTC. He also he placed an alert with ChexSystems, a nationwide specialty consumer reporting agency, and obtained a copy of his credit report through it. Although the charges were ultimately reversed, Mr. Martinho spent several hours and approximately $20 taking measures to protect himself from future fraud. As a result of the data breach, Mr. Martinho's Personal Information has been compromised, and he has spent significant time attempting to remediate the financial fraud that he experienced and attempting to protect himself and his family from future incidents of identity theft and fraud.

North Carolina

34. Plaintiff Thomas Albrecht is a citizen of the State of North Carolina and resides in the City of Charlotte. Mr. Albrecht has been insured under a policy with United Healthcare since August 2014. He was previously employed at Chobani, Inc., where he received health benefits under a policy with Excellus. Excellus collected and received Mr. Albrecht's PII and PHI, which it maintained in the Excellus Networks. In March 2015, and then again in early September 2015, Mr. Albrecht and his wife were the victims of credit card fraud. In the fall of 2015, Mr. Albrecht received a letter from Excellus informing him that his PII and PHI may have been compromised in the data breach. Following his notification of the breach, Mr. Albrecht filed an identity theft complaint with the FTC. Over the past two years, he has noticed that he is also frequent recipient of "phishing" emails. As a result of the breach, Mr. Albrecht's Personal Information has been compromised, and he has spent numerous hours researching methods to protect himself and his wife from future instances of identity theft and fraud.

Pennsylvania

35. Plaintiff Brenda Caltagarone is a citizen of the State of Pennsylvania and resides in the City of DuBois. Ms. Caltagarone is unsure how or why her information was compromised in the Excellus data breach, but she believes her employer, Cenclear, obtains services from one of the Defendants. Lifetime collected and received Ms. Caltagarone's PII and PHI, which it maintained in the Excellus Networks. In the fall of 2015, Ms. Caltagarone received a letter from The Lifetime Healthcare Companies informing her that her PII and PHI may have been compromised in the data breach. As a result of the breach, Ms. Caltagarone's Personal Information has been compromised.

Defendants

36. Defendant Excellus Health Plan Inc. is a New York domestic not-for-profit corporation registered with the New York Department of State to do business in New York and organized under Article 43 of the New York State Insurance Law. Excellus' headquarters are located at 165 Court Street, Rochester, New York 14647.

37. Excellus is the primary healthcare provider in upstate New York. It is a licensee of the Blue Cross Blue Shield Association and operates under the following trade names: Excellus BlueCross BlueShield; Excellus BlueCross BlueShield Rochester Region; Excellus BlueCross BlueShield Central New York Region; Excellus BlueCross BlueShield Central New York Southern Tier Region; Excellus BlueCross BlueShield Utica Region; and Univera Healthcare. Excellus conducts extensive business throughout upstate New York and maintains regional headquarters in Buffalo, Rochester, Utica, Elmira, and Syracuse, as well as field offices in Watertown, Binghamton, Oneonta, and Plattsburgh.

38. Because Excellus also contracts with the federal government, at least some of its healthcare plans qualify as health plans for individuals receiving Medicare. Indeed, Excellus is the parent of two health maintenance organizations ("HMOs") in the New York State Health Insurance Program: Blue Choice and HMO Blue.

39. Excellus is a subsidiary of Defendant Lifetime, which is Excellus' sole parent company. Excellus is also a parent company to the remaining Lifetime Defendants.

40. Defendant Lifetime Healthcare, Inc. is a New York domestic not-for-profit corporation registered with the New York Department of State to do business in New York. Lifetime's headquarters are located at 165 Court Street, Rochester, New York 14647.

41. Lifetime is the parent and/or holding company of a $6.6 billion family of companies, known as The Lifetime Healthcare Companies, that finances and delivers health care in New York State, as well as long-term care nationwide. The Lifetime Healthcare Companies include Excellus BlueCross BlueShield, Univera Healthcare, Lifetime Benefit Solutions, Inc., Lifetime Care, Lifetime Health Medical, and MedAmerica Insurance Company.

42. As the sole member of Excellus, Lifetime exercises complete domination over Excellus such that there is no essential difference between the two entities with respect to, *inter alia*, the December 2013 data breach described herein. For example, Lifetime and Excellus released a single Annual Financial Report in 2013 and 2014, which shows that the companies' high level employees, including the CEO and vice presidents, as well as the Board of Directors, are identical.

43. According to The Lifetime Healthcare Companies' 2014 Annual Financial Report, Lifetime's 2014 total revenue exceeded $13,500,000,000.

44. Defendant Lifetime Benefit Solutions, Inc. is a domestic business corporation registered with the New York Department of State to do business in New York. Its headquarters are located at 115 Continuum Drive, Liverpool, New York 13088, and it has additional offices in Rochester, Buffalo, and Cobleskill, New York. Lifetime Benefit primarily provides employee benefits administration and risk management services across the United States. Lifetime Benefit is an affiliate of The Lifetime Healthcare Companies, and Lifetime and Excellus own and exercise complete control over Lifetime Benefit.

45. Defendant Genesee Region Home Care Association, Inc. d/b/a Lifetime Care is a domestic not-for-profit corporation registered with the New York Department of

State to do business in New York. Lifetime Care provides in-home and specialty service care to over 30,000 hospice patients per year in Monroe, Wayne, Seneca, Cayuga, Yates, Schuyler, Ontario, and Livingston counties in New York. Lifetime Care is an affiliate of The Lifetime Healthcare Companies, and Lifetime and Excellus own and exercise complete control over Lifetime Care.

46. Defendant Genesee Valley Group Health Association d/b/a Lifetime Health Medical Group is a domestic not-for-profit corporation registered with the New York Department of State to do business in New York. Lifetime Health Medical is a physician group that provides primary health care to patients in Rochester and Buffalo, New York. Health centers associated with Lifetime Health Medical provide pharmacy, laboratory, radiology, internal medicine, pediatrics, family practice, and specialty care. Lifetime Health Medical is an affiliate of The Lifetime Healthcare Companies, and Lifetime and Excellus own and exercise complete control over Lifetime Health Medical.

47. Defendant MedAmerica, Inc. is a domestic business corporation registered with the New York Department of State to do business in New York. Its headquarters are located at 165 Court Street, Rochester, New York 14647. MedAmerica, Inc. is the parent company of three MedAmerica affiliates: MedAmerica Insurance Company of New York, MedAmerica Insurance Company of Pennsylvania, and MedAmerica Insurance Company of Florida. These entities, collectively referred to as "MedAmerica," provide health insurance products primarily in New York, Pennsylvania, and Florida. MedAmerica is a subsidiary of The Lifetime Healthcare Companies, and Lifetime and Excellus own and exercise complete control over MedAmerica.

48. Defendant Univera Healthcare is a not-for-profit organization with its headquarters located at 205 Park Club Lane, Buffalo, New York 14221. Univera markets health insurance products primarily in western New York, maintaining business relationships with over 5700 providers. Univera is part of The Lifetime Healthcare Companies, and Lifetime and Excellus own and exercise complete control over Univera.

49. Defendants Blue Cross and Blue Shield Association is incorporated and headquartered in Illinois. BCBSA is a federation of 36 health insurance organizations and companies that provides health insurance to over 106 million individuals.

50. Throughout this Amended Consolidated Master Complaint, Excellus, Lifetime, Lifetime Benefit, Lifetime Care, Lifetime Health Medical, and MedAmerica, and Univera are collectively referred to collectively as the "Lifetime Defendants." Defendants Lifetime Benefit, Lifetime Care, Lifetime Health Medical, and MedAmerica, and Univera may also be referred to collectively as the "Affiliate Defendants."

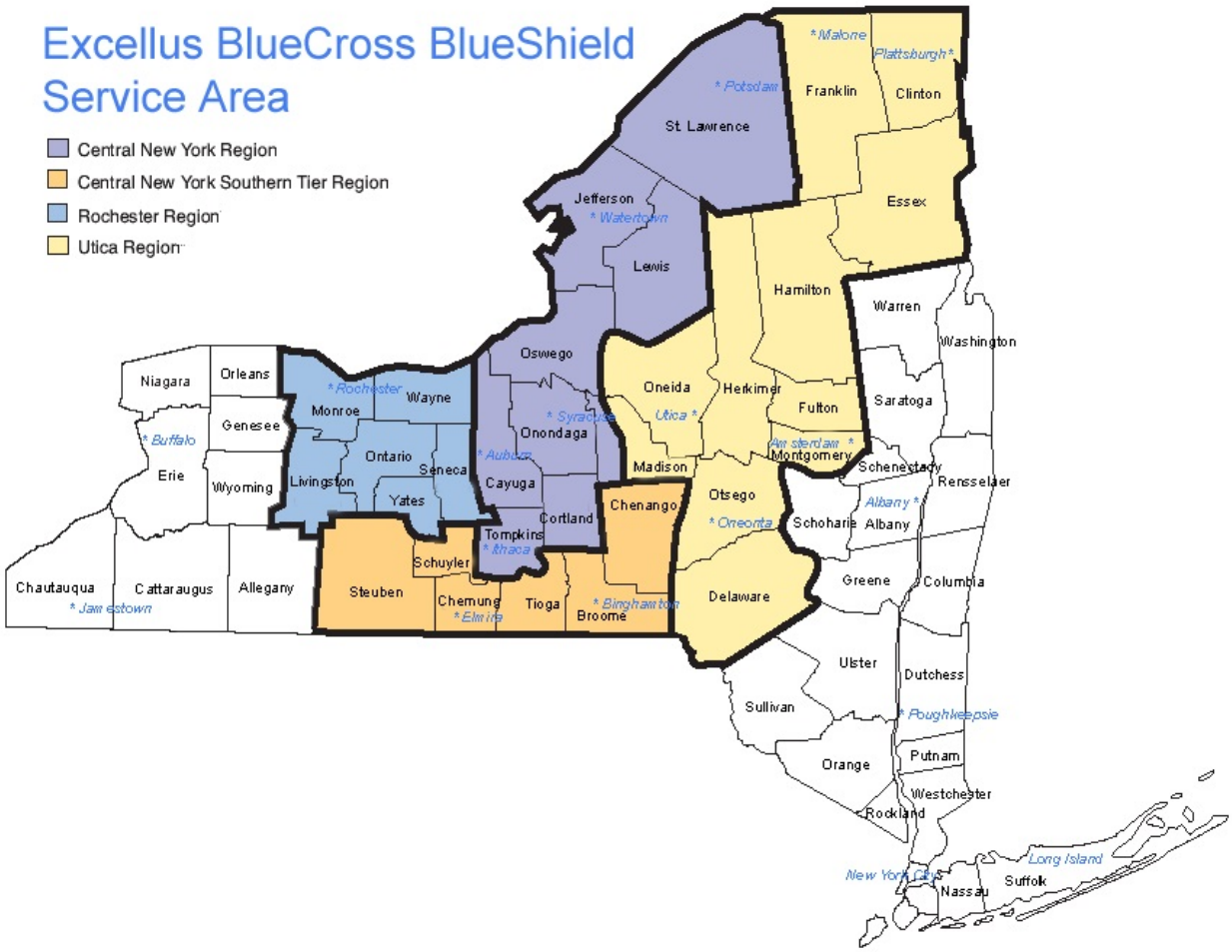
FACTUAL BACKGROUND

51. On or before December 23, 2013, hackers infiltrated Excellus' Information Technology systems, eventually gaining access to Personal Information on approximately 10 million adults and minor children. Defendants promised customers they would safeguard their Personal Information; indeed, customers would not have engaged Defendants' services or provided Defendants with their Personal Information but for such promises. Defendants undertook to store in the Excellus Networks sensitive—and valuable—Personal Information that they collected from current and former customers, as well as potential customers. Worse yet, although Defendants were required by law to implement certain safeguards to protect the information, they failed to do so. The result was not only one of the most serious data breaches in US history, but also one that went undetected for an abnormally lengthy period of time. Defendants failed to detect that intruders were freely operating in their systems for twenty months, thereby exposing Plaintiffs and Class Members to significantly more actual and prospective harm than they would have faced had Defendants diligently monitored the Excellus Networks. The facts set forth below demonstrate that Defendants failed to comply with the obligations imposed by law and that Plaintiffs and Class Members suffered injury as a result.

Defendants Collect and Store Significant Amounts of Valuable Personal Information

52. The Lifetime Healthcare Companies comprise one of the largest healthcare conglomerates in New York State. Excellus currently insures more than 1.6 million individuals in upstate New York alone, and provides direct health care to many more.

53. The primary Excellus "service area" encompasses 31 upstate New York counties, covering central New York, the Southern Tier, the Rochester region, and the Utica region. A map of the Excellus service area is set forth below:



Source: http://www.excellus.com/webcontent/docs/map.html

54. Excellus also cooperates with BCBSA and other independent Blue Cross Blue Shield ("BCBS") licensees to participate in the BlueCard program. Under the BlueCard program, members of one BCBS licensee may access another BCBS licensee's provider networks and discounts. Thus, an individual insured by a BCBS licensee may access Excellus' provider network if he or she requires healthcare services in the Excellus service area.

55. As part of their routine business, Defendants collect, receive, and access records of customers' and members' Personal Information, as well as the Personal Information of healthcare providers. These records include PII, such as names, dates of birth, social security numbers, member identification numbers, home addresses, telephone numbers, and financial information. Defendants also collect, receive, and access PHI, such as clinical and medical claims information.

56. The Lifetime Defendants' Information Technology security policies and infrastructure were largely centralized at the corporate level. Accordingly, the Excellus Networks contain Personal Information held by each of the Lifetime Defendants. This includes the Personal Information of approximately 7 million current and former Excellus customers and approximately 3 million customers who received services from the Affiliate Defendants. Upon information and belief, the database also contained the Personal Information of individuals who applied for insurance with Defendants but never purchased a plan, as well as individuals who are or were listed as beneficiaries on a policy. Some of the information within the database pertains to services rendered for individuals as far back as the early 1980s. Many of the individuals whose Personal Information was stored in the Excellus Networks had not been insured or received services from any Defendant in a number of years and, in some cases, even decades. The Excellus Networks also contain Personal Information pertaining to individuals insured by other BCBS entities, but who received treatment in the Excellus service area through the BlueCard program.

57. Upon information and belief, Defendants do not retain customer insurance contracts for longer than ten years. However, as evidenced by the information compromised in the Excellus data breach, Defendants apparently maintain the Personal

Information of current and former customers for decades, including individuals who applied for insurance but never enrolled in a policy.

58. Discovery is likely to demonstrate additional facts regarding the Excellus Networks and Defendants' inadequate data security practices and its unreasonable and unnecessary Personal Information retention practices.

Defendants Promised to Protect and Safeguard Personal Information

The Lifetime Defendants' Privacy Policies

59. Defendants understand that customers place a premium on privacy, especially as it pertains to sensitive health-related information. Thus, Defendants provide each of its customers with a notice of privacy practices and other privacy statements.[2] Each also dedicates a section of its website to explaining its privacy and data collection policies.[3]

60. At all times relevant hereto, Excellus' notice of privacy practices assured its customers of the privacy of their PII and PHI. The Excellus notice states:

> We understand that medical information about you and your health is personal. We are committed to safeguarding your protected health information (PHI). . . . We (Excellus BlueCross BlueShield) are required by applicable federal and state laws to maintain the privacy of your PHI. We are required to give you notice about our privacy practices, our legal duties, and your rights concerning PHI. We must follow the privacy practices that are described in this notice while it is in effect, including notification should there be a breach of your unsecured PHI.

[2] *See, e.g.*, Exhibit A, Excellus Privacy Practices.

[3] *See, e.g.*, Excellus Website Privacy Policies, *available at* https://www.excellusbcbs.com/wps/portal/xl/our/compliance/privacy (last visited Mar. 25, 2016). The privacy section of Excellus's website is substantially similar to the printed notice of privacy practices provided to each Excellus customer.

61. Under the heading, "Uses and Disclosures of Nonpublic Personal Information," the notice represents that Excellus "will not give out your nonpublic personal information to anyone unless [it] is permitted to do so by law" or authorized by individual consent. The notice further explains that "nonpublic personal information" is defined as, *inter alia*, "names, member identification number, social security number, addresses, type of health care benefits, payment amounts, etc."

62. Excellus' notice of privacy practices acknowledges that Excellus may provide customer PII or PHI for treatment, payment, healthcare operations, and other limited purposes, but in each instance, the notice stresses that Excellus will only disclose information where it is required to do so by law or authorized by individual consent.

63. The privacy notice underscores Excellus' commitment to privacy by highlighting the following security measures: Excellus "employees sign an agreement to follow [its] Code of Business Conduct"; "employees are required to complete [its] privacy training program"; Excellus has "implemented the necessary sanctions for violation of [its] privacy practices"; Excellus has "a privacy oversight committee that reviews [its] privacy practices" and a "security coordinator to detect and prevent security breaches"; "all computer systems that contain personal information have security protections; and Excellus "randomly check[s] provider offices on a routine basis to ensure that medical records are kept in secure locations."

64. In addition, Excellus' notice of privacy practices states that it "will notify you should there be a breach of unsecured information." The notice acknowledges that Excellus is "required to notify [customers] if there is any acquisition, access, use, or disclosure" of their unsecured PII or PHI that compromises its security or privacy.

65. The website privacy policy on Excellus' website repeats and adds to these assurances. It states that Excellus is "committed to protecting any personal information that [customers] provide [it] on this website according to applicable laws, regulations and accreditation standards and practices."

66. What is more, Excellus emphasizes that customers must provide it with their PII in order to obtain its healthcare services:

> In order to access certain services and restricted areas within the website or to respond to specific inquiries, Excellus BlueCross BlueShield requires that you provide Personally Identifiable Information. This information may include, without limitation, your legal name, address, telephone number, email address, subscriber name or "screen name," and password used to access these services. We may also collect the email addresses of visitors that communicate with us via email; information provided by the visitor in online forums, registration forms, surveys, email messages, and other online features (including demographic and personal profile data); and visitor-specific information about the pages on this site that our visitors access. We reserve the right to request any additional information necessary to establish and maintain your account for use of the services and access to the restricted areas.

67. Excellus' website privacy policy represents that "Personally Identifiable Information collected when [users] visit this website will not be shared with or otherwise disclosed to anyone outside the Excellus BlueCross BlueShield family of companies without the consent of the person(s) authorized to permit [Excellus] to do so," unless disclosure is required by law.

68. Lifetime's privacy policies, which are applicable to all The Lifetime Healthcare Companies, also promise to safeguard the PII and PHI of its customers.[4] These

[4] *See* Lifetime Healthcare Companies' Privacy Policy, *available at* http://www.lifethc.com/privacy.html (last visited Mar. 25, 2016).

policies are substantially similar to Excellus' website privacy policy, and assure customers that Lifetime "is committed to protecting [customers'] personal information when [users] provide it over the phone, in person, or through the mail." The Lifetime policy further states that PII "will not be shared with or otherwise disclosed to anyone outside the Lifetime Health Family of Companies" without individual consent unless required by law. Lifetime's policy does not disclose that all PII or PHI provided to Lifetime or any of the Defendants will be stored indefinitely in the Excellus Networks.

69. The Affiliate Defendants also provide customers with a notice of privacy policies that is substantially similar to the notice of privacy policies provided by Excellus to its customers,[5] and, like the Excellus notice of privacy policy set forth above, promises to safeguard customer PII and PHI. The Affiliate Defendants' notice of privacy policies state that the Affiliate Defendants will not disclose customer PII or PHI without customer authorization unless required by law. None of the Affiliate Defendants' policies disclose that customer PII or PHI will be transferred to Excellus and/or stored indefinitely in the Excellus Networks.

70. Many documents provided by the Lifetime Defendants to customers, including their contract documents, referred to these privacy policies and notices and encouraged customers to view online the information regarding their privacy policies and practices set forth in those notices.

[5] *See, e.g.*, Exhibit B, Lifetime Benefit Privacy Policies; Exhibit C, Lifetime Care Privacy Policies; Exhibit D, Lifetime Health Medical Privacy Policies; Exhibit E, MedAmerica Privacy Policies.; Exhibit F, Univera Privacy Policies.

The Lifetime Defendants' Contracts

72. The importance of maintaining customers' privacy and protecting sensitive customer information is also explicitly acknowledged in the Lifetime Defendants' contracts with their customers.

73. For customers with individual policies through Excellus, the documents containing the terms of these contracts are sometimes called the "Contract," the "Certificate of Coverage," or "Evidence of Coverage."

74. Excellus provides individuals enrolled under a group insurance policy with a policy document referred to alternately as a "Certificate of Coverage," a "Member Handbook," or a "Member Certificate." These documents set out the benefits, terms, and conditions that are incorporated in the contracts between Excellus and the individuals enrolled in the group policy.

75. Excellus policy documents incorporate the Excellus notice of privacy practices, either by reference or by appending the notice to the policy document. This is the case for both individual policy contracts and group contracts.

76. For example, excerpts of the 2015 individual policy Contract between Matthew Fero and Excellus are attached hereto as Exhibit G and include the notice of privacy practices as appended to Mr. Fero's Contract.

77. Likewise, excerpts from the 2013 Certificate of Coverage provided to Thomas Albrecht reflecting the terms of the group insurance policy in which Mr. Albrecht enrolled through his employer, Chobani Global Holdings Inc., are attached hereto as Exhibit H and include the notice of privacy practices as appended to Mr. Albrecht's Certificate.

78. Additionally, excerpts from the 2014 Evidence of Coverage provided to Barbara Palmer, which by its terms is part of Excellus' Medicare Advantage HMO Plan contract with Ms. Palmer, are attached hereto as Exhibit I and explicitly incorporate Excellus' notice of privacy practices by reference while also setting forth the following simplified summary of the privacy practices to which Excellus is obligated to adhere:

> **Section 1.4 We must protect the privacy of your personal health information**
> Federal and state laws protect the privacy of your medical records and personal health information. We protect your personal health information as required by these laws.
> • Your "personal health information" includes the personal information you gave us when you enrolled in this plan as well as your medical records and other medical and health information.
> • The laws that protect your privacy give you rights related to getting information and controlling how your health information is used. We give you a written notice, called a "Notice of Privacy Practice," that tells about these rights and explains how we protect the privacy of your health information.
> **How do we protect the privacy of your health information?**
> •We make sure that unauthorized people don't see or change your records.
> • In most situations, if we give your health information to anyone who isn't providing your care or paying for your care, *we are required to get written permission from you first*. Written permission can be given by you or by someone you have given legal power to make decisions for you.
> • There are certain exceptions that do not require us to get your written permission first. These exceptions are allowed or required by law.
> • For example, we are required to release health information to government agencies that are checking on quality of care.
> • Because you are a member of our plan through Medicare, we are required to give Medicare your health information including information about your Part D prescription drugs. If Medicare releases your information for research or other uses, this will be done according to Federal statutes and regulations.

> **You can see the information in your records and know how it has been shared with others**
> You have the right to look at your medical records held at the plan, and to get a copy of your records. We are allowed to charge you a fee for making copies. You also have the right to ask us to make additions or corrections to your medical records. If you ask us to do this, we will work with your healthcare provider to decide whether the changes should be made.
> You have the right to know how your health information has been shared with others for any purposes that are not routine. If you have questions or concerns about the privacy of your personal health information, please call Customer Service (phone numbers are printed on the back cover of this booklet).

79. Defendants, like all healthcare and health insurance providers, draft their insurance policy contracts and provides them to their customers. Plaintiffs and Class Members did not draft these contracts. Defendants use template documents to generate their insurance policy contracts that they provide to customers, and these documents use language and structure that is consistent across plans (despite containing differences in medical services covered, deductibles, and the like).

80. Moreover, as Plaintiffs allege above and as the attached examples reflect, Defendants drafted all of their policy contracts to include references to their privacy policies and notices and to Defendants' websites where those privacy policies were set forth for their customers. There is no material difference in the manner in which these contracts incorporate Defendants' privacy policies, which, upon information and belief, are materially uniform across all of Defendants' customers.[6]

[6] As of the date of this filing, Plaintiffs are not in possession of, and Defendants have not produced, a copy of Dr. Carroll's healthcare provider contract (or any Healthcare Provider Class Member contract). Plaintiffs reserve the right to amend this pleading to set forth the various promises set forth in these contracts.

81. Defendants were therefore contractually obligated to abide by the terms set forth in their notices of privacy practices, and Defendants' customers were entitled to rely upon Defendants' promises to adhere to the privacy practices described therein.

The Federal Blue Cross Blue Shield Plan Policies

82. BCBSA and Excellus also promised to protect the Personal Information of federal government employees who enrolled in the Blue Cross Blue Shield Government-Wide Service Benefit Plan, also known as the Federal Employee Program ("Federal BCBS Plan").

83. The Federal Employees Health Benefits Act of 1959 establishes a comprehensive program of health insurance for federal employees and their families and authorizes the Office of Personnel Management ("OPM") to contract with private carriers to offer federal employees an array of health plans.

84. The Plan Booklet (called the "FEHB Brochure") describes the benefits and services under the Federal BCBS Plan. BCBSA distributed this FEHB Brochure to all enrollees. At all times relevant to this litigation, the then-current year's FEHB Brochure is available on the BCBS Federal Employee Program website (www.fepblue.org). BCBSA also distributed the FEHB Brochure to members of the Federal Employee Class.

85. Enrollees in the Federal BCBS Plan are current and former federal employees and annuitants, including Plaintiff Nina Mottern (collectively, the "Federal Employee Plaintiffs"), who obtained coverage under the Federal BCBS Plan.

86. The Federal Employee Plaintiff and Federal Employee Class Members all were enrolled in the Federal BCBS Plan prior to the Excellus data breach and received the FEHB Brochure.

87. BCBSA, as agent for Excellus and other participating Blue Cross and/or Blue Shield Plans, made specific, material representations with respect to protecting PII, PHI and other sensitive personal information. Among other things, BCBSA, by the terms of its contract, was required to:

a) hold all medical records, and information relating thereto, of federal subscribers, confidential (with limited exceptions that do not apply here); and

b) maintain the necessary resources to meet the obligations under the contract, including security obligations.

88. The FEHB Brochures for 2014 and 2015 both state, "If you are enrolled in this Plan, you are entitled to the benefits described in this brochure." The Brochures define "you/your" to mean "the enrollee (the contract holder eligible for enrollment and coverage under the Federal Employees Health Benefits Program and enrolled in the Plan) and each covered family member." Under the heading, "Your Medical and Claims Records are Confidential," the Brochure promises that "We will keep your medical and claims information confidential."

89. The FEHB Brochures for 2014 and 2015 also incorporate by reference the Notice of Privacy Policy, available at all times at www.fepblue.org. The 2015 Notice of Privacy Practice states:

> This notice describes how we, the Blue Cross and Blue Shield (BCBS) Service Benefit Plan, may use and disclose your protected health information (PHI). It also includes our legal obligations concerning your PHI. . . . Members receive a copy of this Notice at the time of enrollment and annually thereafter.
>
> …
>
> We have measures in place to protect PHI according to state and federal standards. The measures are designed to protect oral, written, and electronic PHI, and include:

- Security and privacy training for all employees.
- Employee access is limited to need-to-know basis. . . .
- All users of our electronic systems are required to use strong passwords.
- All users must change their computer passwords periodically.

90. The www.fepblue.org website also states on its "Rights and Responsibilities" page that the plan will "hold all our member records confidential, and will only release them to the appropriate entities if required to do so by law."

91. The www.fepblue.org website has at all relevant times been incorporated by reference into the FEHB Brochure.[7]

92. BCBSA and Excellus made material misrepresentations and misrepresented and fraudulently advertised material facts about safeguarding federal employees' and annuitant's, including Plaintiff Nina Mottern's, PII and PHI. Instead, they failed to do the following:

- Limit the uses of PII to those specifically allowed;
- Limit access to PII to those on a "need-to-know" basis;
- Allocate the resources necessary to maintain the confidentiality of this information;
- Comply with applicable federal laws regarding data security and

[7] *E.g.*, Blue Cross and Blue Shield Service Benefit Plan 2015, https://www.opm.gov/healthcare-insurance/healthcare/plan-information/plan-codes/2015/brochures/71-005.pdf, at p. 14 ("You may view our Notice of Privacy Practice for more information about how we may use and disclose member information by visiting our website at www.fepblue.org."); Blue Cross and Blue Shield Service Benefit Plan 2011, https://www.opm.gov/healthcare-insurance/healthcare/plan-information/plan-codes/2011/brochures/71-005.pdf, at p. 8 (same).

privacy, including HIPAA;

- Conduct audits or otherwise employ best practices to prevent or halt the unauthorized access to PII;
- Use technical and procedural safeguards adequate to protect PII.

Defendants Were Obligated to Protect PII and PHI under Federal and State Law and the Applicable Standard of Care

96. Defendants Excellus, Lifetime Benefit, Lifetime Care, Lifetime Health Medical, MedAmerica, Univera, and BCBSA are either entities covered by HIPAA, *see* 54 C.F.R. § 160.102, or "business associates" covered by HIPAA, *see* 45 C.F.R. § 160.103, and therefore must comply with the HIPAA Privacy Rule and Security Rule, *see* 45 C.F.R. Part 160 and Part 164, Subparts A and E (setting forth "Standards for Privacy of Individually Identifiable Health Information").

97. HIPAA's Privacy Rule, otherwise known as "Standards for Privacy of Individually Identifiable Health Information," establishes national standards for the protection of health information.

98. HIPAA's Security Rule, otherwise known as "Security Standards for the Protection of Electronic Protected Health Information," establishes national security standards for the protection of health information that is held or transferred in electronic form.

99. HIPAA limits the permissible uses of "protected health information" and prohibits the unauthorized disclosure of "protected health information." 45 C.F.R. § 164.502. HIPAA requires that covered entities implement appropriate safeguards for this information. *See* 45 C.F.R. § 164.530(c)(1).

100. HIPAA obligated Defendants to implement technical policies and procedures for electronic information systems that maintain electronic protected health information so that such systems were accessible only to those persons or software programs that had been granted access rights. *See* 45 C.F.R. § 164.312(a)(1).

101. HIPAA also obligated Defendants to implement policies and procedures to prevent, detect, contain, and correct security violations, *see* 45 C.F.R. § 164.306(a)(1), and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules, *see* 45 C.F.R. § 164.306(a)(3).

102. HIPAA further obligated Defendants to ensure that their workforces comply with HIPAA security standard rules, *see* 45 C.F.R. § 164.306(a)(4), to effectively train their workforces on the policies and procedures with respect to protected health information, as necessary and appropriate for those individuals to carry out their functions and maintain the security of protected health information, 45 C.F.R. § 164.530(b)(1).

103. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule.[8] *See* 45 C.F.R. §§ 164.302-318. For example, the guidance regarding Risk Analysis clarifies the expectations of HHS for organizations required to meet the Security Rule requirements, including information on risk analysis requirements, elements of risk analysis, and a list of resources for covered

[8] *See* US Department of Health & Human Services, Security Rule Guidance, http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html (last visited April 13, 2016).

entities to access.[9] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI." *Id.* These documents are freely available in the public domain.

104. Defendants are and were prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45, from engaging in "unfair or deceptive acts or practices in or affecting commerce." A company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice."

105. As described below, Defendants were also obligated by various state laws and regulations to protect Plaintiffs' and Class Members' sensitive, confidential information.

106. In addition to obligations imposed by federal and state law, Defendants owed and continue to owe a common law duty to Class Members, who entrusted Defendants with sensitive Personal Information, to exercise reasonable care in receiving, maintaining, storing, and deleting the Personal Information in Defendants' possession. Defendants owed and continue to owe a duty to prevent Class Members' Personal Information from being compromised, lost, stolen, accessed, or misused by unauthorized third parties. Part and parcel of Defendants' duty was and is the obligation to provide reasonable security consistent with current industry best practices and requirements, and to ensure Information Technology systems and networks, and the personnel responsible for

[9] *See* US Department of Health and Human Services, Final Guidance on Risk Analysis, http://www.hhs.gov/hipaa/for-professionals/security/guidance/final-guidance-risk-analysis/index.html (last visited April 13, 2016).

those systems and networks, adequately protected and continue to protect Class Members' Personal Information.

107. Defendants owed a duty to Plaintiffs and Class Members, who entrusted Defendants with sensitive Personal Information, to design, maintain, and test the Information Technology systems that housed Class Members' Personal Information, and to ensure that the Personal Information in Defendants' possession was adequately secured and protected.

108. Defendants owed a duty to Plaintiffs and Class Members to create, implement, and maintain reasonable data security practices and procedures sufficient to protect the Personal Information stored in Defendants' computer systems. This duty required Defendants to adequately train employees and others with access to Class Members' Personal Information on the procedures and practices necessary to safeguard sensitive Personal Information.

109. Defendants owed a duty to Plaintiffs and Class Members to implement processes that would enable Defendants to timely detect a breach of its Information Technology systems.

110. Defendants owed a duty to Plaintiffs and Class Members to act upon data security warnings and red flags in a timely fashion.

111. Defendants owed a duty to Plaintiffs and Class Members to disclose when and if Defendants' Information Technology systems and data security practices were not sufficiently adequate to protect and safeguard Class Members' Personal Information.

112. Defendants owed a duty to Plaintiffs and Class Members to timely disclose the fact that a data breach had occurred.

113. Defendants owed these duties to Plaintiffs and Class Members because Plaintiffs and Class Members were foreseeable and probable victims of Defendants' inadequate data security practices. Defendants collected Class Members' Personal Information directly or, in some cases, indirectly from the Affiliate Defendants and BCBSA. The Lifetime Defendants knew that a breach of their data systems would cause Class Members to incur damages and, as detailed below, they knew or should have known that the Excellus Networks were prime targets for a cyberattack. Further, the Affiliate Defendants and BCBSA collected Plaintiffs' and Class Members' Personal Information and provided that information to Excellus. They also entered into business associate and other agreements related to the transmission of Plaintiffs' and Class Members' Personal Information. Accordingly, the Affiliate Defendants and BCBSA knew or should have known that a breach of the Excellus Networks would cause Class Members to incur damages and suffer harm as described herein.

Defendants Knew That They Were Likely Cyberattack Targets, Yet Failed to Implement Adequate Data Security Measures

114. Defendants knew or should have known that their data security systems were inadequate long before the data breach occurred and long before it was discovered.

115. In May 2012, the OCR notified Univera that it would be conducting an audit to verify Univera's compliance with HIPAA's Privacy, Security, and Breach Notification Rules. The OCR engaged KPMG, an audit, tax, and advisory firm, to perform the audit. Univera is a subsidiary of Excellus and Lifetime, and operates under their complete control. Moreover, due to the network infrastructure, the audit of Univera was an audit of the Excellus Network.

116. Between June and August 2012, KPMG evaluated documents submitted in

support of Univera's security practices, and conducted an on-site evaluation.

117. In its documentary submissions to KPMG, Univera's Corporate Privacy Officer, who used a lifetime.com email address, indicated that Univera's policies and procedures were dictated by its parent company.

118. The audit found that Univera's (and thus, the Lifetime Defendants') Risk Assessment Policies & Procedures failed to identify the risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI ("ePHI"). Furthermore, Univera was not even aware that it was required by law to conduct an accurate and thorough assessment of the potential risks to ePHI and had not even identified all of the processes that involve creating, receiving, maintaining, and transmitting ePHI.

119. In the wake of the audit findings, Univera claimed that it would improve its risk assessment programs for ePHI as a priority project for 2013.

120. In addition to the OCR's express warnings about Defendants' deficient data security practices, Defendants were, or should have been, on notice before, during, and after the breach that healthcare companies were prime targets for cyberattacks, as health care industry authorities on cybersecurity had widely announced the severity of the threat and urged the industry to take protective action.

121. For example, in December 2012, the Ponemon Institute issued its Third Annual Benchmark Study on Patient Privacy and Data Security. The study, which included data from 80 participating healthcare organizations, found that cyber attacks were involved in approximately 33 percent of all healthcare data breaches.[10] The healthcare companies

[10] Third Annual Benchmark Study on Patient Privacy & Data Security at 9, Ponemon Institute, Dec. 2012, http://lpa.idexpertscorp.com/acton/attachment/6200/f-0033/1/-/-/-/-/file.pdf.

themselves generally "agree[d] that patients are at a greater risk of financial identity theft if their records are lost or stolen."[11]

122. In September 2013, the Ponemon Institute issued its 2013 Report on Medical Identity Theft, which reached similar conclusions.

123. In April 2014, the Federal Bureau of Investigation (FBI) Cyber Division issued a "Private Industry Notification" that explained how "the health care industry is not technically prepared to combat against cyber criminals' basic cyber intrusion tactics, techniques and procedures (TTPs), much less against more advanced persistent threats (APTs). The health care industry is not as resilient to cyber intrusions compared to the financial and retail sectors, therefore the possibility of increased cyber intrusions is likely."

124. As if on cue, the records of over 12,000 patients were compromised when hackers gained access to the accounts of employees of Centura Health Systems of Colorado Springs. This event was followed in August 2014 by a data breach of Community Health Systems, Inc., the second largest for-profit hospital chain in the United States. In that incident, hackers stole the social security numbers of 4.5 million customers.

125. After news broke of the breach of Community Health Systems, the FBI warned that hackers were targeting health care companies.[12] The FBI stated that it "has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[13]

---

[11] *Id.* at 12.

[12] *See* Jim Finkle, *FBI warns healthcare firms* that *they are targeted by hackers*, Reuters (Aug. 2014, 4:32 PM), http://www.reuters.com/article/2014/08/20/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820.

[13] *Id.*

126. These events were not surprising to security analysts who were paying attention to the healthcare industry. Martin Walter, senior director at cybersecurity firm RedSeal, stated that companies in the healthcare industry "in comparison spend significantly less on security, making them tentatively easier targets."[14]

127. Dave Kennedy, chief executive of information security firm TrustedSEC, has explained that healthcare organizations are targets because they maintain troves of data with significant resale value in black markets and their security practices are less sophisticated than those of other industries. "Health organizations sometimes rely on legacy systems, and some have not invested in cybersecurity at a rate that matches the urgency of the threats they face. The medical industry is years behind other industries when it comes to security."[15]

128. The cybersecurity firm WhiteHat recently reported that in the healthcare industry, only 24 percent of known security flaws are fixed at any given time.[16]

129. These warnings, and others like them, put Defendants on notice that healthcare and health insurance companies were a target of cyberattack, and that these

---

[14] *See* Data Breach at Anthem May Forecast a Trend, New York Times, Reed Abelson & Julie Creswell, Feb. 6, 2015, *available at* http://www.nytimes.com/2015/02/07/business/data-breach-at-anthem-may-lead-to-others.html (last visited Mar. 29, 2016).

[15] *See* 2015 is Already the Year of the Health-Care Hack—and It's Only Going to Get Worse, Wash. Post, Andrea Peterson, Mar. 20, *available at* http://www.washingtonpost.com/blogs/the-switch/wp/2015/03/20/2015-is-already-the-year-of-the-health-care-hack-and-its-only-going-to-get-worse/ (last visited Mar. 29, 2016). In this context, the term "legacy systems" refers to computers and networks acquired by a company as part of the purchase or merger of another company; the acquired company's computers and networks become the property and responsibility of the acquiring company.

[16] Premera Hack: What Criminals Can Do With Your Healthcare Data, Christian Science Monitor, Jaikumar Vijayan, Mar. 20, 2015, *available at* http://www.csmonitor.com/World/Passcode/2015/0320/Premera-hack-What-criminals-can-do-with-your-healthcare-data (last visited Mar. 29, 2016).

companies had an obligation to implement reasonable safeguards to keep pace. Defendants, quite simply, failed to heed the clear and unequivocal warning.

Defendants Allowed Their Information Technology System To Be Hacked and Failed, Despite Several Opportunities, to Uncover the Intrusion for Nearly 600 Days

130. Despite ample warning that hackers were targeting healthcare companies, Defendants failed to implement sufficient safeguards to detect the hackers—let alone prevent the attack.

131. In December 2013, hackers gained access to the Lifetime Defendants' Information Technology systems. For the next twenty months, these intruders operated in the Excellus Networks with impunity while defendants missed several opportunities to detect the attacker's presence.

132. For example, on December 23, 2013, Attorneys' Eyes Only Pursuant to Protective Order [redacted].

133. On March 4, 2015, Attorneys' Eyes Only Pursuant to Protective Order [redacted]

134. In the wake of other high-profile healthcare data breaches at Anthem, Inc., and Premera Blue Cross, Defendants hired cybersecurity company Mandiant to forensically assess their systems. On August 4, 2015, while conducting this assessment,

Mandiant discovered malware on Defendants' Information Technology systems.

135. Over the next several weeks, Mandiant continued scanning Defendants' Information Technology environment. The evidence Mandiant was able to locate indicated that the data breach began on or more likely before December 23, 2013 and continued until at least August 18, 2014 (though Defendants have publicly conceded that the cyber attackers had the ability to access to their Information Technology systems as recently as May 11, 2015).

136. During the data breach, the hackers had access to highly sensitive personal, health, and financial information, including names, dates of birth, social security numbers, mailing addresses, telephone numbers, member identification, financial payment information, and medical insurance claims information. Some of this financial payment information included credit card numbers.

137. The cyber attackers also obtained the Personal Information of healthcare providers, including copies of their medical licenses.

138. Although the information in Defendants' system was encrypted, this traditional safeguard was largely irrelevant because the hackers accessed the Excellus systems with administrators' credentials and then went undetected for months. Indeed, Defendants have acknowledged that during this breach, hackers likely circumvented their encryption by accessing decryption keys available to administrators on the system.

139. Adam Kujawa, malware intelligence leader at cybersecurity firm Malwarebytes, recently stated: "With an attack of this magnitude, being done over the course of more than a year, cybercriminals probably stole information by simply copying and pasting it from its unencrypted form on the secure network to their own systems, or

utilizing built-in tools to parse the information for the most valuable data."[17]

140. On or about September 9, 2015, Defendants publicly disclosed the breach, and stated that between 10 and 10.5 million individuals were affected. The affected individuals include not only past and current Excellus policyholders, but also those insured and/or receiving healthcare-related services through Defendants' affiliates. Defendants then offered all adult victims two years of free credit monitoring through non-party credit monitoring service provider Kroll, Inc.

141. Remarkably, although Defendants know that many of the affected victims are minors, they have offered no protection specifically tailored to the protection of minor victims. For example, the letter sent to Plaintiff Matthew Fero's children states: "[W]e have secured the services of Kroll to provide identity theft protection at no cost to your child for two years," and explains that those services include "Identity Theft Consultation and Restoration." The letter sent to Mr. Fero, however, and other adult victims specifically states: "To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file." This provision means that the minor children victims of the data breach cannot receive credit services through Kroll and renders Defendants' belated offer of protection an empty gesture.

142. Moreover, the letter sent to victims of the breach provides no guidance to parents seeking to protect affected minors.

143. In the weeks following Defendants' disclosure of the breach, law

[17] *Hackers Home In On Health, Education, Government Sectors*, http://www.technewsworld.com/story/82495.html (last visited Mar. 29, 2015).

enforcement authorities in western New York reported a sharp uptick in incidents of identity theft and/or fraud. Police in Batavia, New York, for example, stated that they received several identity theft complaints possibly linked to the Excellus breach. Plaintiffs' experiences demonstrate that the injuries caused by this data breach continue to mount and, unfortunately for the victims of this breach, are likely to continue well into the future.

PII and PHI was Stolen from Excellus' Network as a Result of the Data Breach

144. The Mandiant Intrusion Report documents that the attacker [redacted]

145. The attackers Attorneys' Eyes Only Pursuant to Protective Order [redacted].

146. The attackers Attorneys' Eyes Only Pursuant to Protective Order [redacted]

147. The attackers Attorneys' Eyes Only Pursuant to Protective Order [redacted]

148. Mandiant also found Attorneys' Eyes Only Pursuant to Protective Order [redacted]

149. Mandiant also found Attorneys' Eyes Only Pursuant to Protective Order [redacted]

150. When considering the attackers' activities and plaintiffs' PII and PHI for sale on the DarkNet (Dark Web), it is clear that the attackers targeted and exfiltrated PII and PHI from the Excellus Network for sale on the DarkNet.

The Data Breach Was the Result of Defendants' Failure to Implement Adequate Cyber Security in the Face of a Known Risk

151. In the wake of the data breach, Mandiant issued a number of recommendations for Defendants to employ in improving their data security. These included standard remediation actions such as resetting passwords for known compromised accounts and removing infected systems from the network. Mandiant also recommended that Defendants implement basic security precautions, including the following:

- requiring all employees to use two-factor authentication when logging in remotely;
- strengthening password policies for privileged user accounts to stymie attempts at password cracking and brute force password guessing;
- making it more difficult to locate passwords stored on key systems, particularly for privileged accounts like local administrator and domain accounts;

- segmenting the network in a manner that prevents system-to-system communications within the Windows environment;
- permitting servers only to communicate with approved IP addresses;
- increasing the types of information captured by log files and forwarded to Defendants' System Information and Event Management ("SIEM") software, for automated analysis and threat assessment;
- prioritizing a then-unfinished security project to simply monitor databases that contain sensitive data; and
- improving Defendants' processes for evidence tracking and incident response.

152. Mandiant's recommendations demonstrate that Defendants' computer systems and data security practices were grossly inadequate to secure the extremely sensitive, valuable, and personal information that had been entrusted to them.

153. For example, Defendants failed to implement many simple, industry-accepted data security practices that would have prevented the data breach: (i) Defendants did not implement a two-factor authentication system in time to stop the data breach. Two-factor authentication means that the user enters a password followed by a number or other piece of data that is separately communicated to the user, for example by a text message sent to a mobile phone number. This is a well-known and widely-implemented precaution, particularly for accessing systems that contain sensitive information; (ii) Defendants' password policies did not require users (even those with key administrator accounts) to employ strong passwords resistant to "brute force" password guessing—repeatedly trying passwords until one works; (iii) password information for accounts with increased access

(privileged accounts) was accessible on key systems; (iv) the network was insufficiently segmented, meaning Defendants failed to establish internal barriers to impede the hackers' ability to move between Defendants' Windows computers, for example, in the search for even more password information or intelligence on how to access Defendants' databases; and (v) Defendants failed to adequately implement logging and monitoring solutions that are designed to alert system administrators to intrusions. Mandiant's recommendations (which identify security flaws commonly seen in breached companies) suggest that if Defendants had implemented these precautions, the data breach would have been stopped before much harm was done.

154. As of February 2016 (and likely still) Defendants had not implemented all of Mandiant's recommended security improvements, leaving Plaintiffs' and Class Members' data vulnerable to future data breaches.

Plaintiffs and Class Members Were Seriously Harmed by the Defendants' Data Breach

155. Victims of the Defendants' data breach have suffered, or are at imminent risk of further suffering, identity theft and medical identity theft. Three plaintiffs' PII has already been located for sale on the DarkNet. In fact, as described above, these three plaintiffs who live in three different states and have no relationship to each other except that they are all victims of the data breach, PII was found for sale in the same DarkNet marketplace. As Pam Dixon, executive director of the World Privacy Forum, stated: "When someone has your clinical information, your bank account information, and your Social Security number, they can commit fraud that lasts a long time. Th[is] kind of identity

theft . . . is qualitatively and quantitatively different than what is typically possible when you lose your credit card . . . ."[18]

156. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[19] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[20]

157. Social security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

158. The Social Security Administration has warned that identity thieves can use an individual's social security number and good credit score to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later.[21]

159. Stolen social security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false

[18] Premera Hack: What Criminals Can Do With Your Healthcare Data, Christian Science Monitor, Jaikumar Vijayan, Mar. 20, 2015, *available at* http://www.csmonitor.com/World/Passcode/2015/0320/Premera-hack-What-criminals-can-do-with-your-healthcare-data (last visited Mar. 10, 2016).

[19] 17 C.F.R. § 248.201 (2013).

[20] *Id.*

[21] Social Security Administration, Identity Theft and Your Social Security Number, *available at* http://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Mar. 10, 2016).

identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her social security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

160. What is more, it is no easy task to change or cancel a stolen social security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse is not typically permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

161. Even then, a new social security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[22]

162. The danger of identity theft is compounded when a minor's social security number and personal information is compromised, as they were here. Whereas adults can periodically monitor their own credit reports, minors typically have no credit to monitor. Thus, it can be difficult, if not nearly impossible, to safeguard against fraud because a minor cannot simply place an alert on his or her credit report. Nor can a minor "freeze" his or her credit report in most states. In order to "freeze" a minor's credit report, a report must

[22] Victims of Social Security Number Theft Find It's Hard to Bounce Back, NPR, Brian Naylor, Feb. 9, 2015, *available at* http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Mar. 10, 2016).

exist. In some instances, and with the assistance of the credit reporting bureaus, a parent may create a credit report for the purpose of freezing it, which requires the electronic submission of the child's birth certificate and social security number to the credit agency. This process is not well known to most consumers, is administratively difficult, and sending such information to the credit agencies predictably causes parents fear and anxiety, especially when the very reason a parent is transmitting such information is to remediate a breach of their child's information. Defendants have not offered victims any counseling to guide them through the steps required to adequately protect the credit of a minor child. Indeed, Defendants have offered virtually nothing to assist Plaintiffs and Class Members in protecting their minor children.

163. Another danger, according to the publisher of *Privacy Journal*, Robert Ellis Smith, is that cyber attackers use stolen social security numbers to obtain medical care in someone else's name.[23] Medical identity theft is even more of a concern in this case because the data compromised in Defendants' breach included medical information.

164. The FTC defines medical identity theft as a cyber attacker "us[ing] [a victim's] name or health insurance numbers to see a doctor, get prescription drugs, file claims with [the victim's] insurance provider, or get other care."[24] Medical identity theft can affect the victim's treatment, insurance and payment records, and credit report.[25]

[23] Victims of Social Security Number Theft Find It's Hard to Bounce Back, NPR, Brian Naylor, Feb. 9, 2015, *available at* http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Mar. 10, 2016).

[24] Medical Identity Theft, Federal Trade Commission, https://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited Mar. 8, 2016).

[25] *Id.*

165. A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[26] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third saw their insurance premiums rise, and 40 percent were never able to resolve their identity theft at all.[27] Further, a report released by the Ponemon Institute concluded that 65 percent of medical identity theft victims spend 200 hours with insurers and providers to secure their credentials and check the accuracy of their personal information, invoices, and e-health records.[28]

166. Moreover, fraudulent medical treatment can have non-financial impacts. Deborah Peel, executive director of Patient Privacy Rights, has described scenarios in which an individual may be given an improper blood type or administered medicines because his or her medical records contain information supplied by an individual obtaining treatment under a false name.[29]

167. To guard against medical identity fraud, cybersecurity experts suggest that individuals routinely obtain the most recent copy of their medical records and inspect them for discrepancies. Defendants' proposed customer solutions do nothing to address the

---

[26] CNET, *Study: Medical identity theft is costly for victims*, http://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last visited Mar. 8, 2016).

[27] *Id.*

[28] Ponemon Institute, 2014 Fifth Annual Study on Medical Identity Theft, *available at* http://medidfraud.org/2014-fifth-annual-study-on-medical-identity-theft/ (last visited Mar. 10, 2016).

[29] *See* 2015 is Already the Year of the Health-Care Hack—and It's Only Going to Get Worse, Wash. Post, Andrea Peterson, Mar. 20, *available at* http://www.washingtonpost.com/blogs/the-switch/wp/2015/03/20/2015-is-already-the-year-of-the-health-care-hack-and-its-only-going-to-get-worse/ (last visited Mar. 10, 2016).

problem of medical identity theft, and Defendants have done nothing to advise their customers how to obtain and inspect their medical records for fraud to comport with best practices identified by security experts.

168. The victims of the Excellus data breach also face imminent risk of health insurance discrimination. Individuals risk denial of coverage, improper "redlining," and denial or difficulty obtaining disability or employment benefits because information was improperly disclosed to a provider. This risk is pervasive and widespread. Indeed, most states maintain government agencies that investigate and combat health insurance discrimination, as does the OCR.

169. Victims of healthcare data breaches are also particularly susceptible to tax return fraud. Such fraud resulted in an estimated $21 billion in losses in 2015 alone, and affected several Plaintiffs and numerous Class Members.

170. Based on the foregoing, the information compromised in the Excellus data breach is significantly more valuable to the cyber attacker than, say, credit card information obtained in a large retailer data breach. Victims affected retailer breaches could avoid much of the potential for future harm by cancelling credit or debit cards and obtaining replacements. The information compromised in the Excellus breach is difficult, if not impossible, to change—social security number, name, date of birth, employment information, income data, medical or clinical information, etc.

171. This data, as one would expect, commands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, has explained that on

the black market, PII and social security numbers are worth ten times the price of stolen credit card information.[30]

172. This estimate may be low. A recent PricewaterhouseCoopers report stated that an identity theft kit containing health insurance credentials can be worth up to $1,000 on the black market, while stolen credit cards may go for $1 each.

173. When it disclosed the breach, Defendants announced that they would offer free credit monitoring services for two years. These services, while helpful, are insufficient. Noted cybersecurity journalist and blogger Brian Krebs has explained: "[T]he sad truth is that most services offer little in the way of real preventative protection against the fastest-growing crime in America [identity theft]."[31] Credit monitoring services, in other words, may inform individuals of fraud after the fact, but do little to thwart fraud from occurring in the first instance.

174. Further, the credit monitoring service offered by Defendants fails to meet even the low industry standard for credit monitoring services. Defendants' chosen service, provided by Kroll, only monitors a victim's credit at one of the three major credit bureaus, but not the other two. For example, Kroll will monitor a victim's credit at TransUnion but not Experian or Equifax. If an unauthorized party applies for a credit line that is not reported to TransUnion, the Kroll credit monitoring will not detect it. Given the severity

[30] Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers, IT World, Tim Greene, Feb. 6, 2015, *available at* http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Mar. 10, 2016).

[31] Brian Krebs, Are Credit Monitoring Services Worth It?, Krebs on Security, Mar. 4, 2014, *available at* http://krebsonsecurity.com/2014/03/are-credit-monitoring-services-worth-it/ (last visited Mar. 10, 2016).

of this breach, Defendants at a minimum should be providing a service that will monitor credit at each of the three major reporting agencies.

175. Further, and as described above, Defendants are not offering credit monitoring for any victim under the age of eighteen, nor providing any information on how to protect minor victims from identity theft, even though they know and understand that many of the victims of this incident are minors. Credit monitoring services that make no attempt to protect the identities and credit of minors and only offer restoration services should a problem arise are not reasonable under the circumstances.

176. All of these injuries suffered by the Plaintiffs and Class Members are a direct and proximate result of the Excellus data breach and include:

a. theft of their Personal Information;

b. costs associated with the detection and prevention of identity theft and unauthorized use of their PII and financial, business, banking, and other accounts;

c. costs associated with the detection and prevention of medical identity theft and unauthorized use of their PHI and insurance accounts;

d. costs associated with time lost addressing and attempting to ameliorate, mitigate, and deal with the actual and future consequences of the Excellus data breach, including finding fraudulent filed tax returns, theft of social security payments, fraudulent charges, cancelling credit cards, evaluating the burden and potential benefit of applying for a new social security number, signing up for and purchasing credit monitoring and identity theft and medical identity theft protection services, the imposition of withdrawal and purchase limits on

compromised accounts, time spent without access to credit while a new credit card is being issued, and the stress, nuisance, and annoyance of dealing with all issues resulting from the Excellus data breach, including additional phishing emails and phone scams;

e. the imminent and certain impending injury flowing from fraud and identify theft posed by their PII and PHI being placed in the hands of unknown third parties;

f. damages to and diminution in value of their Personal Information entrusted to Defendants for the sole purpose of obtaining health insurance or other services from Defendants, with the mutual understanding that Defendants would safeguard against theft and take all steps available to prevent access to or misuse of Plaintiffs' and Class Members' data by unauthorized third parties;

g. money paid to Defendants for health insurance or other services because Plaintiffs and Class Members would not have obtained health insurance or other services from Defendants had Defendants disclosed that they lacked adequate systems and procedures to reasonably safeguard customers' PII and PHI;

h. overpayments to Defendants for health insurance or other services purchased, in that a portion of the price for insurance or other services paid by Plaintiffs and Class Members to Defendants was for the costs of Defendants to take reasonable and adequate security measures to protect PII and PHI, which Defendants failed to do; and

i. continued risk to Plaintiffs' and Class Members' PII and PHI, which remains in the possession of Defendants and which is subject to further breaches so

long as Defendants fail to undertake appropriate and adequate measures to protect the Personal Information entrusted to them.

CLASS ACTION ALLEGATIONS

A. STATEWIDE CLASSES

177. Pursuant to Federal Rules of Civil Procedure 23(a), (b)(1), (b)(2), (b)(3), and (c)(4), Plaintiffs assert common law claims for negligence (Count I), negligence per se (Count II), breach of contract and breach of the implied covenant of good faith and fair dealing (Count III), unjust enrichment (Count IV)], and statutory claims under state consumer protection statutes (Count V), on behalf of separate statewide classes for the states of California, Florida, Indiana, North Carolina, New Jersey, New York, and Pennsylvania, defined as follows:

Statewide [name of State] Class: All citizens of [name of state] whose PII or PHI was compromised by the Excellus data breach.

178. Excluded from the Statewide Classes are (1) Defendants, any entity or division in which Defendants have a controlling interest, and their legal representatives, officers, directors, assigns, and successors; (2) the Judge to whom this case is assigned and the Judge's staff; and (3) governmental entities. Plaintiffs reserve the right to amend the definition of any Class if discovery and further investigation reveal that the Class should be expanded, divided into subclasses, or modified in any other way.

B. FEDERAL EMPLOYEE CLASS

179. Pursuant to Federal Rules of Civil Procedure 23(a), (b)(1), (b)(2), (b)(3), and (c)(4), Plaintiffs assert statutory claims under state consumer protection statutes (Count IV) on behalf of a federal employee class, defined as follows:

> **Federal Employee Class:** All enrollees in the Federal Employee Health Benefits Plan whose Personal Information was compromised by the Excellus data breach.

180. Excluded from the Class are: (1) Defendants, any entity or division in which Defendants have a controlling interest, and their legal representatives, officers, directors, assigns, and successors; (2) the Judge to whom this case is assigned and the Judge's staff; and (3) governmental entities. Plaintiffs reserve the right to amend the Class definition if discovery and further investigation reveal that the Class should be expanded, divided into subclasses, or modified in any other way.

C. HEALTHCARE PROVIDER CLASS

181. Pursuant to Federal Rules of Civil Procedure 23(a), (b)(1), (b)(2), (b)(3), and (c)(4), Plaintiffs assert a common law claim for breach of contract and breach of the implied covenant of good faith and fair dealing on behalf of a class of physicians who submitted Personal Information to Defendants for billing purposes, defined as follows:

> **Healthcare Provider Class:** All healthcare providers and/or medical professionals who submitted PII directly or indirectly to Defendants and whose PII was compromised by the Excellus data breach.

182. Excluded from the Class are: (1) Defendants, any entity or division in which Defendants have a controlling interest, and their legal representatives, officers, directors, assigns, and successors; (2) the Judge to whom this case is assigned and the Judge's staff; and (3) governmental entities. Plaintiffs reserve the right to amend the Class definition if discovery and further investigation reveal that the Class should be expanded, divided into subclasses, or modified in any other way.

D. CERTIFICATION OF THE PROPOSED CLASSES IS APPROPRIATE

Numerosity

183. The exact number of members of the Classes is unknown to Plaintiffs at this time but there are approximately 10 million individuals in all of the Classes combined, and there are thousands to millions of individuals in each class, making joinder of each individual member impracticable. Disposition of the claims of these class members in a single action will provide substantial benefits to all parties and to the Court. Class membership is readily identifiable from information and records in Defendants' possession, custody, or control.

Typicality

184. Plaintiffs' claims are typical of the claims of the Classes in that the representative Plaintiffs, like all Class members, had their PII and PHI compromised in the Excellus data breach. Further, the factual bases of Defendants' misconduct are common to all Class Members and represent a common thread of misconduct resulting in injury to all Class Members.

Adequate Representation

185. Plaintiffs will fairly and adequately represent and protect the interests of the Classes. Plaintiffs have retained counsel with substantial litigation experience, including substantial experience prosecuting consumer and data breach class actions, and therefore Plaintiffs' counsel is also adequate under Rule 23.

186. Plaintiffs and their counsel are committed to vigorously prosecuting this action on behalf of the Classes and have the financial resources to do so. No Plaintiff has interests adverse to those of the Classes, nor do counsel.

Predominance of Common Issues

187. There are numerous questions of law and fact common to Plaintiffs and the Class Members that predominate over any questions affecting only individual Class Members. The answers to these common questions will advance resolution of the litigation as to all Class Members. These common legal and factual issues include:

a. Whether Defendants owed a duty to Plaintiffs and members of the Classes to take reasonable measures to safeguard their Personal Information;

b. Whether Defendants failed to adequately safeguard Plaintiffs' and the Classes' Personal Information;

c. Whether Defendants failed to protect Plaintiffs and the Classes' Personal Information;

d. Whether Defendants knew or should have known that their cybersecurity systems were vulnerable;

e. Whether Defendants' computer systems and data security practices violated HIPAA, federal and state local laws, or Defendants' duties;

f. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiffs' and the Classes' Personal Information properly and/or as promised;

g. Whether Defendants violated the consumer protection statutes applicable to Plaintiffs and each of the Classes;

h. Whether Defendants failed to notify Plaintiffs and members of the Classes about the Excellus data breach as soon as practicable and without delay after the breach was discovered;

i. Whether Defendants acted negligently in failing to safeguard Plaintiffs' and the Classes' Personal Information;

j. Whether implied or express contracts existed between Defendants, on the one hand, and Plaintiffs and the members of the each of the Classes, on the other;

k. Whether Defendants' conduct described herein constitutes a breach of their implied or express contracts with Plaintiffs and the members of each of the Classes;

l. Whether Defendants should retain the money paid by Plaintiffs and members of each of the Classes to protect their Personal Information;

m. Whether Plaintiffs and the members of the Classes are entitled to actual damages, statutory damages, and/or punitive damages as a result of Defendants' wrongful conduct;

n. Whether Plaintiffs and the members of the Classes are entitled to restitution as a result of Defendants' wrongful conduct;

o. What equitable relief is appropriate to redress Defendants' wrongful conduct; and

p. What injunctive relief is appropriate to redress the imminent and currently ongoing harm faced by members of the Classes.

Superiority

188. Plaintiffs and members of the Classes have all suffered and will continue to suffer harm and damages as a result of Defendants' unlawful and wrongful conduct. A

class action is superior to other available methods for the fair and efficient adjudication of this controversy.

189. Absent a class action, most Class Members would likely find the cost of litigating their claims prohibitively high and would therefore have no effective remedy at law. Further, without class litigation, Class Members will continue to incur damages, and Defendants are likely to repeat their misconduct.

190. Class treatment of common questions of law and fact is also a superior method for litigating multiple individual actions in that class treatment will conserve the resources of the courts and the litigants, and will promote consistency and efficiency of adjudication.

CAUSES OF ACTION

FIRST CLAIM FOR RELIEF

Negligence
Brought by Statewide Classes and Healthcare Provider Class Against All Defendants Except BCBSA

191. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Consolidated Master Complaint.

192. Plaintiffs bring this Claim on behalf of the Statewide Classes and the Healthcare Provider Class under their respective state's law.

193. Defendants required Plaintiffs and Statewide Class Members and Healthcare Provider Class Members to entrust with Defendants Personal Information in order to obtain insurance coverage and/or to receive health care services or other services.

194. Defendants, therefore, were entrusted with a massive amount of personally identifiable information belonging to individuals, including Defendants' past and current

insureds and those individuals for whom Defendants provided employee benefit administration or risk management services and/or billing services.

195. Defendants collected and stored this data and knew, or should have known, of the risks inherent in collecting and storing the Personal Information of Plaintiffs and Statewide Class Members and Healthcare Provider Class Members.

196. Defendants owed, undertook, and/or assumed duties of care to use reasonable means to secure and safeguard this Personal Information, to prevent disclosure of the information, and to guard the information from cyber attacks. Defendants' duties include, among others, a responsibility to implement reasonable technical, administrative, and physical security measures that would permit them to detect, respond to, remedy, and promptly notify affected individuals of security breaches in a reasonably expeditious period of time as well as a duty to maintain PII and PHI in their networks only as long as necessary and required by law.

197. Defendants' duties arise from the common law, state statutes cited in this Complaint, the Federal Trade Commission Act, and the following HIPAA regulations:

a. 45 C.F.R. § 164.306(a)(1) for failing to ensure the confidentiality and integrity of ePHI that Defendants created, received, maintained, and transmitted;

b. 45 C.F.R. § 164.306(a)(2) for failing to protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI;

c. 45 C.F.R. § 164.306(a)(3) for failing to protect against reasonably anticipated uses or disclosures of ePHI not permitted under the privacy rules regarding individually identifiable health information;

d. 45 C.F.R. § 164.306(a)(4) for failing to ensure compliance with the HIPAA security standard rules;

e. 45 C.F.R. § 164.308(a)(1)(i) for failing to implement policies and procedures to prevent, detect, contain, and correct security violations;

f. 45 C.F.R. § 164.308(a)(1)(ii)(D) for failing to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports;

g. 45 C.F.R. § 164.312(a)(1) for failing to implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only where access rights have been granted; and

h. 45 C.F.R. § 164.530(b) for failing to effectively and adequately train all members of their workforce on the policies and procedures with respect to protected health information.

198. Defendants' duties also arise from New York's Insurance Laws and Protection Mechanisms for Insurance Payment Information Act, which do not provide private rights of action, but express the public policy of New York and provide evidence of Defendants' duties:

a. N.Y. Ins. Law §§ 2403, 2601(a)(1), which prohibits the knowing misrepresentation of pertinent facts or policy provisions;

b. N.Y. Soc. Serv. § 367-a(2)(b), which requires insurance providers to establish mechanisms to maintain the confidentiality of all individually identifiable information or records;

c. N.Y. Soc. Serv. § 367-a(2)(b), which requires insurance providers to limit the use of individually identifiable information to the specific purpose for which the information was entrusted with Defendants; and

d. N.Y. Soc. Serv. § 367-a(2)(b), which requires insurance providers to not further disclose individually identifiable information entrusted with Defendants.

199. Defendants breached their duties of care by failing to secure and safeguard the Personal Information of Plaintiffs and the Classes. Defendants negligently maintained systems that were vulnerable to a security breach, and they knew or should have known of these vulnerabilities. Further, Defendants' cybersecurity systems were so poorly implemented and maintained that malware was present in the Excellus Networks and permitted to remain undetected in Defendants' systems for nearly 600 days, a period of time far outside the time within which an entity typical discovers a cyber intrusion.

200. Defendants further breached their duty of care by violating the HIPAA regulations and the provisions of the New York Insurance Law and New York Social Services Law set forth above.

201. Defendants acted with wanton disregard for the security of Plaintiffs' and Statewide Class Members' and Healthcare Provider Class Members' Personal Information. Defendants knew or should have known that they had inadequate computer systems and data security practices to safeguard such information, and Defendants knew or should have known that hackers were attempting to access the Personal Information in health care systems, such as Defendants' systems.

202. A "special relationship" exists between Defendants and the Plaintiffs and Statewide Class Members, as well as between Defendants and Healthcare Provider Class Members. Defendants entered into a "special relationship" with the Plaintiffs and Class Members whose Personal Information was requested, collected, and received by Defendants. A "special relationship" also exists between Defendants and Plaintiffs and the Class Members because Defendants are insurers and providers of health plan services and thus stand in a fiduciary or quasi-fiduciary relationship with Plaintiffs and Class Members.

203. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and Statewide Class Members, Plaintiffs and Statewide Class Members and Healthcare Provider Class Members would not have been injured.

204. The injury and harm suffered by Plaintiffs, Statewide Class Members, and Healthcare Provider Class Members was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that they were failing to meet their duties, and that Defendants' breach would cause Plaintiffs, Statewide Class Members, and Healthcare Provider Class Members to experience the foreseeable harms associated with the exposure of their Personal Information.

205. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs, Statewide Class Members, and Healthcare Provider Class Members have suffered injury because, among other things, their Personal Information has been exposed, imminently subjecting each member of the Classes to identity theft, credit and bank fraud, social security fraud, tax fraud, medical identity fraud, and other varieties of identity fraud.

206. Plaintiffs and the Classes have suffered monetary damages and will continue to be injured and incur damages in the future both in an effort to protect

themselves and to remedy acts of fraudulent activity. Plaintiffs and the Classes have suffered, and/or face an imminent risk of suffering, the theft of Personal Information; costs associated with prevention, detection, and mitigation of identity theft, medical identity theft, and/or fraud; costs associated with time spent and productivity loss resulting from addressing the consequences of, or preventing, fraud in any of its forms; and damages from the unconsented exposure of Personal Information due to this breach.

SECOND CLAIM FOR RELIEF

Negligence Per Se
Brought by Statewide Classes and Healthcare Provider Class Against All Defendants Except BCBSA

207. Plaintiffs incorporate by reference the allegations contained in the preceding paragraphs of this Consolidated Master Complaint.

208. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security practices in order to safeguard Plaintiffs' and Class Members' Personal Information.

209. Pursuant to HIPAA, 42 U.S.C. § 1302d *et seq.*, Defendants Excellus Lifetime Benefit, Lifetime Care, Lifetime Health Medical, MedAmerica, and Univera had a duty to implement reasonable safeguards to protect Plaintiffs' and Class Members' Personal Information.

210. Pursuant to the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801, Defendants had a duty to protect the security and confidentiality of Plaintiffs' and Class Members' Personal Information.

211. Pursuant to state laws in the following states, Lifetime, Excellus, and all Defendants operating in the states set forth below had a duty to those respective states'

Class Members to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs' and Class Members' Personal Information:

a. California: Cal. Civ. Code § 1798.81.5

b. Florida: Fla. Stat. § 501.171(2);

c. Indiana: Ind. Code § 24-4.9-3.5.

212. Defendants breached their duties to Plaintiffs, Statewide Class Members, and Healthcare Provider Class Members under the Federal Trade Commission Act, 15 U.S.C. § 45; HIPAA, 42 U.S.C. § 1302d *et seq.*; and the above-referenced state laws requiring reasonable data security. Defendants breached their duties by failing to provide fair, reasonable, or adequate Information Technology systems and data security practices sufficient to safeguard Plaintiffs' and Class Members' Personal Information.

213. Defendants' failure to comply with applicable laws and regulations constitutes negligence per se.

214. But for Defendants' wrongful and negligent breach of the duties owed to Plaintiffs and Statewide Class Members, and Healthcare Provider Class Members, Plaintiffs and Class Members would not have suffered injury as described herein.

215. The injury and harm suffered by Plaintiffs, Statewide Class Members, and Healthcare Provider Class Members was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that their duties were not being fulfilled, and that Defendants' breach of duty was likely to cause Plaintiffs, Statewide Class Members, and Healthcare Provider Class Members to experience the foreseeable harms associated with the loss and/or exposure of Plaintiffs' and Class Members' Personal Information.

216. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

THIRD CLAIM FOR RELIEF

Breach of Contract and Breach of Implied Covenant of Good Faith and Fair Dealing Brought by Statewide Classes and Healthcare Provider Class Against All Defendants Except BCBSA

217. Plaintiffs incorporate by reference the allegations contained in the preceding paragraphs of this Consolidated Master Complaint.

218. As set forth above in paragraphs 73 through 81, Plaintiffs and those Class Members who purchased individual insurance plans from Excellus and/or the Affiliate Defendants, or who enrolled pursuant to the terms of a group contract with Excellus and/or the Affiliate Defendants, or who entered contracts with Defendants as healthcare providers, entered into binding and enforceable contracts with Excellus and/or the Affiliate Defendants.

219. As set forth above in paragraphs 73 through 81, the contracts between Plaintiffs and Class Members and Excellus and/or the Affiliate Defendants were supported by consideration in many forms, including the payment of premiums, contributions or fees by all Plaintiffs and Class Members (and/or their employers in whole or in part on their behalf) to Excellus and/or the Affiliate Defendants, and other performance under these contracts by Plaintiffs and Class Members, including by providing PII to Excellus and/or the Affiliate Defendants as required by the contracts.

220. To the extent that group contracts with Excellus and/or the Affiliate Defendants in which Plaintiffs and Class Members enrolled are also contracts with an employer, fund or group, Plaintiffs and Class Members are intended beneficiaries of those group contracts, including the provisions incorporating Excellus' and/or The Lifetime Healthcare Companies' privacy policies and otherwise pertaining to the confidentiality of Personal Information provided to Excellus and/or the Affiliate Defendants. Plaintiffs and Class Members sue in the alternative for breach of contract as third-party beneficiaries.

221. With respect to contracts between employers and Excellus and/or the Affiliate Defendants, the applicable contract is not the ERISA plan instrument described in 29 U.S.C. § 1102(a)(1).

222. All contracts between Excellus and the Affiliate Defendants and Plaintiffs and Class Members (and/or their employers or other groups) were entered into prior to disclosure of the Excellus data breach.

223. Plaintiffs and Class Members (and/or their employers or other groups) performed pursuant to these contracts, including by paying premiums, contributions or fees to Excellus and/or the Affiliate Defendants, and by providing Excellus and/or the Affiliate Defendants with PII and/or PHI as required by these contracts. Plaintiffs and Class Members (and/or their employers or other groups) fully performed their obligations under their contracts with Excellus and/or the Affiliate Defendants and satisfied all conditions, covenants, obligations, and promises of these agreements.

224. As set forth above in paragraphs 73 through 81, all Plaintiffs and Class Members who purchased individual policies from Excellus and/or the Affiliate Defendants entered into contracts with Excellus and/or the Affiliate Defendants that incorporated,

either by express provision or attachment, or incorporation by reference, the relevant Defendant's then-current privacy policy pertaining to personal and health-related information governing the privacy policies of the Lifetime Healthcare Companies.

225. As set forth in paragraphs 73 through 81 above, all Plaintiffs and Class Members who enrolled in group plans from Excellus and/or the Affiliate Defendants entered into contracts with Excellus and/or the Affiliate Defendants that, upon enrollment incorporated, either by express provision or attachment, or incorporation by reference, The Lifetime Healthcare Companies' then-current privacy policies pertaining to personal and health-related information. The group contracts for which Plaintiffs and Class Members were beneficiaries likewise incorporated these policies and notices.

226. As set forth herein, all Plaintiffs and Healthcare Provider Class Members who entered into contracts with Excellus and/or the Affiliate Defendants that, upon agreement, incorporated, either by express provision or attachment, or incorporation by reference, The Lifetime Healthcare Companies' then-current privacy policies pertaining to Personal Information.

227. These contracts were subject to implied covenants of good faith and fair dealing that all parties would act in good faith and with reasonable efforts to perform their contractual obligations (both explicit and fairly implied) and not to impair the rights of the other parties to receive their rights, benefits, and reasonable expectations under the contracts. These included the covenants that Excellus and/or the Affiliate Defendants would act fairly, reasonably, and in good faith in carrying out their contractual obligations to protect the confidentiality of Plaintiffs' and Class Members' Personal Information and

to comply with industry standards and best practices, as well as federal and state law and applicable regulations for the security of this information.

228. "Special relationships" exist between Excellus and/or the Affiliate Defendants and Plaintiffs and Class Members. Excellus and/or the Affiliate Defendants each entered into a "special relationship" with those Plaintiffs and Class Members who purchased insurance plans from them and/or enrolled in health services plans with them and who entrusted their confidential Personal Information to Excellus and/or the Affiliate Defendants.

229. Excellus and/or the Affiliate Defendants materially breached the terms of their respective contracts with Plaintiffs and Class Members, and the contract terms intended to benefit Plaintiffs and Class Members, by violating the commitment to maintain the confidentiality and security of Personal Information compiled by Defendants and stored in the Excellus Networks. Excellus and the Affiliate Defendants further materially breached the terms of their contracts by failing to comply with their policies and applicable laws, regulations, industry standards, and best practices for data security and protecting the confidentiality of Personal Information.

230. Even if Defendants are held not to have breached any express promise in these contracts, Excellus and/or the Affiliate Defendants breached the covenant of good faith and fair dealing by failing to take adequate measures to protect the confidentiality of Plaintiffs' and Class Members' Personal Information. Excellus and/or the Affiliate Defendants unreasonably interfered with the contract benefits owed to Plaintiffs and Class Members by, *inter alia*: failing to implement reasonable and adequate security measures consistent with industry standards and best practices to protect and limit access to the

Personal Information contained in the Excellus Networks; permitting unrestricted access to the Personal Information in the database; failing to implement and/or follow reasonable security measures to timely detect nefarious activity in the Excellus Networks, and failing to implement reasonable auditing procedures to detect and halt the unauthorized extraction of Personal Information from the database.

231. As a result of the above-described breaches of contract, Plaintiffs and Class Members did not receive the full benefit of their respective bargains with Excellus and/or the Affiliate Defendants, and instead received health insurance and/or health care services that were less valuable than described in their contracts. Plaintiffs and Class Members were therefore damaged in an amount at least equal to the difference in value between that which was promised and the partial, deficient and/or defective performance of Excellus and/or the Affiliate Defendants.

232. Plaintiffs and Class Members performed all conditions, covenants, obligations, and promises owed to Excellus and/or the Affiliate Defendants, including paying Excellus and/or the Affiliate Defendants premiums for their insurance and health benefits and providing Excellus and/or the Affiliate Defendants the confidential Personal Information required by their contracts.

233. In addition, as a result of the breach of contract by Excellus and/or the Affiliate Defendants, Plaintiffs and Class Members have suffered actual damages resulting from the theft of their Personal Information and remain at imminent risk of suffering additional damages in the future.

234. Plaintiffs and Class Members have also suffered actual damages resulting from their attempts to ameliorate the effect of the breach of contract, including but not

limited to purchasing credit monitoring and/or taking other steps to protect themselves from the loss of their Personal Information.

235. Accordingly, Plaintiffs and Statewide Class Members and Healthcare Provider Class Members have been injured as a result of the breach of contract by Excellus and/or the Affiliate Defendants and are entitled to damages and/or restitution in an amount to be proven at trial.

236. As a result of the breach of covenant of good faith and fair dealing by Excellus and/or the Affiliate Defendants, Plaintiffs and Class Members did not receive the full benefit of their respective bargains, and instead received health insurance and/or health care services and related services that were less valuable than what they paid for and less valuable than their reasonable expectations under the contracts. Plaintiffs and Class Members were damaged in an amount at least equal to the difference in value between that which they reasonably expected under the contracts and Excellus and/or the Affiliate Defendants' partial, deficient, and/or defective performance.

237. In addition, as a result of the breach of the covenant of good faith and fair dealing described herein, Plaintiffs and Class Members have suffered actual damages resulting from the theft of their Personal Information and remain at imminent risk of suffering additional damages in the future.

238. As a further result of the breach of the covenant of good faith and fair dealing, Plaintiffs and Class Members have suffered actual damages resulting from their attempt to ameliorate the effect of the Excellus data breach, including but not limited to purchasing credit monitoring services or taking other steps to protect themselves from the imminent loss of their Personal Information.

239. Accordingly, Plaintiffs and Class Members have been injured as a result of breaches of the covenant of good faith and fair dealing by Excellus and/or the Affiliate Defendants, and are entitled to damages and/or restitution in an amount to be proven at trial.

FOURTH CLAIM FOR RELIEF

Unjust Enrichment
Brought by Statewide Classes Against All Defendants Except BCBSA

240. Plaintiffs incorporate by reference the allegations contained in the preceding paragraphs of this Consolidated Master Complaint.

241. In the alternative to the claims alleged above, Plaintiffs allege that they have no adequate remedy at law and bring this unjust enrichment claim on behalf of the Statewide Class Members.

242. Plaintiffs and Class Members conferred a monetary benefit on Defendants in the form of premiums paid for the purchase of health insurance and health benefits services. Plaintiffs and Class Members also provided their PII and PHI to Defendants.

243. Defendants appreciated or had knowledge of the benefits conferred by Plaintiffs and Class Members.

244. The premiums for health insurance and health benefits services that Plaintiffs and Class Members paid, directly or indirectly, to Defendants should have been used by Defendants, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

245. As a result of Defendants' conduct described herein, Plaintiffs and Class Members suffered actual damages in an amount equal to the difference in value between health insurance and health benefit services associated with the reasonable data privacy

and security practices and procedures that Plaintiffs and Class Members paid for, and the inadequate health insurance and health benefits services without reasonable data privacy and security practices and procedures that they received.

246. Under principles of equity and good conscience, Defendants should not be permitted to retain money belonging to Plaintiffs and Class Members because Defendants failed to use that money to implement the reasonable data privacy and security practices and procedures that Plaintiffs and Class Members paid for and that were otherwise mandated by HIPAA regulations, federal and state law, and industry standards and best practices.

247. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class Members all unlawful or inequitable proceeds received by Defendants.

248. A constructive trust should be imposed upon all unlawful or inequitable sums received by Defendants traceable to Plaintiffs and Class Members.

FIFTH CLAIM FOR RELIEF

Violation of State Consumer Protection Laws
Brought by Statewide Classes as Set Forth Below

California
California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 *et seq*.
(Brought by California Class Against Defendants)

249. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Consolidated Master Complaint.

250. Defendants have violated California Business and Professions Code §17200 *et seq*. ("UCL") by engaging in unlawful, unfair, or fraudulent business acts and practices and unfair, deceptive, untrue, or misleading advertising that constitute acts of "unfair

competition" as defined in the UCL with respect to the insurance services, health benefit services, and other services provided to the California Class, including but not limited to the following:

a. Defendants engaged in deceptive acts and practices with regard to the insurance services, health benefits services, and other services provided to the California Class by representing and advertising that they would maintain adequate data privacy and security practices and procedures to safeguard California Class Members' PII and PHI from unauthorized disclosure, release, data breaches, and cyber attack; representing and advertising that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of California Class Members' PII and PHI; and omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for California Class Members' PII and PHI.

b. Defendants engaged in deceptive acts and practices with regard to insurance services, health benefits services, and other services provided to the California Class by omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for California Class Members' PII and PHI. At the time that California Class members were enrolling in insurance, health benefits, and other services, Defendants failed to disclose to California Class Members that the Defendants' data security systems failed to meet legal and industry standards for the protection of their PII and PHI. Plaintiffs would not have enrolled in Defendants' insurance services, health benefits services, and other services if they had known about Defendants' substandard data security practices.

c. Defendants engaged in unfair acts and practices with regard to the insurance services, health benefits services, and other services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiffs' and California Class Members' PII and PHI with knowledge that the information would not be adequately protected; and by storing Plaintiffs' and California Class Members' PII and PHI in an insecure electronic environment. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and California Class Members. Defendants' acts and practices were also contrary to legislatively declared and public policies that seek to protect consumer data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws like the Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d *et seq*.), the Gramm-Leach-Bliley Act (15 U.S.C. § 6801), California's Confidentiality of Medical Information Act (Cal. Civil Code §56 *et seq*.), California's unfair insurance practices statutes (Cal. Ins. Code §790 *et seq*.), California's Insurance Information and Privacy Protection Act (Cal. Ins. Code §791 *et seq*.), and California's data breach statute (Cal. Civ. Code § 1798.81.5). The harm these acts and practices caused to Plaintiffs and the California Class Members outweighed their utility, if any.

d. Defendants engaged in unfair acts and practices with respect to the sale of insurance, health benefits, and other services by failing to disclose the Excellus data breach to California Class Members in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82. These unfair acts and

practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and California Class Members. The harm these practices caused to Plaintiffs and the California Class Members outweighed their utility, if any.

e. Defendants engaged in unfair acts and practices with respect to the provision of insurance, health benefits, and other services by failing to take proper action following the Excellus data breach to enact adequate privacy and security measures and protect California Class Members' PII and PHI from further unauthorized disclosure, release, data breaches, and cyber attack. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and California Class Members. The harm these acts and practices caused to Plaintiffs and the California Class Members outweighed their utility, if any.

f. Defendants engaged in unlawful business practices by violating the privacy and security requirements of HIPAA (42 U.S.C. § 1302d *et seq.*).

g. Defendants engaged in unlawful business practices by violating California's unfair insurance practices statutes (Cal. Ins. Code §790 *et seq.*), and California's Insurance Information and Privacy Protection Act (Cal. Ins. Code §791 *et seq.*, "CIIPA") with respect to California Class Members with health insurance. With respect to CIIPA, Defendants are "insurance institutions" that "collected or received" "personal or privileged information" pertaining to members of the California Class "in connection with an insurance transaction" and, as a result of

the Excellus data breach, failed to maintain the confidentiality and privacy of and disclosed this personal information without authorization, thereby violating CIIPA;

h. Defendants engaged in unlawful business practices by violating Cal. Civ. Code § 1798.82.

251. As a direct and proximate result of Defendants' acts of unfair and unlawful practices and acts, the Plaintiffs were injured and lost money or property, including but not limited to the premiums and/or price received by Defendants for insurance, health benefits, or other services, the loss of their legally protected interest in the confidentiality and privacy of their PII and PHI, and additional losses described above.

252. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard California Class Members' PII and PHI and that the risk of a data breach or cyber attack was highly likely. Defendants' actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the California Class.

253. California Class Members seek relief under California Business and Professions Code § 17200, *et seq.*, including, but not limited to, restitution to Plaintiffs and Class Members of money or property that the Defendants may have acquired by means of Defendants' deceptive, unlawful, and unfair business practices, restitutionary disgorgement of all profits accruing to Defendants because of their unlawful and unfair business practices, declaratory relief, attorney's fees and costs (pursuant to Cal. Code Civil Pro. §1021.5), and injunctive or other equitable relief.

New Jersey
New Jersey Consumer Fraud Act, N.J. Stat. Ann. § 56:8-1 *et seq.*
(Brought by New Jersey Class Against Defendants)

254. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Consolidated Master Complaint.

255. Plaintiffs bring this claim against Defendants on behalf of the New Jersey Class.

256. Defendants sell "merchandise," as meant by N.J. Stat. Ann. § 56:8-1(c), by offering health insurance, health benefits, and other services to the public.

257. Defendants engaged in unconscionable and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of health insurance, health benefits services, and other services in violation of N.J. Stat. Ann. § 56:8-2, including but not limited to the following:

a. Defendants misrepresented material facts, pertaining to the sale of insurance, health benefits, and other services, to the New Jersey Class by representing that they would maintain adequate data privacy and security practices and procedures to safeguard New Jersey Class Members' PII and PHI from unauthorized disclosure, release, data breaches, and cyber attack;

b. Defendants misrepresented material facts, pertaining to the sale of insurance, health benefits, and other services, to the New Jersey Class by representing that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of New Jersey Class Members' PII and PHI;

c. Defendants knowingly omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for New Jersey Class Members' PII and PHI with the intent that others rely on the omission, suppression, and concealment;

d. Defendants engaged in unconscionable and deceptive acts and practices with respect to the sale of insurance, health benefits, and other services by failing to maintain the privacy and security of New Jersey Class Members' PII and PHI, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Excellus data breach. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d, *et seq.*), the Gramm-Leach-Bliley Act (15 U.S.C. § 6801), the New Jersey Insurance Information Practices Act (N.J. Stat. § 17:23A-1, *et seq.*); and the New Jersey Insurance Trade Practices Act (N.J. Stat. §§ 17:29B-4(1) and (2));

e. Defendants engaged in unconscionable and deceptive acts and practices with respect to the sale of insurance, health benefits, and other services by failing to disclose the Excellus data breach to New Jersey Class Members in a timely and accurate manner, in violation of N.J. Stat. Ann. § 56:8-163(a);

f. Defendants engaged in unconscionable and deceptive acts and practices with respect to the sale of insurance, health benefits, and other services by failing to take proper action following the Excellus data breach to enact adequate privacy and security measures and protect New Jersey Class Members' PII and PHI from further unauthorized disclosure, release, data breaches, and theft.

258. The above unlawful and deceptive acts and practices and acts by Defendants were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

259. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard New Jersey Class Members' PII and PHI and that risk of a data breach or cyber attack was highly likely. Defendants' actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the New Jersey Class.

260. As a direct and proximate result of Defendants' unconscionable or deceptive acts and practices, New Jersey Class Members suffered an ascertainable loss in money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their PII and PHI.

261. New Jersey Class Members seek relief under N.J. Stat. Ann. § 56:8-19, including, but not limited to, injunctive relief, other equitable relief, actual damages, treble damages, and attorneys' fees and costs.

New York
New York General Business Law, N.Y. Gen. Bus. Law § 349 *et seq.*
(Brought by New York Class Against Defendants)

262. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Consolidated Master Complaint.

263. New York General Business Law § 349 ("NYGBL § 349") prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of New York.

264. As large insurers and health benefits providers, Defendants conducted business, trade or commerce in New York State.

265. In the conduct of their business, trade, and commerce, and in furnishing services in New York State, Defendants' actions were directed at consumers.

266. In the conduct of their business, trade, and commerce, and in furnishing services in New York State, Defendants collected and stored highly personal and private information, including PII and PHI belonging to Plaintiffs and members of the New York Class.

267. In the conduct of their business, trade, and commerce, and in furnishing services in New York State, Defendants engaged in deceptive, unfair, and unlawful trade acts or practices, in violation of N.Y. Gen. Bus. Law § 349(a), including but not limited to the following:

a. Defendants misrepresented and fraudulently advertised material facts, pertaining to the sale and/or furnishing of insurance, health benefits, and other services, to the New York Class by representing and advertising that they would maintain adequate data privacy and security practices and procedures to safeguard New York Class Members' PII and PHI from unauthorized disclosure, release, data breaches, and cyber attack;

b. Defendants misrepresented material facts, pertaining to the sale and/or furnishing of insurance, health benefits, and other services, to the New York

Class by representing and advertising that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of New York Class Members' PII and PHI;

c. Defendants omitted, suppressed, and concealed the material fact of the inadequacy of their privacy and security protections for New York Class Members' PII and PHI;

d. Defendants engaged in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the Excellus data breach to enact adequate privacy and security measures and protect New York Class Members' PII and PHI from further unauthorized disclosure, release, data breaches, and theft.

268. Defendants systematically engaged in these deceptive, misleading, and unlawful acts and practices, to the detriment of Plaintiffs and members of the New York Class.

269. Defendants willfully engaged in such acts and practices, and knew that they violated N.Y. Gen. Bus. Law § 349 or showed reckless disregard for whether they violated N.Y. Gen. Bus. Law § 349.

270. As a direct and proximate result of all Defendants' except BCBSA deceptive trade practices, New York Class Members suffered injury and/or damages, including the loss of their legally protected interest in the confidentiality and privacy of their PII and PHI, and the loss of the benefit of their respective bargains.

271. As a direct and proximate result of defendants' BCBSA's deceptive trade practices, Federal Employee New York Class Members suffered injury and/or damages,

including the loss of their legally protected interest in the confidentiality and privacy of their PII and PHI.

272. The above unfair and deceptive practices and acts by Defendants were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

273. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard New York Class Members' PII and PHI and that risk of a data breach or cyber attack was highly likely. Defendants' actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the New York Class.

274. Plaintiffs and New York Class Members seek relief under N.Y. Gen. Bus. Law § 349(h), including, but not limited to, actual damages, treble damages, statutory damages, injunctive relief, and/or attorney's fees and costs.

North Carolina

North Carolina Unfair Trade Practices Act, N.C. Gen. Stat. Ann. § 75-1.1 *et seq.*
(Brought by North Carolina Class Against Defendants)

275. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Consolidated Master Complaint.

276. Plaintiffs bring this claim against Defendants on behalf of the North Carolina Class.

277. Defendants' sale, advertising, and marketing of insurance, health benefits, and other services affected commerce, as meant by N.C. Gen. Stat. § 75-1.1.

278. Defendants engaged in unlawful, unfair, and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of health insurance, health benefits services, and other services in violation of N.C. Gen. Stat. § 75-1.1, including but not limited to the following:

a. Defendants misrepresented material facts, pertaining to the sale of insurance, health benefits services, and other services to the North Carolina Class by representing that they would maintain adequate data privacy and security practices and procedures to safeguard North Carolina Class Members' PII and PHI from unauthorized disclosure, release, data breaches, and cyber attack;

b. Defendants misrepresented material facts, pertaining to the sale of insurance, health benefits services, and other services to the North Carolina Class by representing that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of North Carolina Class Members' PII and PHI;

c. Defendants omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for North Carolina Class Members' PII and PHI;

d. Defendants engaged in unfair, unlawful, and deceptive acts and practices with respect to the sale of insurance, health benefits services, and other services by failing to maintain the privacy and security of North Carolina Class Members' PII and PHI, in violation of duties imposed by, and public policies reflected in, applicable federal and state laws, resulting in the Excellus data breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by

laws including Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d, *et seq*.), the Gramm-Leach-Bliley Act (15 U.S.C. § 6801), and the North Carolina Unfair Trade Practices N.C. Gen. Stat. § 58-63-15(1) and (2));

e. Defendants engaged in unfair, unlawful, and deceptive acts and practices with respect to the sale of insurance, health benefits services, and other services by failing to disclose the Excellus data breach to North Carolina Class Members in a timely and accurate manner, in violation of N.C. Gen. Stat. Ann. § 76-65(a);

f. Defendants engaged in unfair, unlawful, and deceptive acts and practices with respect to the sale of insurance, health benefits services, and other services by failing to take proper action following the Excellus data breach to enact adequate privacy and security measures and protect North Carolina Class Members' PII and PHI from further unauthorized disclosure, release, data breaches, and cyber attack.

279. The above unfair, unlawful, and deceptive acts and practices and acts by Defendants were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

280. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard North Carolina Class Members' PII and PHI and that risk of a data breach or cyber attack was highly likely. Defendants' actions in engaging in the above-named unfair, unconscionable, and deceptive acts and practices

were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the North Carolina Class.

281. As a direct and proximate result of Defendants' unfair, unconscionable, and deceptive acts and practices, North Class Members suffered injury and/or damages. North Carolina Class Members seek relief under N.C. Gen. Stat. §§ 75-16 and 75-16.1 including, but not limited to, injunctive relief, actual damages, treble damages, and attorneys' fees and costs.

Pennsylvania

Pennsylvania Unfair Trade Practices, 73 Pa. Stat. Ann. § 201-1 *et seq.*
(Brought by Pennsylvania Class Against Defendants)

282. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Consolidated Master Complaint.

283. Plaintiffs bring this claim against Defendants on behalf of the Pennsylvania Class.

284. The Pennsylvania Class Members purchased insurance, health benefits services, and other services from Defendants in "trade" and "commerce," as meant by 73 Pa. Cons. Stat. § 201-2, for personal, family, and/or household purposes.

285. Defendants engaged in unlawful, unfair, and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the services purchased by the Pennsylvania Class in violation of 73 Pa. Cons. Stat. Ann. § 201-3, including but not limited to the following:

a. Defendants misrepresented material facts pertaining to the sale of insurance, health benefits services, and other services to the Pennsylvania Class by representing that they would maintain adequate data privacy and security practices

and procedures to safeguard Pennsylvania Class Members' PII and PHI from unauthorized disclosure, release, data breaches, and cyber attack in violation of 73 Pa. Cons. Stat. Ann. § 201-3(4)(v), (ix), and (xxi);

b. Defendants misrepresented material facts pertaining to the sale of insurance, health benefits services, and other services to the Pennsylvania Class by representing that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Pennsylvania Class Members' PII and PHI in violation of 73 Pa. Cons. Stat. Ann. § 201-3(4)(v), (ix), and (xxi);

c. Defendants omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Pennsylvania Class Members' PII and PHI in violation of in violation of 73 Pa. Cons. Stat. Ann. § 201-3(4)(v), (ix), and (xxi);

d. Defendants engaged in unfair, unlawful, and deceptive acts and practices with respect to the sale of insurance, health benefits services, and other services by failing to maintain the privacy and security of Pennsylvania Class Members' PII and PHI, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Excellus data breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws including Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d, *et seq*.), the Gramm-Leach-Bliley Act (15 U.S.C. § 6801), the Pennsylvania Quality Healthcare Accountability and Protection statute (40 Pa.

Cons. Stat. Ann. § 991.2131); and the Pennsylvania Unfair Insurance Practices Act (40 Pa. Cons. Stat. Ann. § 1171.1(a)(1)(i) and (a)(2));

e. Defendants engaged in unlawful, unfair, and deceptive acts and practices with respect to the sale of insurance, health benefits services, and other services by failing to disclose the Excellus data breach to Pennsylvania Class Members in a timely and accurate manner, in violation of 73 Pa. Stat. § 2303(a);

f. Defendants engaged in unlawful, unfair, and deceptive acts and practices with respect to the sale of insurance, health benefits services, and other services by failing to take proper action following the Excellus data breach to enact adequate privacy and security measures and protect Pennsylvania Class Members' PII and PHI from further unauthorized disclosure, release, data breaches, and cyber attack.

286. The above unlawful, unfair, and deceptive acts and practices by Defendants were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

287. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard Pennsylvania Class Members' PII and PHI and that risk of a data breach or cyber attack was highly likely. Defendants' actions in engaging in the above-named deceptive acts and practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Pennsylvania Class.

288. As a direct and proximate result of Defendants' deceptive acts and practices, the Pennsylvania Class Members suffered an ascertainable loss of money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their PII and PHI.

289. Pennsylvania Class Members seek relief under 73 Pa. Cons. Stat. § 201-9.2, including, but not limited to, injunctive relief, actual damages or $100 per Class Member, whichever is greater, treble damages, and attorneys' fees and costs.

PRAYER FOR RELIEF

Plaintiffs, on behalf of themselves and all Class Members, request the Court to enter judgment against Defendants as follows:

A. An order certifying this action as a class action under Federal Rule of Civil Procedure 23, defining the Classes as requested herein, appointing the undersigned interim co-lead counsel as Class counsel, and finding that Plaintiffs are proper representatives of the Classes requested herein.

B. Injunctive relief, and other equitable relief as is necessary to protect the interests of the Class, including an order (i) prohibiting Defendants from engaging in the unlawful and wrongful acts described herein; (ii) requiring Defendants to protect all data collected or received in the regular course of business in accordance with HIPAA regulations, the Gramm-Leach Bliley Act, other federal, state and local laws, and industry standards and best practices; (iii) requiring Defendants to design, maintain, and test its Information Technology systems to ensure that Personal Information in its possession is adequately secured and protected; (iv) requiring Defendants to disclose future data breaches in a timely and accurate manner; (v) requiring Defendants to engage third-party

security auditors as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or system deficiencies detected by these audits; (vi) requiring Defendants to audit, test, and train staff security personnel to run automated security monitoring, aggregating, filtering and reporting on log information in a unified manner; (vii) requiring Defendants' employees to change their passwords on a timely and regular basis, consistent with best practices; (viii) requiring Defendants to encrypt all PII and PHI stored in its databases; (ix) requiring Excellus to segment data by, *inter alia*, creating firewalls and access controls so that if one area of the Excellus network is compromised, hackers cannot gain access to other portions of the Excellus Network; (x) requiring Defendants to purge, delete, and destroy in a reasonably secure and timely manner Personal Information no longer necessary for the provision of Defendants' services; (xi) requiring Defendants to provide lifetime credit monitoring and identity theft repair services to Class Members; (xii) establishing a fund that would cover the costs to Class Members associated with freezing and unfreezing their credit with the three major credit reporting bureaus; (xiii) requiring Defendants to provide a service to assist elderly and infirm Class Members to monitor and protect themselves from identity theft and fraud; and (xiv) requiring Defendants to educate all Class Members regarding the threats they face as a result of the loss of their PII and PHI, and to provide Class Members with steps they may take to protect themselves, as well as any other relief that the Court deems appropriate under the facts of this case.

C. Plaintiffs further move for injunctive relief, and other equitable relief as is necessary to protect the interests unique to the minor and/or dependent Class Members,

including an order requiring Defendants to provide each minor and/or dependent Class Member with training regarding proper credit monitoring and identity protection, as well as a credit monitoring and identity protection service that is specially tailored to serve minors, as well as any other relief that the Court deems appropriate under the facts of this case.

D. In addition, Plaintiffs request actual damages, punitive damages, statutory damages, exemplary damages, equitable relief, restitution, disgorgement of profits, attorneys' fees, statutory costs, and such further relief as is just and proper. Plaintiffs seek attorneys' fees under applicable state and federal law.

JURY DEMAND

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury of any and all issues in this action so triable of right.

Dated: March 25, 2019

/s/ Hadley L. Matarazzo
Hadley L. Matarazzo (NY Bar. No. 437785)
hmatarazzo@faraci.com
Kathryn Lee Bruns (NY Bar No. 2874063)
kbruns@faraci.com
FARACI LANGE, LLP
28 E. Main Street, Suite 1100
Rochester, New York 14614
Tel: (585) 325-5150
Fax: (585) 325-3285

/s/ Robin L. Greenwald
Robin L. Greenwald (Admitted *pro hac vice*)
rgreenwald@weitzlux.com
James J. Bilsborrow (NY Bar No. 4702064)
jbilsborrow@weitzlux.com
WEITZ & LUXENBERG, P.C.
700 Broadway
New York, New York 10003
Tel: (212) 558-5500

Fax: (646) 293-7937

Plaintiffs' Co-Lead Interim Class Counsel

/s/ Eric H. Gibbs
Eric H. Gibbs (Admitted *pro hac vice*)
ehg@classlawgroup.com
David M. Berger (Admitted *pro hac vice*)
dmb@classlawgroup.com
GIBBS LAW GROUP LLP
505 14th Street, Suite 1110
Oakland, California 94612
Phone: (510) 350-9700
Fax: (510) 350-9701

/s/ Lynn A. Toops
Lynn A. Toops (Admitted *pro hac vice*)
ltoops@cohenandmalad.com
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
Tel: (317) 636-6481
Fax: (317) 636-2593

Plaintiffs' Executive Committee

EXHIBIT A

165 Court Street
Rochester, New York 14647

A nonprofit independent licensee of the BlueCross BlueShield Association

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION.

PLEASE REVIEW IT CAREFULLY.

THE PRIVACY OF YOUR MEDICAL INFORMATION IS IMPORTANT TO US.

This notice takes effect April 14, 2003.

OUR COMMITMENT TO YOUR PRIVACY

We understand that medical information about you and your health is personal. We are committed to safeguarding your protected health information (PHI).

PHI is any information that can identify you as an individual and your past, present or future physical or mental health condition.

This notice will tell you about the ways in which we may use and disclose medical information about you. We also describe your rights and certain obligations we have regarding the use and disclosure of medical information. The law requires us to:

- make sure that PHI that identifies you is kept private;
- give you this notice of our legal duties and privacy practices with respect to PHI about you; and
- follow the terms of the notice that is currently in effect.

OUR LEGAL DUTY

We **(Excellus BlueCross BlueShield)** are required by applicable federal and state laws to maintain the privacy of your PHI. We are also required to give you this notice about our privacy practices, our legal duties, and your rights concerning PHI. We must follow the privacy practices that are described in this notice while it is in effect, including notification should there be a breach of your unsecured PHI.

We reserve the right to change our privacy practices and the terms of this notice at any time, provided that applicable law permits such changes. We reserve the right to make the changes in our privacy practices and the new terms of our notice effective for all PHI that we maintain, including medical information we created or received before we made the changes. Before we make a significant change in our privacy practices, we will change this notice and send the new notice to our health plan subscribers at the time of the change.

You may request a copy of our notice at any time. For more information about our privacy practices, or for additional copies of this notice, please contact us using the contact information at the end of this notice.

Uses and Disclosures of Nonpublic Personal Information

Nonpublic Personal Information is information you give us on your enrollment form, claim forms, premium payments etc. For example: names, member identification number, social security number, addresses, type of health care benefits, payment amounts, etc.

We will not give out your nonpublic personal information to anyone unless we are permitted to do so by law or have received a signed authorization form from the member. You may revoke this authorization in writing by completing an authorization cancellation form at any time. This revocation will not affect any actions we took in reliance on your authorization before your authorization cancellation form was processed.

Uses and Disclosures of Medical Information

The following categories describe different purposes for which we use and disclose PHI. For each category of uses or disclosures we will explain what we mean and try to give some examples. Not every use or disclosure in a category will be listed. However, all of the ways we are permitted to use and disclose information will fall within one of the categories. If we need to use or disclose your PHI in any other way, we will obtain your signed authorization before our use or disclosure. You may revoke this authorization in writing by completing an authorization cancellation form at any time. This revocation will not affect any actions we took in reliance on your authorization before your authorization cancellation form was processed.

Treatment: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may disclose PHI to doctors or hospitals involved in your care. For example, we may disclose your medications to an emergency room physician so that he/she can avoid dangerous drug interactions. This allows providers to manage, coordinate and administer treatment.

Payment: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may use and disclose PHI to collect premiums, to determine our responsibility to pay claims or to notify members and providers of our claim determinations. We may disclose PHI to providers to assist them in their billing and collection efforts. We may also disclose PHI to other insurance companies to coordinate the reimbursement of health insurance benefits. For example, we may disclose PHI to an automobile no-fault insurance company to determine responsibility for claim payment. Also, if you have health insurance through another insurance company, we may disclose PHI to that other health insurance company in order to determine which company holds the responsibility for your claims.

Healthcare Operations: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may use and disclose PHI for purposes of performing our healthcare operations. Our healthcare operations include using PHI to determine premiums, to conduct quality assessment and improvement activities, to engage in care coordination or case management, to determine eligibility for benefits. For example, we may use or disclose PHI when working with accreditation agencies that monitor and evaluate the quality of our benefit programs.

To You: We must disclose your PHI to you, as described in the Individual Rights section of this notice, below. We may also use and disclose PHI to tell you about recommended possible treatment options or alternatives or to tell you about health related benefits or services that may be of interest to you.

To Family and Friends: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. If you agree or, if you are unable to agree when the situation, (such as medical emergency or disaster relief), indicates that disclosure would be in your best interest, we may disclose PHI to a family member, friend or other person. In an emergency situation, we will only disclose the minimum amount necessary.

To Our Business Associates: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. A business associate is defined as someone that assists us in managing our business. For example, a professional that reviews the quality of our products and services. We may disclose PHI to another company that helps us manage our business. For example, we may disclose PHI to a company that performs case reviews to ensure our members receive quality care. These business associates are required to sign a confidentiality agreement with us that limits their use or disclosure of the PHI they receive.

To Plan Sponsors: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. A plan sponsor is defined as the employer or employee organization that establishes and maintains the employee's benefit plan. If you are enrolled in a group health plan, we may disclose PHI to the plan sponsor to permit the plan sponsor to perform plan administrative functions. For example, the cost analysis of the benefit program. Before PHI is disclosed to your plan sponsor, we will receive certification from the plan sponsor that appropriate amendments have been made to group health plan document(s) and the plan sponsor agrees to limit their use or disclosure of this information to plan administration functions only.

Research: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may use or disclose PHI for research purposes in limited circumstances. For example, a research project may involve comparing the health and recovery of all members who received one medication to those who received another medication for the same condition. All research projects are required to obtain special approval.

Coroners, Medical Examiners and Funeral Directors: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may release PHI to a coroner or medical examiner, to identify a deceased person or determine the cause of death. We may also release PHI about deceased members to funeral directors in order for the funeral directors to carry out their duties.

Organ Donation: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. If you are an organ donor, we may release PHI to organizations that handle organ procurement or organ, eye or tissue transplantation or to an organ donation bank, to facilitate organ or tissue donation and transplantation. This may include a living donor as well as a deceased donor.

Public Health and Safety: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may disclose PHI to the extent necessary to avert a serious and imminent threat to your health or safety, or the health or safety of others. We may disclose PHI to a government agency authorized to oversee the healthcare system or government programs or its contractors, and to public health authorities for public health purposes.

Victims of Abuse, Neglect or Domestic Violence: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may disclose PHI to appropriate authorities if we reasonably believe that you are a possible victim of abuse, neglect, domestic violence or other crimes.

Required by Law: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may use or disclose PHI when we are required to do so by law. For example, we must disclose PHI to the U.S. Department of Health and Human Services upon request to determine whether we are in compliance with federal privacy laws.

Process and Proceedings: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may disclose PHI in response to a court or administrative order, subpoena, discovery request, or other lawful process. Under limited circumstances, such as a court order, warrant, or grand jury subpoena, we may disclose PHI to law enforcement officials.

Law Enforcement: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may disclose PHI to a law enforcement official investigating a suspect, fugitive, material witness, crime victim or missing person. We may disclose PHI of an inmate or other person in lawful custody of a law enforcement official or correctional institution under certain circumstances.

Military and National Security: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may disclose to the military, PHI of Armed Forces personnel under certain circumstances. We may disclose to authorized federal officials medical information required for lawful intelligence, counterintelligence, and other national security activities.

Marketing and Fundraising: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. To the extent we use PHI for marketing or fundraising purposes, you will be contacted by us and have the right to opt out of receiving these communications from us and our use of your information for such purposes.

Genetic Nondiscrimination Act (GINA): We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We will not disclose your PHI containing genetic information for underwriting purposes. GINA expressly prohibits the use or disclosure of genetic information for these purposes.

Breach of Unsecured Information: We will notify you should there be a breach of unsecured information. We are required to notify you if there is any acquisition, access, use, or disclosure of your unsecured PHI that compromises the security or privacy of your PHI.

Psychotherapy Information: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. Should it be applicable that your psychotherapy notes be included in an appropriate use or disclosure of information, in most instances, we are required to obtain your authorization for the release of this information.

Individual Rights

Access: You have the right to inspect and/or copy your PHI, with limited exceptions such as information a licensed health care professional, exercising professional judgment, determines that providing access is reasonably likely to endanger the life, physical safety or cause someone substantial harm. You may contact us using the telephone number on the back of your identification card to obtain a form to be completed and returned to us. If you request copies, we reserve the right to charge you a reasonable fee for each copy, plus postage if the copies are mailed to you.

Disclosure Accounting: You have the right to receive a list of instances in which we or our business associates disclosed your PHI. The list will not include disclosures we made for the purpose of treatment, payment, healthcare operations, disclosures made with your authorization, or certain other disclosures. To request a disclosure accounting you may contact us using the telephone number on the back of your identification card to obtain a form to be completed and returned to us. The request may not exceed a six year time period. We will provide you with the date on which we made the disclosure, the name of the person or entity to whom we disclosed your PHI, a description of the PHI we disclosed and the reason for the disclosure. If you request this list more than once in a 12-month period, we may charge you a reasonable, cost-based fee for responding to these additional requests.

Restriction Requests: You have the right to request that we place additional restrictions on our use or disclosure of your PHI. As permitted by law, we will not honor these requests, as it prohibits us from administering your benefits.

Confidential Communication: You have the right to request that we communicate with you confidentially about your PHI. We will honor a request to communicate to an alternative location if you believe you would be endangered if we do not communicate to the alternative location. We must accommodate your request if it is reasonable and specifies the alternative location. To request a form to be completed and returned to us, you may contact us using the telephone number on the back of your identification card.

Amendment: You have the right to request that we amend your PHI. Your request must be in writing, and it must explain why the information should be amended. We may deny your request if we did not create the information you want amended or if we determine the information is accurate. If we accept your request to amend the information, we will make reasonable efforts to inform others, including people you name, of the amendment and to include the changes in any future disclosures of that information. If we deny your request, we will provide you with a written explanation. You may respond with a statement of disagreement that will be attached to the information you wanted amended. You may contact us using the telephone number on the back of your identification card to obtain a form to be completed and returned to us.

Electronic Notice: If you receive this notice on our web site or by electronic mail (e-mail), you are entitled to receive this notice in written form. Please contact us using the contact information at the end of this notice to obtain this notice in written form.

Safeguards

It is our policy to keep all information about you confidential in all settings. It is so important to us that we take the following steps:

- our employees sign an agreement to follow our Code of Business Conduct;
- our employees are required to complete our privacy training program;
- we have implemented the necessary sanctions for violation of our privacy practices;
- we have a privacy oversight committee that reviews our privacy practices;
- we have a security coordinator to detect and prevent security breaches;
- all computer systems that contain personal information have security protections; and
- we randomly check provider offices on a routine basis to ensure that medical records are kept in secure locations.

Questions and Complaints

If you want more information about our privacy practices or have questions or concerns, please contact us using the contact information at the end of this notice.

If you are concerned that we may have violated your privacy rights, as described above, or you disagree with a decision we made about access to your PHI or in response to a request you made to amend or restrict the use or disclosure of your PHI or to have us confidentially communicate with you at an alternative location, you may complain to us using the contact information at the end of this notice. You also may submit a written complaint to the U.S. Department of Health and Human Services. We will provide you with the address to file your complaint with the U.S. Department of Health and Human Services upon request.

We support your right to protect the privacy of your PHI. We will not retaliate in any way if you choose to file a complaint with us or with the U.S. Department of Health and Human Services.

Privacy Rights or Questions:

Contact Office: Customer Service

Phone: Please call the telephone number on your identification card.

Privacy Complaints:

Contact Office: Privacy Officer
Address: 333 Butternut Dr.
Dewitt, NY 13214-1803

Phone: 1-866-584-2313

E-mail: privacy.officer@excellus.com

EXHIBIT B

Lifetime BENEFIT SOLUTIONS

115 Continuum Drive | Liverpool, NY 13088

315 448-9000 | 315 476-8440 fax

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION.

PLEASE REVIEW IT CAREFULLY.

THE PRIVACY OF YOUR HEALTH INFORMATION IS IMPORTANT TO US.

This notice takes effect April 14, 2003.

OUR COMMITMENT TO YOUR PRIVACY

We understand that health information about you and your health is personal. We are committed to safeguarding your protected health information (PHI).

PHI is any information that can identify you as an individual and your past, present or future physical or mental health condition.

This notice will tell you about the ways in which medical information about you may be used and disclosed. Your rights and certain obligations regarding the use and disclosure of your medical information are also described.

The law requires:

- that PHI that identifies you is kept private;
- this notice of legal duties and privacy practices with respect to PHI about you is provided to you; and
- the terms of the notice that is currently in effect are followed.

OUR LEGAL DUTY

We **(Lifetime Benefit Solutions, Inc.) ("LBS")** are required by applicable federal and state laws to maintain the privacy of your PHI. It is also required that you be provided with this notice about privacy practices, legal duties, and your rights concerning PHI. The privacy practices that are described in this notice must be followed while it is in effect, including notification should there be a breach of your unsecured PHI.

We reserve the right to change our privacy practices and the terms of this notice at any time, provided that applicable law permits such changes. We reserve the right to make the changes in our privacy practices and the new terms of our notice effective for all PHI that we maintain, including medical information we created or received before we made the changes. Before we make a significant change in our privacy practices, we will change this notice and the new notice will be made available to you.

You may request a copy of our notice at any time. For more information about our privacy practices, or for additional copies of this notice, please contact us using the contact information at the end of this notice.

Uses and Disclosures of Nonpublic Personal Information

Nonpublic Personal Information is information you provided on your enrollment form, claim forms, etc. (for example: names, member identification number, social security number, addresses, type of health care benefits, payment amounts, etc.).

Your nonpublic personal information will not be given out to anyone unless permitted by law or a signed authorization form has been received from the member. This authorization may be revoked in writing by completing an authorization cancellation form at any time. This revocation will not affect any actions LBS took in reliance on your authorization before your authorization cancellation form was processed.

Uses and Disclosures of Medical Information

The following categories describe different purposes for which PHI may be used and disclosed. An explanation for each category of uses or disclosures, as well as some examples, is provided. Not every use or disclosure in a category will be listed. However, all of the ways that are permitted to use and disclose information will fall within one of the categories. If your PHI needs to be used or disclosed in any other way, your signed authorization will be obtained before the use or disclosure. You may revoke this authorization in writing by completing an authorization cancellation form at any time. This revocation will not affect any actions LBS took in reliance on your authorization before your authorization cancellation form was processed.

Treatment: PHI will not be disclosed to an unauthorized person not involved in your care or treatment, unless required or permitted by law. PHI may be disclosed to doctors or hospitals involved in your care. This allows providers to manage, coordinate and administer treatment.

Payment: PHI will not be disclosed to an unauthorized person not involved in your care or treatment, unless required or permitted by law. PHI may be used or disclosed to determine coverage and payment responsibility (including billing and collection, claim management and determination, subrogation, review for medical necessity, and utilization review) or to notify members and providers of claim determinations. PHI may be disclosed to other insurance companies to coordinate the reimbursement of health benefits. For example, PHI may be disclosed to an automobile no-fault insurance company to determine responsibility for claim payment. Also, if you have health insurance through another insurance company, PHI may be disclosed to that other health insurance company in order to determine which company holds the responsibility for your claims.

Healthcare Operations: PHI will not be disclosed to an unauthorized person not involved in your care or treatment, unless required or permitted by law. PHI may be used or disclosed for purposes of performing healthcare operations. Healthcare operations include using PHI to conduct quality assessment and improvement activities, to engage in care coordination or case management, to determine eligibility for benefits, to review competence or qualifications of healthcare professionals, underwriting, and other activities related to creating and renewing insurance contracts. Healthcare operations also include disease management programs, medical reviews, auditing, business planning and development, and general administrative activities. For example, PHI may be used or disclosed when working with a case management vendor for medical review purposes.

To You: Your PHI must be disclosed to you, as described in the Individual Rights section of this notice, below. PHI may also be used and disclosed to tell you about recommended possible treatment options or alternatives or to tell you about health-related benefits or services that may be of interest to you.

To Family and Friends: PHI will not be disclosed to an unauthorized person not involved in your care or treatment, unless required or permitted by law. If you agree or, if you are unable to agree when the situation (such as medical emergency or disaster relief) indicates that disclosure would be in your best interest, PHI may be disclosed to a family member, friend or other person. In an emergency situation, only the minimum amount necessary will be disclosed.

To Our Business Associates: PHI will not be disclosed to an unauthorized person not involved in your care or treatment, unless required or permitted by law. A business associate is defined as someone that assists your group health plan sponsor in managing business (for example: a professional that reviews the quality of your group health plan's products and services). LBS is a business associate. PHI may be disclosed to another company that helps manage your health plan's business. For example, PHI may be disclosed to a company that performs case management to ensure members receive quality care. Business associates are required to sign a confidentiality agreement that limits their use or disclosure of the PHI they receive.

To Plan Sponsors: PHI will not be disclosed to an unauthorized person not involved in your care or treatment, unless required or permitted by law. A plan sponsor is defined as the employer or employee organization that establishes and maintains the employee's benefit plan. If you are enrolled in a group health plan, PHI may be disclosed to the plan sponsor to permit the plan sponsor to perform plan administrative functions (for example: the cost analysis of the benefit program). Before PHI is disclosed to your plan sponsor, the plan sponsor will provide certification that appropriate amendments have been made to group health plan document(s) and the plan sponsor agrees to limit their use or disclosure of this information to plan administration functions only.

Research: PHI will not be disclosed to an unauthorized person not involved in your care or treatment, unless required or permitted by law. PHI may be used or disclosed for research purposes in limited circumstances. For example, a research project may involve comparing the health and recovery of all members who received one medication to those who received another, for the same condition. All research projects are required to obtain special approval.

Coroners, Medical Examiners and Funeral Directors: PHI will not be disclosed to an unauthorized person not involved in your care or treatment, unless required or permitted by law. PHI may be released to a coroner or medical examiner, to identify a deceased person or determine the cause of death. PHI may also be released about deceased members to funeral directors in order for the funeral directors to carry out their duties.

Organ Donation: PHI will not be disclosed to an unauthorized person not involved in your care or treatment, unless required or permitted by law. If you are an organ donor, PHI may be released to organizations that handle organ procurement or organ, eye or tissue transplantation or to an organ donation bank, to facilitate organ or tissue donation and transplantation. This may include a living donor as well as a deceased donor.

Public Health and Safety: PHI will not be disclosed to an unauthorized person not involved in your care or treatment, unless required or permitted by law. PHI may be disclosed to the extent necessary to avert a serious and imminent threat to your health or safety, or the health or safety of others. PHI may be disclosed to a government agency authorized to oversee the healthcare system or government programs or its contractors, and to public health authorities for public health purposes.

Victims of Abuse, Neglect or Domestic Violence: PHI may be disclosed to appropriate authorities if it is reasonably believed that you are a possible victim of abuse, neglect, domestic violence or other crimes.

Required by Law: PHI will not be disclosed to an unauthorized person not involved in your care or treatment, unless required or permitted by law. PHI may be used or disclosed

when required to do so by law. For example, PHI must be disclosed to the U.S. Department of Health and Human Services upon request to determine compliance with federal privacy laws.

Process and Proceedings: PHI will not be disclosed to an unauthorized person not involved in your care or treatment, unless required or permitted by law. PHI may be disclosed in response to a court or administrative order, subpoena, discovery request, or other lawful process. Under limited circumstances, such as a court order, warrant, or grand jury subpoena, PHI may be disclosed to law enforcement officials.

Law Enforcement: PHI will not be disclosed to an unauthorized person not involved in your care or treatment, unless required or permitted by law. PHI may be disclosed to a law enforcement official investigating a suspect, fugitive, material witness, crime victim or missing person. PHI may be disclosed of an inmate or other person in lawful custody of a law enforcement official or correctional institution under certain circumstances.

Military and National Security: PHI will not be disclosed to an unauthorized person not involved in your care or treatment, unless required or permitted by law. PHI of Armed Forces personnel may be disclosed to the military under certain circumstances. Medical information required for lawful intelligence, counterintelligence, and other national security activities may be disclosed to authorized federal officials.

Marketing and Fundraising: PHI will not be disclosed for marketing or fundraising purposes without your authorization. To the extent PHI is used for marketing or fundraising purposes, you will be contacted and have the right to opt out of receiving these communications and use of your information for such purposes.

Genetic Nondiscrimination Act (GINA): PHI will not be disclosed containing genetic information for underwriting purposes. GINA expressly prohibits the use or disclosure of genetic information for these purposes.

Breach of Unsecured Information: You will be notified should there be a breach of unsecured information. If there is any acquisition, access, use, or disclosure of your unsecured PHI that compromises the security or privacy of your PHI, you will be notified.

Psychotherapy Information: This information will not be released without authorization. Should it be applicable that your psychotherapy notes be included in an appropriate use or disclosure of information, in most instances, your authorization will be obtained for the release of this information.

Individual Rights

The following information is effective as of 4/14/03:

Access: You have the right to inspect and/or copy your PHI, with limited exceptions such as information a licensed health care professional, exercising professional judgment, determines that providing access is reasonably likely to endanger the life, physical safety or cause someone substantial harm. On or after 4/14/03, you may contact us using the contact information at the end of this notice to obtain a form to be completed and returned. If you request copies, LBS reserves the right to charge you a reasonable fee for each copy, plus postage if the copies are mailed to you.

Disclosure Accounting: You have the right to receive a list of instances in which we disclosed your PHI. The list will not include disclosures made for the purpose of treatment, payment, healthcare operations, disclosures made with your authorization, or certain other disclosures. To request a disclosure accounting, on or after 4/14/03, you may contact us using the contact

information at the end of this notice to obtain a form to be completed and returned. You may request an accounting of disclosures made on or after April 14, 2003 and the request may not exceed a six-year time period. The date on which the disclosure was made, the name of the person or entity to whom your PHI was disclosed, a description of the PHI disclosed and the reason for the disclosure will be provided. If you request this list more than once in a 12-month period, LBS may charge you a reasonable, cost-based fee for responding to these additional requests.

Restriction Requests: You have the right to request that additional restrictions be placed on the use or disclosure of your PHI. As permitted by law, these requests will not be honored, as it prohibits us from administering your benefits.

Confidential Communication: You have the right to request confidential communication about your PHI. Your request to communicate at an alternative location will be honored if you believe you would be endangered if communication does not take place at the alternative location. Your request must be accommodated if it is reasonable and specifies the alternative location. On or after 4/14/03, please contact us using the contact information at the end of this notice to request a form to be completed and returned.

Amendment: You have the right to request that your PHI be amended. Your request must be in writing, and it must explain why the information should be amended. Your request may be denied if we did not create the information you want amended or if it is determined the information is accurate. If your request to amend the information is accepted, reasonable efforts will be made to inform others, including people you name, of the amendment and to include the changes in any future disclosures of that information. If your request is denied, you will be provided with a written explanation. You may respond with a statement of disagreement that will be attached to the information you wanted amended. On or after 4/14/03, you may contact us using the contact information at the end of this notice to obtain a form to be completed and returned to us.

Electronic Notice: If you receive this notice on our website or by electronic mail (e-mail), you are entitled to receive this notice in written form. Please contact us using the contact information at the end of this notice to obtain this notice in written form.

Safeguards

It is our policy to keep all information about you confidential in all settings. It is so important to us that we take the following steps:

- our employees sign an agreement to follow our Code of Business Conduct;
- our employees are required to complete our privacy training program;
- we have implemented the necessary sanctions for violation of our privacy practices;
- we have a privacy oversight committee that reviews our privacy practices;
- we have a security coordinator to detect and prevent security breaches;
- all computer systems that contain personal information have security protections; and

Questions and Complaints

If you want more information about the privacy practices or have questions or concerns, please contact us using the contact information at the end of this notice.

On or after 4/14/03, if you are concerned that your privacy rights may have been violated, as described above, or you disagree with a decision made about access to your PHI or in response to a request you made to amend or restrict the use or disclosure of your PHI or to have us confidentially communicate with you at an alternative location, you may complain to us using the contact information at the end of this notice. You also may submit a written complaint to the U.S. Department of Health and Human Services. We will provide you with the address to file your complaint with the U.S. Department of Health and Human Services upon request.

We support your right to protect the privacy of your PHI. We will not retaliate in any way if you choose to file a complaint with us or with the U.S. Department of Health and Human Services.

Privacy Rights or Questions:

Contact Office: Customer Service

Phone: Please call the telephone number on the back of your benefit identification card.

Privacy Complaints:

Contact Office: Privacy Officer
Address: 115 Continuum Drive
Liverpool, NY 13088

Phone: 1-315-448-9260

E-mail: privacyofficer@lifetimebenefitsolutions.com

EXHIBIT C

Effective Date: April 13, 2003
Revised Date: September 1, 2013

LIFETIME CARE
Home Health and Hospice

HomeCare PLUS

LIFETIME PHARMACY, LLC

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

If you have any questions about this notice, please contact (585) 214-1403

A. OUR COMMITMENT TO YOUR PRIVACY:

We understand that medical information about you and your health is personal. We are committed to protecting medical information about you. We create a record of the care and services you receive from our agency. We need this record to provide you with quality care and to comply with certain legal requirements. This notice applies to all of the records of your care generated by this facility.

This notice will tell you about the ways in which we may use and disclose medical information about you. We also describe your rights and certain obligations we have regarding the use and disclosure of medical information. We are required by law to:

- make sure that medical information that identifies you is kept private;
- give you this notice of our legal duties and privacy practices with respect to medical information about you; and
- follow the terms of the notice that is currently in effect.

B. HOW WE MAY USE AND DISCLOSE MEDICAL INFORMATION ABOUT YOU.

The following categories describe different ways that we use and disclose medical information.

For each category of uses or disclosures we will explain what we mean and try to give some examples. Not every use or disclosure in a category will be listed. However, all of the ways we are permitted to use and disclose information will fall within one of the categories.

1. **For Treatment**. We may use medical information about you to provide you with medical treatment or services. For example, if you have a condition that requires hospitalization, your medical record or portions of your medical record may be forwarded to hospital staff. We might disclose your medial information to a pharmacy when we obtain a prescription for you. Many of the people who work for our facility may use or disclose your medical information to others in order to treat you or assist others in your treatment. We may also disclose medical information about you to people who may be involved in your medical care such as family members.
2. **For Payment**. We may use and disclose medical information about you in order to bill and collect payment for the services you receive from this agency. For example, we may need to give your health plan information about the services you received from Lifetime Care so your health plan will pay us or reimburse you for the care. We may also tell your health plan about services you are going to receive to obtain prior approval or to determine whether your plan will cover the treatment. We may use or disclose your medical information to obtain payment from third parties that may be responsible for such

costs, such as family members. We may also disclose information about you to other health care providers or entities to assist in their billing and collection efforts. If you have paid in full for a particular treatment, you can request that we do not provide information regarding the treatment to your health plan.

3. **For Health Care Operations**. We may use and disclose medical information about you to operate our business. These uses and disclosures are necessary to run the agency and make sure that all of our patients receive quality care. For example, we may use medical information to review our treatment and services and to evaluate the performance of our staff in caring for you. We may also disclose information to doctors, nurses, and students for review and learning purposes. We may disclose your medical information to other health care providers and entities to assist in their health care operations.
4. **Individuals Involved in Your Care or Payment for Your Care**. Unless you object, we may release medical information about you to a friend or family member who is involved in your medical care. We may also give information to someone who helps pay for your care. In addition, we may disclose medical information about you to an entity assisting in a disaster relief effort so that your family can be notified about your condition, status and location.
5. **Appointment Reminders**. We may use and disclose medical information to contact you about your scheduled services.
6. **Treatment Alternatives & Health-Related Benefits and Services**. We may use and disclose medical information to tell you about or recommend possible treatment options or alternatives or to tell you about health-related benefits or services that may be of interest to you.
7. **Research**. Under certain circumstances, we may use and disclose medical information about you for research purposes. For example, a research project may involve comparing the health and recovery of all patients who received one medication to those who received another, for the same condition. All research projects, however, are subject to a special approval process. This process evaluates a proposed research project and its use of medical information, trying to balance the research needs with patients' needs for privacy of their medical information. Before we use or disclose medical information for research, the project will have been approved through this research approval process, but we may, however, disclose medical information about you to people preparing to conduct a research project, for example, to help them look for patients with specific medical needs. **As Required By Law**, we will disclose medical information about you when we are required to do so by federal, state or local law.
8. **To Avert a Serious Threat to Health or Safety**. We may use and disclose medical information about you when necessary to prevent a serious threat to your health and safety or the health and safety of the public or another person. In these circumstances, we will only make disclosures to someone able to help prevent the threat.
9. **To Our Business Associates:** A business associate is defined as someone that assists us in managing our business. For example, a professional that reviews the quality of our products and services. We may disclose PHI to another company that helps us manage our business. These business associates are required to sign a Business Associate Agreement with us that limits their use or disclosure of the PHI they receive.

C. SPECIAL SITUATIONS

1. **Worker's Compensation**. We may release medical information about you for worker's compensation or similar programs. These programs provide benefits for work-related injuries or illness.
2. **Public Health Risks**. We may disclose medical information about you for public health activities. These activities generally include the following:
   - To prevent or control disease, injury or disability;
   - To report births and deaths;
   - To report child abuse or neglect;
   - To report reactions to medications or problems with products;
   - To notify people of recalls of products they may be using;
   - To notify a person who may have been exposed to a disease or be at risk for contracting or spreading a disease or condition;
   - To notify the appropriate government authority if we believe a patient has been the victim of abuse, neglect or domestic violence. We will only make this disclosure if you agree or when required or authorized by law.
3. **Health Oversight Activities**. We may disclose medical information to a health oversight agency for activities authorized by law. These oversight activities include, for example, audits, investigations, inspections, and licensure. These activities are necessary for the government to monitor the health care system, government programs, and compliance with civil rights laws.
4. **Lawsuits and Disputes**. If you are involved in a lawsuit or a dispute, we may disclose medical information about you in response to a court or administrative order. We may also disclose medical information about you in response to a subpoena, discovery request, or other lawful process by someone else involved in the dispute, but only if efforts have been made to tell you about the request or to obtain an order protecting the information requested.
5. **Law Enforcement**. We may release medical information if asked to do so by a law enforcement official:
   - In response to a court order, subpoena, warrant, summons or similar process;
   - To identify or locate a suspect, fugitive, material witness, or missing person;
   - About the victim of a crime, under certain limited circumstances, we are unable to obtain the person's agreement;
   - About a death we believe may be the result of criminal conduct;
   - About criminal conduct at our facility; and
   - In emergency circumstances to report a crime; the location of the crime or victims; or the identity, description or location of the person who committed the crime.
6. **Coroners, Medical Examiners and Funeral Directors**. We may release medical information to a coroner or medical examiner. This may be necessary, for example, to identify a deceased person or determine the cause of death. We may also release medical information about patients to funeral directors in order for the funeral directors to carry out their duties.
7. **Organ and Tissue Donation**. If you are an organ donor, we may release medical information to organizations that handle organ procurement or organ, eye or tissue transplantation or to an organ donation bank, as necessary to facilitate organ or tissue donation and transplantation.

8. **Military and Veterans**. If you are a member of the armed forces, we may release medical information about you as required by military command authorities. We may also release medical information about foreign military personnel to the appropriate foreign military authority.
9. **National Security and Intelligence Activities**. We may release medical information about you to authorized federal officials of intelligence, counterintelligence, and other national security activities authorized by law.
10. **Inmates**. If you are an inmate of a correctional institution or under the custody of a law enforcement official, we may release medical information about you to the correctional institution or law enforcement official. This release would be necessary (1) for the institution to provide you with health care; (2) to protect your health and safety or the health and safety of others; (3) for the safety and security of the correctional institution.
11. **Marketing or Sale of Protected Health Information**. We will not use or disclose your medical information for the purposes of marketing non-health related products or services, or sell it to a third party without first obtaining your consent. You would not be treated differently for choosing not to consent.
12. **Fundraising.** If we engage in any fundraising activities, you have the right to opt out of receiving such communications. You would not be treated differently for opting out.

D. YOUR RIGHTS REGARDING MEDICAL INFORMATION ABOUT YOU.

You have the following rights regarding medical information we maintain about you:

1. **Right to Inspect and Copy**. You have the right to inspect and copy medical information that may be used to make decisions about your care. Usually, this includes medical and billing records, but does not include psychotherapy notes.

   To inspect and copy medical information that may be used to make decisions about you, you must submit your request in writing to Lifetime Care Home Health and Hospice, Medical Records Department, 3111 Winton Road S., Rochester, NY 14623-2905. If you request a copy of the information, we may charge a fee for the costs of copying, mailing or other supplies associated with your request. We may deny your request to inspect and copy in certain very limited circumstances. If you are denied access to medical information, you may request that the denial be reviewed. We will comply with the outcome of the review.

2. **Right to Amend**. If you feel that medical information we have about you is incorrect or incomplete, you may ask to amend the information. You have the right to request an amendment for as long as the information is kept by or for this facility. In certain cases, we may deny your request to amend your medical information.

   To request an amendment, your request must be made in writing and submitted to: Lifetime Care Home Health and Hospice, Privacy Officer, 3111 Winton Road S., Rochester, NY 14623-2905.

   Right to an Accounting of Disclosures. You have the right to request an "accounting of disclosures." This is a list of certain non-routine disclosures that we made of medical information about you. To request this accounting of disclosures, you must submit your request in writing to Lifetime Care Home Health and Hospice, Privacy Officer, 3111 Winton Road S., Rochester, NY 14623-2905. Your request must state a time period that may not be longer than six years and may not include dates before April 14, 2003. The first list you request within a 12 month period will be free. For additional lists, we may

charge you for the costs of providing the list. We will notify you of the cost involved and you may choose to withdraw or modify your request at that time before any costs are incurred.

3. **Right to Request Restrictions**. You have the right to request a restriction or limitation on the medical information we use or disclose about you for treatment, payment or health care operations. If you pay out of pocket in full for a service we provide to you, you have the right to request we restrict disclosure of the health information related to that service to your health plan when it is for the purposes of payment or health care operations. You also have the right to request a limit on the medical information we disclose about you to someone who is involved in your care or the payment for your care, like a family member or friend. For example, you could ask that we not use or disclose information about a surgery you had.

   We are not required to agree to your request. If we do agree, we will comply with your request unless the use or disclosure of your information is required by law, the information is needed to treat you or in certain emergency situations.

   To request restrictions, you must submit a written request to Lifetime Care Home Health and Hospice, Privacy Officer, 3111 Winton Road S., Rochester, NY 14623-2905. Your request must include:
   (1) what information you want to limit;
   (2) whether you want to limit our use, disclosure, or both; and
   (3) to whom you want the limits to apply, for example, disclosures to your spouse.

4. **Right to Request Confidential Communications**. You have the right to request that we communicate with you about medical matters in a certain way or at a certain location. For example, you can ask that we only contact you at work or by mail.

   To request confidential communications, you must make your request in writing to Lifetime Care Home Health and Hospice, Privacy Officer, 3111 Winton Road S., Rochester, NY 14623-2905.

   We will not ask you the reason for your request. We will accommodate all reasonable requests. Your request must specify how or where you wish to be contacted.
5. **Right to a Paper Copy of This Notice**. You have the right to a paper copy of this notice. You may ask us to give you a copy of this notice at any time.

You may obtain a copy of this notice on our website at http://www.lifetimecare.org, see Privacy Policy.

To obtain a paper copy of this notice:

Lifetime Care Home Health and Hospice
Privacy Office
3111 Winton Road S.
Rochester, NY 14623-2905

F. BREACH OF UNSECURED INFORMATION

We will notify you should there be a breach of unsecured information. We are required to notify you if there is any acquisition, access, use, or disclosure of your unsecured personal health information (PHI) that compromises the security or privacy of your PHI.

G. COMPLAINTS

If you believe your privacy rights have been violated, you may file a complaint with this facility or with the Secretary of the Department of Health and Human Services.
To file a complaint with this facility, contact our office at:

Lifetime Care Home Health and Hospice
Privacy Office
3111 Winton Road S.
Rochester, NY 14623-2905

You will not be penalized for filing a complaint.

H. OTHER USES OF MEDICAL INFORMATION

Other uses and disclosures of medical information not covered by this notice or the laws that apply to us will be made only with your written permission. If you provide us permission to use or disclose medical information about you, you may revoke that permission, in writing, at any time. If you revoke your permission, we will no longer use or disclose medical information about you for the reasons covered by your written authorization. This revocation will not affect any actions Lifetime Care Home Health and Hospice took in reliance on your authorization before your authorization cancellation form was processed.

I. CHANGES TO THIS NOTICE

We reserve the right to change this notice. We reserve the right to make the revised or changed notice effective for medical information we already have about you as well as any information we receive in the future. We will post a copy of the current notice at the facility. The notice will contain on the first page, in the top right-hand corner, the effective date. In addition, each time you come to the facility for treatment or health care services, you may ask for a copy of the notice currently in effect.

EXHIBIT D

Lifetime Health medical group

Effective Date: April 13, 2003
Revised Date: September 1, 2013

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

If you have any questions about this notice, please contact 1-877-341- 8576.

A. OUR COMMITMENT TO YOUR PRIVACY:

We understand that medical information about you and your health is personal. We are committed to protecting medical information about you. We create a record of the care and services you receive at our facility. We need this record to provide you with quality care and to comply with certain legal requirements. This notice applies to all of the records of your care generated by this facility.

This notice will tell you about the ways in which we may use and disclose medical information about you. We also describe your rights and certain obligations we have regarding the use and disclosure of medical information. We are required by law to:

- make sure that medical information that identifies you is kept private;
- give you this notice of our legal duties and privacy practices with respect to medical information about you; and
- follow the terms of the notice that is currently in effect.

B. HOW WE MAY USE AND DISCLOSE MEDICAL INFORMATION ABOUT YOU.

The following categories describe different ways that we use and disclose medical information.

For each category of uses or disclosures we will explain what we mean and try to give some examples. Not every use or disclosure in a category will be listed. However, all of the ways we are permitted to use and disclose information will fall within one of the categories.

1. **For Treatment**. We may use medical information about you to provide you with medical treatment or services. For example, if you have a condition that requires hospitalization, your medical record or portions of your medical record may be forwarded to hospital staff. We may use your medical information to write a prescription for you, we might disclose your medical information to a pharmacy when we order a prescription for you. We may ask you to have laboratory tests (such as blood or urine tests), and we may use the results to help us reach a diagnosis. Many of the people who work for our facility, including but not limited to our doctors and nurses, may use or disclose your medical information to others in order to treat you or assist others in your treatment. We may also disclose medical information about you to people who may be involved in your medical care such as family members.
2. **For Payment**. We may use and disclose medical information about you in order to bill and collect payment for the services you receive at this facility. For example, we may need to give your health plan information about an annual physical you received at this facility so your health plan will pay us or reimburse you for the physical. We may also tell your health plan about a treatment you are going to receive to obtain prior approval or to determine whether your plan will cover the treatment. We may use or disclose your medical information to obtain payment from third parties that may be responsible for such costs, such as family members. We may also disclose information about you to other health care providers or entities to assist in their billing and collection efforts. If you

have paid in full for a particular treatment, you can request that we do not provide information regarding the treatment to your health plan.

3. **For Health Care Operations**. We may use and disclose medical information about you to operate our business. These uses and disclosures are necessary to run the facility and make sure that all of our patients receive quality care. For example, we may use medical information to review our treatment and services and to evaluate the performance of our staff in caring for you. We may also combine medical information about many patients to decide what additional services should be offered, what services are not needed, and whether certain new treatments are effective. We may also disclose information to doctors, nurses, technicians, and medical students for review and learning purposes. We may disclose your medical information to other health care providers and entities to assist in their health care operations.
4. **Individuals Involved in Your Care or Payment for Your Care**. Unless you object, we may release medical information about you to a friend or family member who is involved in your medical care. We may also give information to someone who helps pay for your care. In addition, we may disclose medical information about you to an entity assisting in a disaster relief effort so that your family can be notified about your condition, status and location.
5. **Appointment Reminders**. We may use and disclose medical information to contact you as a reminder that you have an appointment for treatment or medical care at this facility.
6. **Treatment Alternatives & Health-Related Benefits and Services**. We may use and disclose medical information to tell you about or recommend possible treatment options or alternatives or to tell you about health-related benefits or services that may be of interest to you.
7. **Research**. Under certain circumstances, we may use and disclose medical information about you for research purposes. For example, a research project may involve comparing the health and recovery of all patients who received one medication to those who received another, for the same condition. All research projects, however, are subject to a special approval process. This process evaluates a proposed research project and its use of medical information, trying to balance the research needs with patients' needs for privacy of their medical information. Before we use or disclose medical information for research, the project will have been approved through this research approval process, but we may, however, disclose medical information about you to people preparing to conduct a research project, for example, to help them look for patients with specific medical needs, so long as the medical information they review does not leave the facility.
8. **As Required By Law**. We will disclose medical information about you when we are required to do so by federal, state or local law.
9. **To Avert a Serious Threat to Health or Safety**. We may use and disclose medical information about you when necessary to prevent a serious threat to your health and safety or the health and safety of the public or another person. In these circumstances, we will only make disclosures to someone able to help prevent the threat.

C. SPECIAL SITUATIONS

1. **Worker's Compensation**. We may release medical information about you for worker's compensation or similar programs. These programs provide benefits for work-related injuries or illness.
2. **Public Health Risks**. We may disclose medical information about you for public health activities. These activities generally include the following:
   - To prevent or control disease, injury or disability;
   - To report births and deaths;
   - To report child abuse or neglect;
   - To report reactions to medications or problems with products;
   - To notify people of recalls of products they may be using;
   - To notify a person who may have been exposed to a disease or be at risk for contracting or spreading a disease or condition;
   - To notify the appropriate government authority if we believe a patient has been the victim of abuse, neglect or domestic violence. We will only make this disclosure if you agree or when required or authorized by law.
3. **Health Oversight Activities**. We may disclose medical information to a health oversight agency for activities authorized by law. These oversight activities include, for example, audits, investigations, inspections, and licensure. These activities are necessary for the government to monitor the health care system, government programs, and compliance with civil rights laws.
4. **Lawsuits and Disputes**. If you are involved in a lawsuit or a dispute, we may disclose medical information about you in response to a court or administrative order. We may also disclose medical information about you in response to a subpoena, discovery request, or other lawful process by someone else involved in the dispute, but only if efforts have been made to tell you about the request or to obtain an order protecting the information requested.
5. **Law Enforcement**. We may release medical information if asked to do so by a law enforcement official:
   - In response to a court order, subpoena, warrant, summons or similar process;
   - To identify or locate a suspect, fugitive, material witness, or missing person;
   - About the victim of a crime, under certain limited circumstances, we are unable to obtain the person's agreement;
   - About a death we believe may be the result of criminal conduct;
   - About criminal conduct at our facility; and
   - In emergency circumstances to report a crime; the location of the crime or victims; or the identity, description or location of the person who committed the crime.
6. **Coroners, Medical Examiners and Funeral Directors**. We may release medical information to a coroner or medical examiner. This may be necessary, for example, to identify a deceased person or determine the cause of death. We may also release medical information about patients to funeral directors in order for the funeral directors to carry out their duties.
7. **Organ and Tissue Donation**. If you are an organ donor, we may release medical information to organizations that handle organ procurement or organ, eye or tissue transplantation or to an organ donation bank, as necessary to facilitate organ or tissue donation and transplantation.

8. **Military and Veterans**. If you are a member of the armed forces, we may release medical information about you as required by military command authorities. We may also release medical information about foreign military personnel to the appropriate foreign military authority.
9. **National Security and Intelligence Activities**. We may release medical information about you to authorized federal officials of intelligence, counterintelligence, and other national security activities authorized by law.
10. **Protective Services for the President and Others**. We may disclose medical information about you to authorized federal officials so they may provide protection to the President, other authorized persons or foreign heads of state or conduct special investigations.
11. **Inmates**. If you are an inmate of a correctional institution or under the custody of a law enforcement official, we may release medical information about you to the correctional institution or law enforcement official. This release would be necessary (1) for the institution to provide you with health care; (2) to protect your health and safety or the health and safety of others; (3) for the safety and security of the correctional institution.
12. **Marketing or Sale of Protected Health Information**. We will not use or disclose your medical information for the purposes of marketing non-health related products or services, or sell it to a third party without first obtaining your consent. You would not be treated differently for choosing not to consent.
13. **Fundraising.** If we engage in any fundraising activities, you have the right to opt out of receiving such communications. You would not be treated differently for opting out.
14. **Psychotherapy Notes**. If your medical record contains psychotherapy notes, your authorization is required for most uses and disclosures of these notes.

D. YOUR RIGHTS REGARDING MEDICAL INFORMATION ABOUT YOU.

You have the following rights regarding medical information we maintain about you:

1. **Right to Inspect and Copy**. You have the right to inspect and copy medical information that may be used to make decisions about your care. Usually, this includes medical and billing records, but does not include psychotherapy notes.

   To inspect and copy medical information that may be used to make decisions about you, you must submit your request in writing to Lifetime Health Medical Group, Medical Records Department, 800 Carter Street, Rochester, New York 14621. If you request a copy of the information, we may charge a fee for the costs of copying, mailing or other supplies associated with your request. We may deny your request to inspect and copy in certain very limited circumstances. If you are denied access to medical information, you may request that the denial be reviewed. We will comply with the outcome of the review.
2. **Right to Amend**. If you feel that medical information we have about you is incorrect or incomplete, you may ask to amend the information. You have the right to request an amendment for as long as the information is kept by or for this facility. In certain cases, we may deny your request to amend your medical information.

   To request an amendment, your request must be made in writing and submitted to: Lifetime Health Medical Group, Privacy Officer, 77 Sully's Trail, Pittsford, NY 14534.
3. **Right to an Accounting of Disclosures**. You have the right to request an “accounting

of disclosures." This is a list of certain non-routine disclosures that we made of medical information about you. To request this accounting of disclosures, you must submit your request in writing to Lifetime Health Medical Group, Privacy Officer, 77 Sully's Trail, Pittsford, NY 14534. Your request must state a time period that may not be longer than six years and may not include dates before April 14, 2003. The first list you request within a 12 month period will be free. For additional lists, we may charge you for the costs of providing the list. We will notify you of the cost involved and you may choose to withdraw or modify your request at that time before any costs are incurred.

4. **Right to Request Restrictions**. You have the right to request a restriction or limitation on the medical information we use or disclose about you for treatment, payment or health care operations. If you pay out of pocket in full for a service we provide to you, you have the right to request we restrict disclosure of the health information related to that service to your health plan when it is for the purposes of payment or health care operations. You also have the right to request a limit on the medical information we disclose about you to someone who is involved in your care or the payment for your care, like a family member or friend. For example, you could ask that we not use or disclose information about a surgery you had.

   We are not required to agree to your request. If we do agree, we will comply with your request unless the use or disclosure of your information is required by law, the information is needed to treat you or in certain emergency situations.

   To request restrictions, you must submit a written request to Lifetime Health Medical Group, Privacy Officer, 77 Sully's Trail, Pittsford, NY 14534. Your request must include:
   (1) what information you want to limit;
   (2) whether you want to limit our use, disclosure, or both; and
   (3) to whom you want the limits to apply, for example, disclosures to your spouse.

5. **Right to Request Confidential Communications**. You have the right to request that we communicate with you about medical matters in a certain way or at a certain location. For example, you can ask that we only contact you at work or by mail.
   To request confidential communications, you must make your request in writing to Lifetime Health Medical Group, Privacy Officer, 77 Sully's Trail, Pittsford, NY 14534. We will not ask you the reason for your request. We will accommodate all reasonable requests. Your request must specify how or where you wish to be contacted.

6. **Right to a Paper Copy of This Notice**. You have the right to a paper copy of this notice. You may ask us to give you a copy of this notice at any time.

You may obtain a copy of this notice on our website at www.lifetimehealth.org/PrivacyPolicy

To obtain a paper copy of this notice: Lifetime Health Medical Group, Privacy Officer
77 Sully's Trail
Pittsford, NY 14534

F. BREACH OF UNSECURED INFORMATION

We will notify you should there be a breach of unsecured information. We are required to notify you if there is any acquisition, access, use, or disclosure of your unsecured PHI that compromises the security or privacy of your PHI.

G. COMPLAINTS

If you believe your privacy rights have been violated, you may file a complaint with this facility or with the Secretary of the Department of Health and Human Services.

To file a complaint with this facility, contact our office at:

Lifetime Health Medical Group, Privacy Officer
77 Sully's Trail
Pittsford, NY 14534
or call 1-877-341-8576

You will not be penalized for filing a complaint.

H. OTHER USES OF MEDICAL INFORMATION

Other uses and disclosures of medical information not covered by this notice or the laws that apply to us will be made only with your written permission. If you provide us permission to use or disclose medical information about you, you may revoke that permission, in writing, at any time. If you revoke your permission, we will no longer use or disclose medical information about you for the reasons covered by your written authorization. This revocation will not affect any actions Lifetime Health Medical Group took in reliance on your authorization before your authorization cancellation form was processed.

I. CHANGES TO THIS NOTICE

We reserve the right to change this notice. We reserve the right to make the revised or changed notice effective for medical information we already have about you as well as any information we receive in the future. We will post a copy of the current notice at the facility. The notice will contain on the first page, in the top right-hand corner, the effective date. In addition, each time you come to the facility for treatment or health care services, you may ask for a copy of the notice currently in effect.

EXHIBIT E

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION.

PLEASE REVIEW IT CAREFULLY.

THE PRIVACY OF YOUR MEDICAL INFORMATION IS IMPORTANT TO US.

This notice takes effect April 14, 2003.

OUR COMMITMENT TO YOUR PRIVACY

We understand that medical information about you and your health is personal. We are committed to safeguarding your protected health information (PHI).

PHI is any information that can identify you as an individual and your past, present or future physical or mental health condition.

This notice will tell you about the ways in which we may use and disclose medical information about you. We also describe your rights and certain obligations we have regarding the use and disclosure of medical information.
The law requires us to:

- make sure that PHI that identifies you is kept private;
- give you this notice of our legal duties and privacy practices with respect to PHI about you; and
- follow the terms of the notice that is currently in effect.

OUR LEGAL DUTY

We at **MedAmerica Insurance Company, MedAmerica Insurance Company of New York and MedAmerica Insurance Company of Florida ("MedAmerica")** are required by applicable federal and state laws to maintain the privacy of your PHI. We are also required to give you this notice about our privacy practices, our legal duties, and your rights concerning PHI. We must follow the privacy practices that are described in this notice while it is in effect, including notification should there be a breach of your unsecured PHI.

We reserve the right to change our privacy practices and the terms of this notice at any time, provided that applicable law permits such changes. We reserve the right to make the changes in our privacy practices and the new terms of our notice effective for all PHI that we maintain, including medical information we created or received before we made the changes. Before we make a significant change in our privacy practices, we will change this notice and send the new notice to our insureds at the time of the change.

You may request a copy of our notice at any time. For more information about our privacy practices, or for additional copies of this notice, please visit our website at www.medamericaltc.com or contact us using the contact information at the end of this notice.

Uses and Disclosures of Nonpublic Personal Information

Nonpublic Personal Information is information you give us on your application, claim forms, premium payments etc. For example: your name, identification number, social security number, address(es), type of benefits, payment amounts, etc.

We will not give out your nonpublic personal information to anyone unless we are permitted to do so by law or have received a signed authorization form. You may revoke this authorization in writing at any time. Your revocation will not affect any actions taken in reliance on your authorization before your authorization cancellation was processed.

Uses and Disclosures of Medical Information

The following categories describe different purposes for which we use and disclose PHI. For each category of uses or disclosures we will explain what we mean and try to give some examples. Not every use or disclosure in a category will be listed. However, all of the ways we are permitted to use and disclose information will fall within one of the categories. If we need to use or disclose your PHI in any other way, we will obtain your signed authorization before our use or disclosure. You may revoke this authorization in writing at any time. Your revocation will not affect any actions taken in reliance on your authorization before your authorization cancellation was processed.

Treatment: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may disclose PHI to health care professionals involved in your care. For example, we may disclose at claim time your current health status to our Business Associates or other Licensed Health Care Professionals contracted with us. This allows providers to manage, coordinate and administer your treatment.

Payment: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may use and disclose PHI to collect premiums, to determine our responsibility to pay claims or to notify insureds and providers of our claim determinations. We may disclose PHI to providers to assist them in their billing and collection efforts. We may also disclose PHI to other insurance companies to coordinate the reimbursement of insurance benefits. For example, we may disclose PHI to another insurance company in order to determine which company holds the primary responsibility for your claim(s).

Healthcare Operations: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may use and disclose PHI for purposes of performing our healthcare operations. Our healthcare operations include using PHI to determine insurability and premiums, to conduct quality assessment and improvement activities, to engage in care coordination, or to determine eligibility for benefits. For example, we may use or disclose PHI to an agency and contracted Business Associate that will assess your functional and cognitive impairment for us so that we may determine your eligibility for benefits.

To You: We must disclose your PHI to you, as described in the Individual Rights section of this notice, below. We may also use and disclose PHI when we recommend a Plan of Care to tell you about value-added health related benefits or services that may be of interest to you.

To Family and Friends: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. If you agree, or if you are unable to agree when the situation (such as a medical emergency or disaster relief), indicates that disclosure would be in your best interest, we may disclose PHI to a family member, friend or other person. In an emergency situation, we will only disclose the minimum amount necessary.

To Our Business Associates: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. A business associate is defined as someone that assists us in managing our business or performing our healthcare operations. For example, a professional that conducts assessments for us in your place of residence. We may disclose PHI to another company that helps us manage our business. For example, we may disclose PHI to an independent agency to review your health and medical history for us during the application process (i.e. medical underwriting). These business associates are required to sign a confidentiality agreement with us that limits their use or disclosure of the PHI they receive.

To Plan Sponsors: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. A plan sponsor is defined as the employer, employee organization or group that establishes and maintains the insured's benefit plan. If you are enrolled in a group plan, we may disclose PHI to the plan sponsor to the extent necessary to permit the plan sponsor to perform plan administrative functions. For example, if you choose to have your premiums paid via a deduction from your payroll. Before PHI is disclosed to your plan sponsor, we will receive certification from the plan sponsor that they agree to limit their use or disclosure of this information to plan administration functions only.

Research: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may use or disclose PHI for research purposes in limited circumstances. For example, a research project may involve analyzing enrollment data to illustrate consumer behavior. All research projects that disclose PHI are required to obtain special approval.

Coroners, Medical Examiners and Funeral Directors: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may release PHI to a coroner or medical examiner, to identify a deceased person or determine the cause of death. We may also release PHI about deceased insureds to funeral directors in order for the funeral directors to carry out their duties.

Organ Donation: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. If you are an organ donor, we may release PHI to organizations that handle organ procurement or organ, eye or tissue transplantation or to an organ donation bank, to facilitate organ or tissue donation and transplantation. This may include a living donor as well as a deceased donor.

Public Health and Safety: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may disclose PHI to the extent necessary to avert a serious and imminent threat to your health or safety, or the health or safety of others. We may disclose PHI to a government agency authorized to oversee insurance companies, the healthcare system or government programs or its contractors, and to public health authorities for public health purposes.

Victims of Abuse, Neglect or Domestic Violence: We may disclose PHI to appropriate authorities if we reasonably believe that you are a possible victim of abuse, neglect, domestic violence or other crimes.

Required by Law: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may use or disclose PHI when we are required to do so by law. For example, we must disclose PHI to the U.S. Department of Health and Human Services upon request to determine whether we are in compliance with federal privacy laws.

Process and Proceedings: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may disclose PHI in response to a court or administrative order, subpoena, discovery request, or other lawful process. Under limited circumstances, such as a court order, warrant, or grand jury subpoena, we may disclose PHI to law enforcement officials.

Law Enforcement: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may disclose PHI to a law enforcement official investigating a suspect, fugitive, material witness, crime victim or missing person. We may disclose PHI of an inmate or other person in lawful custody of a law enforcement official or correctional institution under certain circumstances.

Military and National Security: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may disclose to the military, PHI of Armed Forces personnel under certain circumstances. We may disclose to authorized federal officials medical information required for lawful intelligence, counterintelligence, and other national security activities.

Marketing and Fundraising: We will not disclose PHI for marketing or fundraising purposes without your authorization. To the extent we use PHI for marketing or fundraising purposes, you will be contacted by us and have the right to opt out of receiving these communications from us and our use of your information for such purposes.

Breach of Unsecured Information: We will notify you should there be a breach of unsecured information. We are required to notify you if there is any acquisition, access, use or disclosure of your unsecured PHI that compromises the security or privacy of your PHI.

Psychotherapy Information: We will not release this information without authorization. Should it be applicable that your psychotherapy notes be included in an appropriate use or disclosure of information, in most instances, we are required to obtain your authorization for the release of this information.

Individual Rights

The following information is effective as of 4/14/03:

Access: You have the right to inspect and/or copy your PHI, with limited exceptions such as information a licensed health care professional, exercising professional judgment, determines that providing access is reasonably likely to endanger the life, physical safety or cause someone substantial harm. On or after 4/14/03, you may contact us using the contact information at the end of this notice to obtain a form to be completed and returned to us. If you request copies, we reserve the right to charge you a reasonable fee for each copy, plus postage if the copies are mailed to you.

Disclosure Accounting: You have the right to receive a list of instances in which we, or our business associates, disclosed your PHI. The list will not include disclosures we made for the purpose of treatment, payment, healthcare operations, disclosures made with your authorization, or certain other disclosures. To request a disclosure accounting, on or after 4/14/03, you may contact us using the contact information at the end of this notice to obtain a form to be completed and returned to us. You may request an accounting of disclosures made on or after 4/14/03 and the request may not exceed a six (6) year time period. We will provide you with the date on which we made the disclosure, the name of the person or

entity to whom we disclosed your PHI, a description of the PHI we disclosed and the reason for the disclosure. If you request this list more than once in a 12-month period, we may charge you a reasonable, cost-based fee for responding to these additional requests.

Restriction Requests: You have the right to request that we place additional restrictions on our use or disclosure of your PHI. As permitted by law, we will not honor these requests, as it prohibits us from administering your benefits.

Confidential Communication: You have the right to request that we communicate with you confidentially about your PHI. We will honor a request to communicate with you at an alternative location if you believe you would be endangered if we do not communicate to the alternative location. We must accommodate your request if it is reasonable and specifies the alternative location. To request confidential communication, you may contact us using the contact information at the end of this notice.

Amendment: You have the right to request that we amend your PHI. Your request must be in writing, and it must explain why the information should be amended. We may deny your request if we did not create the information you want amended or if we determine the information is accurate. If we accept your request to amend the information, we will make reasonable efforts to inform others, including people you name, of the amendment and to include the changes in any future disclosures of that information. If we deny your request, we will provide you with a written explanation. You may respond with a statement of disagreement that will be attached to the information you wanted amended. On or after 4/14/13, you may contact us using the contact information at the end of this notice to obtain a form to be completed and returned to us.

Electronic Notice: If you receive this notice on our web site or by electronic mail (e-mail), you are entitled to receive this notice in written form. Please contact us using the contact information at the end of this notice to obtain this notice in written form.

Safeguards

It is our policy to keep all information about you confidential in all settings. It is so important to us that we take the following steps:

- our employees sign an agreement to follow our Code of Business Conduct;
- our employees are required to complete our privacy training program;
- we have implemented the necessary sanctions for violation of our privacy practices;
- we have a privacy oversight committee that reviews our privacy practices;
- we have a security coordinator to detect and prevent security breaches;
- all computer systems that contain personal information have security protections; and
- we randomly audit third party administrator's offices to ensure that PHI is kept in secure locations.

Questions and Complaints

If you want more information about our privacy practices or have questions or concerns, please contact us using the contact information at the end of this notice.

On or after 4/14/03, if you are concerned that we may have violated your privacy rights, as described above, or you disagree with a decision we made about access to your PHI or in response to a request you made to amend or restrict the use or disclosure of your PHI or to have us confidentially communicate with you at an alternative location, you may complain to us using the contact information at the end of this notice. You also may submit a written complaint to the U.S. Department of Health and Human Services. We will provide you with the address to file your complaint with the U.S. Department of Health and Human Services upon request.

We support your right to protect the privacy of your PHI. We will not retaliate in any way if you choose to file a complaint with us or with the U.S. Department of Health and Human Services.

Privacy Complaints, Rights or Questions:

Contact Office:	Privacy Officer
Address:	PO Box 41930 Rochester, New York 14604-0620
Phone:	1-800-544-0327 Ext. 3413
E-mail:	LTCprivacy.officer@medamericaltc.com

EXHIBIT F

univera HEALTHCARE
AN EXCELLUS COMPANY

165 Court Street, Rochester, New York 14647

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION.

PLEASE REVIEW IT CAREFULLY.

THE PRIVACY OF YOUR MEDICAL INFORMATION IS IMPORTANT TO US.

This notice takes effect April 14, 2003.

OUR COMMITMENT TO YOUR PRIVACY

We understand that medical information about you and your health is personal. We are committed to safeguarding your protected health information (PHI).

PHI is any information that can identify you as an individual and your past, present or future physical or mental health condition.

This notice will tell you about the ways in which we may use and disclose medical information about you. We also describe your rights and certain obligations we have regarding the use and disclosure of medical information. The law requires us to:

- make sure that PHI that identifies you is kept private;
- give you this notice of our legal duties and privacy practices with respect to PHI about you; and
- follow the terms of the notice that is currently in effect.

OUR LEGAL DUTY

We **(Univera Healthcare)** are required by applicable federal and state laws to maintain the privacy of your PHI. We are also required to give you this notice about our privacy practices, our legal duties, and your rights concerning PHI. We must follow the privacy practices that are described in this notice while it is in effect, including notification should there be a breach of your unsecured PHI.

We reserve the right to change our privacy practices and the terms of this notice at any time, provided that applicable law permits such changes. We reserve the right to make the changes in our privacy practices and the new terms of our notice effective for all PHI that we maintain, including medical information we created or received before we made the changes. Before we make a significant change in our privacy practices, we will change this notice and send the new notice to our health plan subscribers at the time of the change.

You may request a copy of our notice at any time. For more information about our privacy practices, or for additional copies of this notice, please contact us using the contact information at the end of this notice.

Uses and Disclosures of Nonpublic Personal Information

Nonpublic Personal Information is information you give us on your enrollment form, claim forms, premium payments etc. For example: names, member identification number, social security number, addresses, type of health care benefits, payment amounts, etc.

We will not give out your nonpublic personal information to anyone unless we are permitted to do so by law or have received a signed authorization form from the member. You may revoke this authorization in writing by completing an authorization cancellation form at any time. This revocation will not affect any actions we took in reliance on your authorization before your authorization cancellation form was processed.

Uses and Disclosures of Medical Information

The following categories describe different purposes for which we use and disclose PHI. For each category of uses or disclosures we will explain what we mean and try to give some examples. Not every use or disclosure in a category will be listed. However, all of the ways we are permitted to use and disclose information will fall within one of the categories. If we need to use or disclose your PHI in any other way, we will obtain your signed authorization before our use or disclosure. You may revoke this authorization in writing by completing an authorization cancellation form at any time. This revocation will not affect any actions we took in reliance on your authorization before your authorization cancellation form was processed.

Treatment: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may disclose PHI to doctors or hospitals involved in your care. For example, we may disclose your medications to an emergency room physician so that he/she can avoid dangerous drug interactions. This allows providers to manage, coordinate and administer treatment.

Payment: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may use and disclose PHI to collect premiums, to determine our responsibility to pay claims or to notify members and providers of our claim determinations. We may disclose PHI to providers to assist them in their billing and collection efforts. We may also disclose PHI to other insurance companies to coordinate the reimbursement of health insurance benefits. For example, we may disclose PHI to an automobile no-fault insurance company to determine responsibility for claim payment. Also, if you have health insurance through another insurance company, we may disclose PHI to that other health insurance company in order to determine which company holds the responsibility for your claims.

Healthcare Operations: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may use and disclose PHI for purposes of performing our healthcare operations. Our healthcare operations include using PHI to determine premiums, to conduct quality assessment and improvement activities, to engage in care coordination or case management, to determine eligibility for benefits. For example, we may use or disclose PHI when working with accreditation agencies that monitor and evaluate the quality of our benefit programs.

To You: We must disclose your PHI to you, as described in the Individual Rights section of this notice, below. We may also use and disclose PHI to tell you about recommended possible treatment options or alternatives or to tell you about health related benefits or services that may be of interest to you.

To Family and Friends: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. If you agree or, if you are unable to agree when the situation, (such as medical emergency or disaster relief), indicates that disclosure would be in your best interest, we may disclose PHI to a family member, friend or other person. In an em ergency situation, we will only disclose the minimum amount necessary.

To Our Business Associates: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. A business associate is defined as someone that assists us in managing our business. For example, a professional that reviews the quality of our products and services. We may disclose PHI to another company that helps us manage our business. For example, we may disclose PHI to a company that performs case reviews to ensure our members receive quality care. These business associates are required to sign a confidentiality agreement with us that limits their use or disclosure of the PHI they receive.

To Plan Sponsors: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. A plan sponsor is defined as the employer or employee organization that establishes and maintains the employee's benefit plan. If you are enrolled in a group health plan, we may disclose PHI to the plan sponsor to permit the plan sponsor to perform plan administrative functions. For example, the cost analysis of the benefit program. Before PHI is disclosed to your plan sponsor, we will receive certification from the plan sponsor that appropriate amendments have been made to group health plan document(s) and the plan sponsor agrees to limit their use or disclosure of this information to plan administration functions only.

Research: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may use or disclose PHI for research purposes in limited circumstances. For example, a r esearch project may involve comparing the health and recovery of all members who received one medication to those who received another medication for the same condition. All research projects are required to obtain special approval.

Coroners, Medical Examiners and Funeral Directors: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may release PHI to a coroner or medical examiner, to identify a deceased person or determine the cause of death. We may also release PHI about deceased members to funeral directors in order for the funeral directors to carry out their duties.

Organ Donation: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. If you are an organ donor, we may release PHI to organizations that handle organ procurement or organ, eye or tissue transplantation or to an organ donation bank, to facilitate organ or tissue donation and transplantation. This may include a living donor as well as a deceased donor.

Public Health and Safety: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may disclose PHI to the extent necessary to avert a s erious and imminent threat to your health or safety, or the health or safety of others. We may disclose PHI to a government agency authorized to oversee the healthcare system or government programs or its contractors, and t o public health authorities for public health purposes.

Victims of Abuse, Neglect or Domestic Violence: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may disclose PHI to appropriate authorities if w e r easonably believe that you are a possible victim of abuse, neglect, domestic violence or other crimes.

Required by Law: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may use or disclose PHI when we are required to do so by law. For example, we must disclose PHI to the U.S. Department of Health and Human Services upon request to determine whether we are in compliance with federal privacy laws.

Process and Proceedings: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may disclose PHI in response to a court or administrative order, subpoena, discovery request, or other lawful process. Under limited circumstances, such as a court order, warrant, or grand jury subpoena, we may disclose PHI to law enforcement officials.

Law Enforcement: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may disclose PHI to a law enforcement official investigating a suspect, fugitive, material witness, crime victim or missing person. We may disclose PHI of an inmate or other person in lawful custody of a law enforcement official or correctional institution under certain circumstances.

Military and National Security: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may disclose to the military, PHI of Armed Forces personnel under certain circumstances. We may disclose to authorized federal officials medical information required for lawful intelligence, counterintelligence, and other national security activities.

Marketing and Fundraising: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. To the extent we use PHI for marketing or fundraising purposes, you will be contacted by us and have the right to opt out of receiving these communications from us and our use of your information for such purposes.

Genetic Nondiscrimination Act (GINA): We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We will not disclose your PHI containing genetic information for underwriting purposes. GINA expressly prohibits the use or disclosure of genetic information for these purposes.

Breach of Unsecured Information: We will notify you should there be a breach of unsecured information. We are required to notify you if there is any acquisition, access, use, or disclosure of your unsecured PHI that compromises the security or privacy of your PHI.

Psychotherapy Information: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. Should it be applicable that your psychotherapy notes be included in an appropriate use or disclosure of information, in most instances, we are required to obtain your authorization for the release of this information.

Individual Rights

Access: You have the right to inspect and/or copy your PHI, with limited exceptions such as information a licensed health care professional, exercising professional judgment, determines that providing access is reasonably likely to endanger the life, physical safety or cause someone substantial harm. You may contact us using the telephone number on the back of your identification card to obtain a form to be completed and returned to us. If you request copies, we reserve the right to charge you a reasonable fee for each copy, plus postage if the copies are mailed to you.

Disclosure Accounting: You have the right to receive a list of instances in which we or our business associates disclosed your PHI. The list will not include disclosures we made for the purpose of treatment, payment, healthcare operations, disclosures made with your authorization, or certain other disclosures. To request a disclosure accounting you may contact us using the telephone number on the back of your identification card to obtain a form to be completed and returned to us. The request may not exceed a six year time period. We will provide you with the date on which we made the disclosure, the name of the person or entity to whom we disclosed your PHI, a description of the PHI we disclosed and the reason for the disclosure. If you request this list more than once in a 12-month period, we may charge you a reasonable, cost-based fee for responding to these additional requests.

Restriction Requests: You have the right to request that we place additional restrictions on our use or disclosure of your PHI. As permitted by law, we will not honor these requests, as it prohibits us from administering your benefits.

Confidential Communication: You have the right to request that we communicate with you confidentially about your PHI. We will honor a request to communicate to an alternative location if you believe you would be endangered if we do not communicate to the alternative location. We must accommodate your request if it is reasonable and specifies the alternative location. To request a form to be completed and returned to us, you may contact us using the telephone number on the back of your identification card.

Amendment: You have the right to request that we amend your PHI. Your request must be in writing, and it must explain why the information should be amended. We may deny your request if we did not create the information you want amended or if we determine the information is accurate. If we accept your request to amend the information, we will make reasonable efforts to inform others, including people you name, of the amendment and to include the changes in any future disclosures of that information. If we deny your request, we will provide you with a written explanation. You may respond with a statement of disagreement that will be attached to the information you wanted amended. You may contact us using the telephone number on the back of your identification card to obtain a form to be completed and returned to us.

Electronic Notice: If you receive this notice on our web site or by electronic mail (e-mail), you are entitled to receive this notice in written form. Please contact us using the contact information at the end of this notice to obtain this notice in written form.

Safeguards

It is our policy to keep all information about you confidential in all settings. It is so important to us that we take the following steps:

- our employees sign an agreement to follow our Code of Business Conduct;
- our employees are required to complete our privacy training program;
- we have implemented the necessary sanctions for violation of our privacy practices;
- we have a privacy oversight committee that reviews our privacy practices;
- we have a security coordinator to detect and prevent security breaches;
- all computer systems that contain personal information have security protections; and
- we randomly check provider offices on a routine basis to ensure that medical records are kept in secure locations.

Questions and Complaints

If you want more information about our privacy practices or have questions or concerns, please contact us using the contact information at the end of this notice.

If you are concerned that we may have violated your privacy rights, as described above, or you disagree with a decision we made about access to your PHI or in response to a request you made to amend or restrict the use or disclosure of your PHI or to have us confidentially communicate with you at an alternative location, you may complain to us using the contact information at the end of this notice. You also may submit a written complaint to the U.S. Department of Health and Human Services. We will provide you with the address to file your complaint with the U.S. Department of Health and Human Services upon request.

We support your right to protect the privacy of your PHI. We will not retaliate in any way if you choose to file a complaint with us or with the U.S. Department of Health and Human Services.

Privacy Rights or Questions:

Contact Office: Customer Service

Phone: Please call the telephone number on your identification card.

Privacy Complaints:

Contact Office: Privacy Officer
Address: 333 Butternut Dr.
Dewitt, NY 13214-1803

Phone: 1-866-584-2313

E-mail: privacy.officer@univerahealthcare.com

EXHIBIT G

Excellus

This is Your
EXCLUSIVE PROVIDER ORGANIZATION CONTRACT
Issued by

EXCELLUS HEALTH PLAN, INC.

A nonprofit independent licensee of the BlueCross BlueShield Association

This is Your individual direct payment Contract for exclusive provider organization coverage issued by Excellus Health Plan, Inc. This Contract, together with the attached Schedule of Benefits, applications and any amendment or rider amending the terms of this Contract, constitute the entire agreement between You and Us.

You have the right to return this Contract. Examine it carefully. If You are not satisfied, You may return this Contract to Us and ask Us to cancel it. Your request must be made in writing within ten (10) days from the date You receive this Contract. We will refund any Premium paid including any Contract fees or other charges.

Renewability. Refer to the Termination of Coverage section of this Contract for the renewal provisions.

In-Network Benefits. This Contract only covers in-network benefits. To receive in-network benefits You must receive care exclusively from Participating Providers in Our network. Except for care for an Emergency Condition described in the Emergency Services and Urgent Care section of this Contract, You will be responsible for paying the cost of all care that is provided by Non-Participating Providers.

READ THIS ENTIRE CONTRACT CAREFULLY. IT IS YOUR RESPONSIBILITY TO UNDERSTAND THE TERMS AND CONDITIONS IN THIS CONTRACT.

This Contract is governed by the laws of New York State.

EXCELLUS HEALTH PLAN, INC.
doing business as

Excellus BlueCross BlueShield
165 Court Street
Rochester, NY 14647

By:
Christopher C. Booth
President and Chief Executive Officer

Excellus
165 Court Street
Rochester, New York 14647

A nonprofit independent licensee of the BlueCross BlueShield Association

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION.

PLEASE REVIEW IT CAREFULLY.

THE PRIVACY OF YOUR MEDICAL INFORMATION IS IMPORTANT TO US.

This notice takes effect April 14, 2003

OUR COMMITMENT TO YOUR PRIVACY

We understand that medical information about you and your health is personal. We are committed to safeguarding your protected health information (PHI).

PHI is any information that can identify you as an individual and your past, present or future physical or mental health condition.

This notice will tell you about the ways in which we may use and disclose medical information about you. We also describe your rights and certain obligations we have regarding the use and disclosure of medical information. The law requires us to:

- make sure that PHI that identifies you is kept private;
- give you this notice of our legal duties and privacy practices with respect to PHI about you; and
- follow the terms of the notice that is currently in effect.

OUR LEGAL DUTY

We **(Excellus BlueCross BlueShield)** are required by applicable federal and state laws to maintain the privacy of your PHI. We are also required to give you this notice about our privacy practices, our legal duties, and your rights concerning PHI. We must follow the privacy practices that are described in this notice while it is in effect, including notification should there be a breach of your unsecured PHI.

We reserve the right to change our privacy practices and the terms of this notice at any time, provided that applicable law permits such changes. We reserve the right to make the changes in our privacy practices and the new terms of our notice effective for all PHI that we maintain, including medical information we created or received before we made the changes. Before we make a significant change in our privacy practices, we will change this notice and send the new notice to our health plan subscribers at the time of the change.

You may request a copy of our notice at any time. For more information about our privacy practices, or for additional copies of this notice, please contact us using the contact information at the end of this notice.

Uses and Disclosures of Nonpublic Personal Information

Nonpublic Personal Information is information you give us on your enrollment form, claim forms, premium payments etc. For example: names, member identification number, social security number, addresses, type of health care benefits, payment amounts, etc.

We will not give out your nonpublic personal information to anyone unless we are permitted to do so by law or have received a signed authorization form from the member. You may revoke this authorization in writing by completing an authorization cancellation form at any time. This revocation will not affect any actions we took in reliance on your authorization before your authorization cancellation form was processed.

Uses and Disclosures of Medical Information

The following categories describe different purposes for which we use and disclose PHI. For each category of uses or disclosures we will explain what we mean and try to give some examples. Not every use or disclosure in a category will be listed. However, all of the ways we are permitted to use and disclose information will fall within one of the categories. If we need to use or disclose your PHI in any other way, we will obtain your signed authorization before our use or disclosure. You may revoke this authorization in writing by completing an authorization cancellation form at any time. This revocation will not affect any actions we took in reliance on your authorization before your authorization cancellation form was processed.

Treatment: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may disclose PHI to doctors or hospitals involved in your care. For example, we may disclose your medications to an emergency room physician so that he/she can avoid dangerous drug interactions. This allows providers to manage, coordinate and administer treatment.

Payment: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may use and disclose PHI to collect premiums, to determine our responsibility to pay claims or to notify members and providers of our claim determinations. We may disclose PHI to providers to assist them in their billing and collection efforts. We may also disclose PHI to other insurance companies to coordinate the reimbursement of health insurance benefits. For example, we may disclose PHI to an automobile no-fault insurance company to determine responsibility for claim payment. Also, if you have health insurance through another insurance company, we may disclose PHI to that other health insurance company in order to determine which company holds the responsibility for your claims.

Healthcare Operations: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may use and disclose PHI for purposes of performing our healthcare operations. Our healthcare operations include using PHI to determine premiums, to conduct quality assessment and improvement activities, to

engage in care coordination or case management, to determine eligibility for benefits. For example, we may use or disclose PHI when working with accreditation agencies that monitor and evaluate the quality of our benefit programs.

To You: We must disclose your PHI to you, as described in the Individual Rights section of this notice, below. We may also use and disclose PHI to tell you about recommended possible treatment options or alternatives or to tell you about health related benefits or services that may be of interest to you.

To Family and Friends: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. If you agree or, if you are unable to agree when the situation, (such as medical emergency or disaster relief), indicates that disclosure would be in your best interest, we may disclose PHI to a family member, friend or other person. In an emergency situation, we will only disclose the minimum amount necessary.

To Our Business Associates: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. A business associate is defined as someone that assists us in managing our business. For example, a professional that reviews the quality of our products and services. We may disclose PHI to another company that helps us manage our business. For example, we may disclose PHI to a company that performs case reviews to ensure our members receive quality care. These business associates are required to sign a confidentiality agreement with us that limits their use or disclosure of the PHI they receive.

To Plan Sponsors: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. A plan sponsor is defined as the employer or employee organization that establishes and maintains the employee's benefit plan. If you are enrolled in a group health plan, we may disclose PHI to the plan sponsor to permit the plan sponsor to perform plan administrative functions. For example, the cost analysis of the benefit program. Before PHI is disclosed to your plan sponsor, we will receive certification from the plan sponsor that appropriate amendments have been made to group health plan document(s) and the plan sponsor agrees to limit their use or disclosure of this information to plan administration functions only.

Research: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may use or disclose PHI for research purposes in limited circumstances. For example, a research project may involve comparing the health and recovery of all members who received one medication to those who received another medication for the same condition. All research projects are required to obtain special approval.

Coroners, Medical Examiners and Funeral Directors: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may release PHI to a coroner or medical examiner, to identify a deceased person or determine the cause of death. We may also release PHI about deceased members to funeral directors in order for the funeral directors to carry out their duties.

Organ Donation: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. If you are an organ donor, we may release PHI to organizations that handle organ procurement or organ, eye or tissue transplantation or to an organ donation bank, to facilitate organ or tissue donation and transplantation. This may include a living donor as well as a deceased donor.

Public Health and Safety: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may disclose PHI to the extent necessary to avert a serious and imminent threat to your health or safety, or the health or safety of others. We may disclose PHI to a government agency authorized to oversee the healthcare system or government programs or its contractors, and to public health authorities for public health purposes.

Victims of Abuse, Neglect or Domestic Violence: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may disclose PHI to appropriate authorities if we reasonably believe that you are a possible victim of abuse, neglect, domestic violence or other crimes.

Required by Law: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may use or disclose PHI when we are required to do so by law. For example, we must disclose PHI to the U.S. Department of Health and Human Services upon request to determine whether we are in compliance with federal privacy laws.

Process and Proceedings: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may disclose PHI in response to a court or administrative order, subpoena, discovery request, or other lawful process. Under limited circumstances, such as a court order, warrant, or grand jury subpoena, we may disclose PHI to law enforcement officials.

Law Enforcement: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may disclose PHI to a law enforcement official investigating a suspect, fugitive, material witness, crime victim or missing person. We may disclose PHI of an inmate or other person in lawful custody of a law enforcement official or correctional institution under certain circumstances.

Military and National Security: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may disclose to the military, PHI of Armed Forces personnel under certain circumstances. We may disclose to authorized federal officials medical information required for lawful intelligence, counterintelligence, and other national security activities.

Marketing and Fundraising: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. To the extent we use PHI for marketing or fundraising purposes, you will be contacted by us and have the right to opt out of receiving these communications from us and our use of your information for such purposes.

Genetic Nondiscrimination Act (GINA): We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We will not disclose your PHI containing genetic information for underwriting purposes. GINA expressly prohibits the use or disclosure of genetic information for these purposes.

Breach of Unsecured Information: We will notify you should there be a breach of unsecured information. We are required to notify you if there is any acquisition, access, use, or disclosure of your unsecured PHI that compromises the security or privacy of your PHI.

Psychotherapy Information: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. Should it be applicable that your psychotherapy notes be included in an appropriate use or disclosure of information, in most instances, we are required to obtain your authorization for the release of this information.

Individual Rights

Access: You have the right to inspect and/or copy your PHI, with limited exceptions such as information a licensed health care professional, exercising professional judgment, determines that providing access is reasonably likely to endanger the life, physical safety or cause someone substantial harm. You may contact us using the telephone number on the back of your identification card to obtain a form to be completed and returned to us. If you request copies, we reserve the right to charge you a reasonable fee for each copy, plus postage if the copies are mailed to you.

Disclosure Accounting: You have the right to receive a list of instances in which we or our business associates disclosed your PHI. The list will not include disclosures we made for the purpose of treatment, payment, healthcare operations, disclosures made with your authorization, or certain other disclosures. To request a disclosure accounting you may contact us using the telephone number on the back of your identification card to obtain a form to be completed and returned to us. The request may not exceed a six year time period. We will provide you with the date on which we made the disclosure, the name of the person or entity to whom we disclosed your PHI, a description of the PHI we disclosed and the reason for the disclosure. If you request this list more than once in a 12-month period, we may charge you a reasonable, cost-based fee for responding to these additional requests.

Restriction Requests: You have the right to request that we place additional restrictions on our use or disclosure of your PHI. As permitted by law, we will not honor these requests, as it prohibits us from administering your benefits.

Confidential Communication: You have the right to request that we communicate with you confidentially about your PHI. We will honor a request to communicate to an alternative location if you believe you would be endangered if we do not communicate to the alternative location. We must accommodate your request if it is reasonable and specifies the alternative location. To request a form to be completed and returned to us, you may contact us using the telephone number on the back of your identification card.

Amendment: You have the right to request that we amend your PHI. Your request must be in writing, and it must explain why the information should be amended. We may deny your request if we did not create the information you want amended or if we determine the information is accurate. If we accept your request to amend the information, we will make reasonable efforts to inform others, including people you name, of the amendment and to include the changes in any future disclosures of that information. If we deny your request, we will provide you with a written explanation. You may respond with a statement of disagreement that will be attached to the information you wanted amended. You may contact us using the telephone number on the back of your identification card to obtain a form to be completed and returned to us.

Electronic Notice: If you receive this notice on our web site or by electronic mail (e-mail), you are entitled to receive this notice in written form. Please contact us using the contact information at the end of this notice to obtain this notice in written form.

Safeguards

It is our policy to keep all information about you confidential in all settings. It is so important to us that we take the following steps:

- our employees sign an agreement to follow our Code of Business Conduct;
- our employees are required to complete our privacy training program;
- we have implemented the necessary sanctions for violation of our privacy practices;
- we have a privacy oversight committee that reviews our privacy practices;
- we have a security coordinator to detect and prevent security breaches;
- all computer systems that contain personal information have security protections; and
- we randomly check provider offices on a routine basis to ensure that medical records are kept in secure locations.

Questions and Complaints

If you want more information about our privacy practices or have questions or concerns, please contact us using the contact information at the end of this notice.

If you are concerned that we may have violated your privacy rights, as described above, or you disagree with a decision we made about access to your PHI or in response to a request you made to amend or restrict the use or disclosure of your PHI or to have us confidentially communicate with you at an alternative location, you may complain to us using the contact information at the end of this notice. You also may submit a written complaint to the U.S. Department of Health and Human Services. We will provide you with the address to file your complaint with the U.S. Department of Health and Human Services upon request.

We support your right to protect the privacy of your PHI. We will not retaliate in any way if you choose to file a complaint with us or with the U.S. Department of Health and Human Services.

Privacy Rights or Questions:

Contact Office: Customer Service

Phone: Please call the telephone number on your identification card.

Privacy Complaints:

Contact Office: Privacy Officer
Address: 333 Butternut Dr.
Dewitt, NY 13214-1803

Phone: 1-866-584-2313

E-mail: privacy.officer@excellus.com

EXHIBIT H

Excellus

This is your

SimplyBlue PREFERRED PROVIDER ORGANIZATION CERTIFICATE OF COVERAGE

Issued by

EXCELLUS HEALTH PLAN, INC.
A nonprofit independent licensee of the BlueCross BlueShield Association

This Certificate of Coverage ("Certificate") explains the benefits available to you under a Group Contract between Excellus Health Plan, Inc. (hereinafter referred to as "we", "us", "our", or "the Plan") and the group contract holder listed in the Group Contract. This Certificate is not a contract between you and us. Amendments, riders or endorsements may be delivered with the Certificate or added thereafter.

This Certificate offers each person the option to receive covered services on two benefit levels:

In-Network Benefits. In-Network Benefits are the highest level of coverage available. In-Network Benefits apply when your care is provided by In-Network Providers. You should always consider receiving health care services first through the In-Network Benefits portion of this Certificate.

Out-of-Network Benefits. The Out-of-Network Benefits portion of this Certificate covers health care services described in this Certificate when you choose to receive the covered services from Out-of-Network Providers. When you receive Out-of-Network Benefits, you will incur higher out-of-pocket expenses. You will be responsible for meeting an annual Deductible and paying a higher Coinsurance amount, as well as for paying any difference between the Allowable Expense and the provider's charge.

READ THIS ENTIRE CERTIFICATE CAREFULLY. IT DESCRIBES THE BENEFITS AVAILABLE UNDER THE GROUP CONTRACT. IT IS YOUR RESPONSIBILITY TO UNDERSTAND THE TERMS AND CONDITIONS IN THIS CERTIFICATE.

EXCELLUS HEALTH PLAN, INC.
doing business as

Excellus BlueCross BlueShield
165 Court Street
Rochester, NY 14647

By: Christopher C. Booth

Christopher C. Booth
President and Chief Executive Officer

Excellus

165 Court Street
Rochester, New York 14647

A nonprofit independent licensee of the BlueCross BlueShield Association

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION.

PLEASE REVIEW IT CAREFULLY.

THE PRIVACY OF YOUR MEDICAL INFORMATION IS IMPORTANT TO US.

This notice takes effect April 14, 2003.

OUR COMMITMENT TO YOUR PRIVACY

We understand that medical information about you and your health is personal. We are committed to safeguarding your protected health information (PHI).

PHI is any information that can identify you as an individual and your past, present or future physical or mental health condition.

This notice will tell you about the ways in which we may use and disclose medical information about you. We also describe your rights and certain obligations we have regarding the use and disclosure of medical information. The law requires us to:

- make sure that PHI that identifies you is kept private;
- give you this notice of our legal duties and privacy practices with respect to PHI about you; and
- follow the terms of the notice that is currently in effect.

OUR LEGAL DUTY

We **(Excellus BlueCross BlueShield)** are required by applicable federal and state laws to maintain the privacy of your PHI. We are also required to give you this notice about our privacy practices, our legal duties, and your rights concerning PHI. We must follow the privacy practices that are described in this notice while it is in effect, including notification should there be a breach of your unsecured PHI.

We reserve the right to change our privacy practices and the terms of this notice at any time, provided that applicable law permits such changes. We reserve the right to make the changes in our privacy practices and the new terms of our notice effective for all PHI that we maintain, including medical information we created or received before we made the changes. Before we make a significant change in our privacy practices, we will change this notice and send the new notice to our health plan subscribers at the time of the change.

You may request a copy of our notice at any time. For more information about our privacy practices, or for additional copies of this notice, please contact us using the contact information at the end of this notice.

Uses and Disclosures of Nonpublic Personal Information

Nonpublic Personal Information is information you give us on your enrollment form, claim forms, premium payments etc. For example: names, member identification number, social security number, addresses, type of health care benefits, payment amounts, etc.

We will not give out your nonpublic personal information to anyone unless we are permitted to do so by law or have received a signed authorization form from the member. You may revoke this authorization in writing by completing an authorization cancellation form at any time. This revocation will not affect any actions we took in reliance on your authorization before your authorization cancellation form was processed.

Uses and Disclosures of Medical Information

The following categories describe different purposes for which we use and disclose PHI. For each category of uses or disclosures we will explain what we mean and try to give some examples. Not every use or disclosure in a category will be listed. However, all of the ways we are permitted to use and disclose information will fall within one of the categories. If we need to use or disclose your PHI in any other way, we will obtain your signed authorization before our use or disclosure. You may revoke this authorization in writing by completing an authorization cancellation form at any time. This revocation will not affect any actions we took in reliance on your authorization before your authorization cancellation form was processed.

Treatment: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may disclose PHI to doctors or hospitals involved in your care. For example, we may disclose your medications to an emergency room physician so that he/she can avoid dangerous drug interactions. This allows providers to manage, coordinate and administer treatment.

Payment: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may use and disclose PHI to collect premiums, to determine our responsibility to pay claims or to notify members and providers of our claim determinations. We may disclose PHI to providers to assist them in their billing and collection efforts. We may also disclose PHI to other insurance companies to coordinate the reimbursement of health insurance benefits. For example, we may disclose PHI to an automobile no- fault insurance company to determine responsibility for claim payment. Also, if you have health insurance through another insurance company, we may disclose PHI to that other health insurance company in order to determine which company holds the responsibility for your claims.

Healthcare Operations: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may use and disclose PHI for purposes of performing our healthcare operations. Our healthcare operations include using PHI to determine premiums, to conduct quality assessment and improvement activities, to engage in care coordination or case management, to determine eligibility for benefits. For example, we may use or disclose PHI when working with accreditation agencies that monitor and evaluate the quality of our benefit programs.

To You: We must disclose your PHI to you, as described in the Individual Rights section of this notice, below. We may also use and disclose PHI to tell you about recommended possible treatment options or alternatives or to tell you about health related benefits or services that may be of interest to you.

To Family and Friends: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. If you agree or, if you are unable to agree when the situation, (such as medical emergency or disaster relief), indicates that disclosure would be in your best interest, we may disclose PHI to a family member, friend or other person. In an emergency situation, we will only disclose the minimum amount necessary.

To Our Business Associates: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. A business associate is defined as someone that assists us in managing our business. For example, a professional that reviews the quality of our products and services. We may disclose PHI to another company that helps us manage our business. For example, we may disclose PHI to a company that performs case reviews to ensure our members receive quality care. These business associates are required to sign a confidentiality agreement with us that limits their use or disclosure of the PHI they receive.

To Plan Sponsors: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. A plan sponsor is defined as the employer or employee organization that establishes and maintains the employee's benefit plan. If you are enrolled in a group health plan, we may disclose PHI to the plan sponsor to permit the plan sponsor to perform plan administrative functions. For example, the cost analysis of the benefit program. Before PHI is disclosed to your plan sponsor, we will receive certification from the plan sponsor that appropriate amendments have been made to group health plan document(s) and the plan sponsor agrees to limit their use or disclosure of this information to plan administration functions only.

Research: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may use or disclose PHI for research purposes in limited circumstances. For example, a research project may involve comparing the health and recovery of all members who received one medication to those who received another medication for the same condition. All research projects are required to obtain special approval.

Coroners, Medical Examiners and Funeral Directors: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may release PHI to a coroner or medical examiner, to identify a deceased person or determine the cause of death. We may also release PHI about deceased members to funeral directors in order for the funeral directors to carry out their duties.

Organ Donation: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. If you are an organ donor, we may release PHI to organizations that handle organ procurement or organ, eye or tissue transplantation or to an organ donation bank, to facilitate organ or tissue donation and transplantation. This may include a living donor as well as a deceased donor.

Public Health and Safety: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may disclose PHI to the extent necessary to avert a serious and imminent threat to your health or safety, or the health or safety of others. We may disclose PHI to a government agency authorized to oversee the healthcare system or government programs or its contractors, and to public health authorities for public health purposes.

Victims of Abuse, Neglect or Domestic Violence: We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law. We may disclose PHI to appropriate authorities if we reasonably believe that you are a possible victim of abuse, neglect, domestic violence or other crimes.

Required by Law: **We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law.** We may use or disclose PHI when we are required to do so by law. For example, we must disclose PHI to the U.S. Department of Health and Human Services upon request to determine whether we are in compliance with federal privacy laws.

Process and Proceedings: **We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law.** We may disclose PHI in response to a court or administrative order, subpoena, discovery request, or other lawful process. Under limited circumstances, such as a court order, warrant, or grand jury subpoena, we may disclose PHI to law enforcement officials.

Law Enforcement: **We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law.** We may disclose PHI to a law enforcement official investigating a suspect, fugitive, material witness, crime victim or missing person. We may disclose PHI of an inmate or other person in lawful custody of a law enforcement official or correctional institution under certain circumstances.

Military and National Security: **We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law.** We may disclose to the military, PHI of Armed Forces personnel under certain circumstances. We may disclose to authorized federal officials medical information required for lawful intelligence, counterintelligence, and other national security activities.

Marketing and Fundraising: **We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law.** To the extent we use PHI for marketing or fundraising purposes, you will be contacted by us and have the right to opt out of receiving these communications from us and our use of your information for such purposes.

Genetic Nondiscrimination Act (GINA): **We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law.** We will not disclose your PHI containing genetic information for underwriting purposes. GINA expressly prohibits the use or disclosure of genetic information for these purposes.

Breach of Unsecured Information: **We will notify you should there be a breach of unsecured information.** We are required to notify you if there is any acquisition, access, use, or disclosure of your unsecured PHI that compromises the security or privacy of your PHI.

Psychotherapy Information: **We will not disclose PHI to an unauthorized person not involved in your care or treatment, unless we are required or permitted to do so by law.** Should it be applicable that your psychotherapy notes be included in an appropriate use or disclosure of information, in most instances, we are required to obtain your authorization for the release of this information.

Individual Rights

Access: You have the right to inspect and/or copy your PHI, with limited exceptions such as information a licensed health care professional, exercising professional judgment, determines that providing access is reasonably likely to endanger the life, physical safety or cause someone substantial harm. You may contact us using the telephone number on the back of your identification card to obtain a form to be completed and returned to us. If you request copies, we reserve the right to charge you a reasonable fee for each copy, plus postage if the copies are mailed to you.

Disclosure Accounting: You have the right to receive a list of instances in which we or our business associates disclosed your PHI. The list will not include disclosures we made for the purpose of treatment, payment, healthcare operations, disclosures made with your authorization, or certain other disclosures. To request a disclosure accounting you may contact us using the telephone number on the back of your identification card to obtain a form to be completed and returned to us. The request may not exceed a six year time period. We will provide you with the date on which we made the disclosure, the name of the person or entity to whom we disclosed your PHI, a description of the PHI we disclosed and the reason for the disclosure. If you request this list more than once in a 12-month period, we may charge you a reasonable, cost-based fee for responding to these additional requests.

Restriction Requests: You have the right to request that we place additional restrictions on our use or disclosure of your PHI. As permitted by law, we will not honor these requests, as it prohibits us from administering your benefits.

Confidential Communication: You have the right to request that we communicate with you confidentially about your PHI. We will honor a request to communicate to an alternative location if you believe you would be endangered if we do not communicate to the alternative location. We must accommodate your request if it is reasonable and specifies the alternative location. To request a form to be completed and returned to us, you may contact us using the telephone number on the back of your identification card.

Amendment: You have the right to request that we amend your PHI. Your request must be in writing, and it must explain why the information should be amended. We may deny your request if we did not create the information you want amended or if we determine the information is accurate. If we accept your request to amend the information, we will make reasonable efforts to inform others, including people you name, of the amendment and to include the changes in any future disclosures of that information. If we deny your request, we will provide you with a written explanation. You may respond with a statement of disagreement that will be attached to the information you wanted amended. You may contact us using the telephone number on the back of your identification card to obtain a form to be completed and returned to us.

Electronic Notice: If you receive this notice on our web site or by electronic mail (e-mail), you are entitled to receive this notice in written form. Please contact us using the contact information at the end of this notice to obtain this notice in written form.

Safeguards

It is our policy to keep all information about you confidential in all settings. It is so important to us that we take the following steps:

- our employees sign an agreement to follow our Code of Business Conduct;
- our employees are required to complete our privacy training program;
- we have implemented the necessary sanctions for violation of our privacy practices;
- we have a privacy oversight committee that reviews our privacy practices;
- we have a security coordinator to detect and prevent security breaches;
- all computer systems that contain personal information have security protections; and
- we randomly check provider offices on a routine basis to ensure that medical records are kept in secure locations.

Questions and Complaints

If you want more information about our privacy practices or have questions or concerns, please contact us using the contact information at the end of this notice.

If you are concerned that we may have violated your privacy rights, as described above, or you disagree with a decision we made about access to your PHI or in response to a request you made to amend or restrict the use or disclosure of your PHI or to have us confidentially communicate with you at an alternative location, you may complain to us using the contact information at the end of this notice. You also may submit a written complaint to the U.S. Department of Health and Human Services. We will provide you with the address to file your complaint with the U.S. Department of Health and Human Services upon request.

We support your right to protect the privacy of your PHI. We will not retaliate in any way if you choose to file a complaint with us or with the U.S. Department of Health and Human Services.

Privacy Rights or Questions:

Contact Office: Customer Service

Phone: Please call the telephone number on your identification card.

Privacy Complaints:

Contact Office: Privacy Officer
Address: 333 Butternut Dr.
Dewitt, NY 13214-1803

Phone: 1-866-584-2313

E-mail: privacy.officer@excellus.com

EXHIBIT I

Excellus

A nonprofit independent licensee of the Blue Cross Blue Shield Association

January 1 - December 31, 2014

Evidence of Coverage:

Your Medicare Health Benefits and Services and Prescription Drug Coverage as a Member of Medicare Blue Choice® Value (HMO)

This booklet gives you the details about your Medicare health care and prescription drug coverage from January 1 - December 31, 2014. It explains how to get coverage for health care services and prescription drugs you need. **This is an important legal document. Please keep it in a safe place.**

This plan, Medicare Blue Choice Value, is offered by Excellus BlueCross BlueShield. (When this *Evidence of Coverage* says "we," "us," or "our," it means Excellus BlueCross BlueShield. When it says "plan" or "our plan," it means Medicare Blue Choice Value.)

Excellus BlueCross BlueShield contracts with the federal government and is an HMO plan with a Medicare contract. Enrollment in Excellus BlueCross BlueShield depends on contract renewal.

Customer Service has free language interpreter services available for non-English speakers (phone numbers are printed on the back cover of this booklet).

Benefits, formulary, pharmacy network, premium, and/or copayments/coinsurance may change on January 1, 2015.

H3351_1533_5 Accepted
MCC-57Y14

Section 4.3 Can we change your monthly plan premium during the year?

No. We are not allowed to begin charging monthly plan premium during the year. If the monthly plan premium changes for next year we will tell you in September and the change will take effect on January 1.

However, in some cases, you may need to start paying or may be able to stop paying a late enrollment penalty. (The late enrollment penalty may apply if you had a continuous period of 63 days or more when you didn't have "creditable" prescription drug coverage.) This could happen if you become eligible for the "Extra Help" program or if you lose your eligibility for the "Extra Help" program during the year:

- If you currently pay the late enrollment penalty and become eligible for "Extra Help" during the year, you would be able to stop paying your penalty.
- If the "Extra Help" program is currently paying your late enrollment penalty and you lose your eligibility during the year, you would need to start paying your penalty.

You can find out more about the "Extra Help" program in Chapter 2, Section 7.

SECTION 5 Please keep your plan membership record up to date

Section 5.1 How to help make sure that we have accurate information about you

Your membership record has information from your enrollment form, including your address and telephone number. It shows your specific plan coverage including your Primary Care Provider.

The doctors, hospitals, pharmacists, and other providers in the plan's network need to have correct information about you. **These network providers use your membership record to know what services and drugs are covered and the cost-sharing amounts for you.** Because of this, it is very important that you help us keep your information up to date.

Let us know about these changes:

- Changes to your name, your address, or your phone number
- Changes in any other health insurance coverage you have (such as from your employer, your spouse's employer, workers' compensation, or Medicaid)
- If you have any liability claims, such as claims from an automobile accident
- If you have been admitted to a nursing home
- If you receive care in an out-of-area or out-of-network hospital or emergency room
- If your designated responsible party (such as a caregiver) changes
- If you are participating in a clinical research study

If any of this information changes, please let us know by calling Customer Service (phone numbers are printed on the back cover of this booklet).

It is also important to contact Social Security if you move or change your mailing address. You can find phone numbers and contact information for Social Security in Chapter 2, Section 5.

Read over the information we send you about any other insurance coverage you have

Medicare requires that we collect information from you about any other medical or drug insurance coverage that you have. That's because we must coordinate any other coverage you have with your benefits under our plan. (For more information about how our coverage works when you have other insurance, see Section 7 in this chapter.)

Once each year, we will send you a letter that lists any other medical or drug insurance coverage that we know about. Please read over this information carefully. If it is correct, you don't need to do anything. If the information is incorrect, or if you have other coverage that is not listed, please call Customer Service (phone numbers are printed on the back cover of this booklet).

SECTION 6 We protect the privacy of your personal health information

Section 6.1 We make sure that your health information is protected

Federal and state laws protect the privacy of your medical records and personal health information. We protect your personal health information as required by these laws.

For more information about how we protect your personal health information, please go to Chapter 8, Section 1.4 of this booklet.

SECTION 1 Our plan must honor your rights as a member of the plan

Section 1.1 We must provide information in a way that works for you (in languages other than English, in Braille, in large print, or other alternate formats, etc.)

To get information from us in a way that works for you, please call Customer Service (phone numbers are printed on the back cover of this booklet).

Our plan has people and free language interpreter services available to answer questions from non-English speaking members. We can also give you information in Braille, in large print, or other alternate formats if you need it. If you are eligible for Medicare because of a disability, we are required to give you information about the plan's benefits that is accessible and appropriate for you.

If you have any trouble getting information from our plan because of problems related to language or a disability, please call Medicare at 1-800-MEDICARE (1-800-633-4227), 24 hours a day, 7 days a week, and tell them that you want to file a complaint. TTY users call 1-877-486-2048.

Section 1.2 We must treat you with fairness and respect at all times

Our plan must obey laws that protect you from discrimination or unfair treatment. **We do not discriminate** based on a person's race, ethnicity, national origin, religion, gender, age, mental or physical disability, health status, claims experience, medical history, genetic information, evidence of insurability, or geographic location within the service area.

If you want more information or have concerns about discrimination or unfair treatment, please call the Department of Health and Human Services' **Office for Civil Rights** 1-800-368-1019 (TTY 1-800-537-7697) or your local Office for Civil Rights.

If you have a disability and need help with access to care, please call us at Customer Service (phone numbers are printed on the back cover of this booklet). If you have a complaint, such as a problem with wheelchair access, Customer Service can help.

Section 1.3 We must ensure that you get timely access to your covered services and drugs

As a member of our plan, you have the right to choose a primary care provider (PCP) in the plan's network to provide and arrange for your covered services (Chapter 3 explains more about this). Call Customer Service to learn which doctors are accepting new patients (phone numbers are printed on the back cover of this booklet). You also have the right to go to a women's health specialist (such as a gynecologist) without a referral.

As a plan member, you have the right to get appointments and covered services from the plan's network of providers *within a reasonable amount of time.* This includes the right to get timely services from specialists when you need that care. You also have the right to get your prescriptions filled or refilled at any of our network pharmacies without long delays.

If you think that you are not getting your medical care or Part D drugs within a reasonable amount of time, Chapter 9, Section 10 of this booklet tells what you can do. (If we have denied coverage for your medical care or drugs and you don't agree with our decision, Chapter 9, Section 4 tells what you can do.)

Section 1.4 We must protect the privacy of your personal health information

Federal and state laws protect the privacy of your medical records and personal health information. We protect your personal health information as required by these laws.

- Your "personal health information" includes the personal information you gave us when you enrolled in this plan as well as your medical records and other medical and health information.
- The laws that protect your privacy give you rights related to getting information and controlling how your health information is used. We give you a written notice, called a "Notice of Privacy Practice," that tells about these rights and explains how we protect the privacy of your health information.

How do we protect the privacy of your health information?

- We make sure that unauthorized people don't see or change your records.
- In most situations, if we give your health information to anyone who isn't providing your care or paying for your care, *we are required to get written permission from you first*. Written permission can be given by you or by someone you have given legal power to make decisions for you.
- There are certain exceptions that do not require us to get your written permission first. These exceptions are allowed or required by law.
  - For example, we are required to release health information to government agencies that are checking on quality of care.

- Because you are a member of our plan through Medicare, we are required to give Medicare your health information including information about your Part D prescription drugs. If Medicare releases your information for research or other uses, this will be done according to Federal statutes and regulations.

You can see the information in your records and know how it has been shared with others

You have the right to look at your medical records held at the plan, and to get a copy of your records. We are allowed to charge you a fee for making copies. You also have the right to ask us to make additions or corrections to your medical records. If you ask us to do this, we will work with your healthcare provider to decide whether the changes should be made.

You have the right to know how your health information has been shared with others for any purposes that are not routine.

If you have questions or concerns about the privacy of your personal health information, please call Customer Service (phone numbers are printed on the back cover of this booklet).

Section 1.5 We must give you information about the plan, its network of providers, and your covered services

As a member of Medicare Blue Choice Value, you have the right to get several kinds of information from us. (As explained above in Section 1.1, you have the right to get information from us in a way that works for you. This includes getting the information in languages other than English and in large print or other alternate formats.)

If you want any of the following kinds of information, please call Customer Service (phone numbers are printed on the back cover of this booklet):

- **Information about our plan.** This includes, for example, information about the plan's financial condition. It also includes information about the number of appeals made by members and the plan's performance ratings, including how it has been rated by plan members and how it compares to other Medicare health plans.
- **Information about our network providers including our network pharmacies.**
  - For example, you have the right to get information from us about the qualifications of the providers and pharmacies in our network and how we pay the providers in our network.
  - For a list of the providers and/or pharmacies in the plan's network, see the *Provider/Pharmacy Directory*.
  - For more detailed information about our providers or pharmacies, you can call Customer Service (phone numbers are printed on the back cover of this booklet) or visit our website at www.excellusbcbs.com/medicare.
- **Information about your coverage and rules you must follow in using your coverage.**
  - In Chapters 3 and 4 of this booklet, we explain what medical services are covered for you, any restrictions to your coverage, and what rules you must follow to get your covered medical services.
  - To get the details on your Part D prescription drug coverage, see Chapters 5 and 6 of this booklet plus the plan's *List of Covered Drugs (Formulary)*. These chapters, together with the *List of Covered Drugs (Formulary)*, tell you what drugs are covered and explain the rules you must follow and the restrictions to your coverage for certain drugs.
  - If you have questions about the rules or restrictions, please call Customer Service (phone numbers are printed on the back cover of this booklet).
- **Information about why something is not covered and what you can do about it.**
  - If a medical service or Part D drug is not covered for you, or if your coverage is restricted in some way, you can ask us for a written explanation. You have the right to this explanation even if you received the medical service or drug from an out-of-network provider or pharmacy.
  - If you are not happy or if you disagree with a decision we make about what medical care or Part D drug is covered for you, you have the right to ask us to change the decision. You can ask us to change the decision by making an appeal. For details on what to do if something is not covered for you in the way you think it should be covered, see Chapter 9 of this booklet. It gives you the details about how to make an appeal if you want us to change our decision. (Chapter 9 also tells about how to make a complaint about quality of care, waiting times, and other concerns.)
  - If you want to ask our plan to pay our share of a bill you have received for medical care or a Part D prescription drug, see Chapter 7 of this booklet.