BURR FORMAN LLP

Don't Get Caught Red-Handed: Update Your HIPAA Compliance Efforts to Avoid Penalties

HLA Alabama

July 22, 2025

KELLI C. FLEMING, ESQ.
(205) 458-5429
KFLEMING@BURR.COM

1

1

2

2

Agenda

1. HIPAA Overview
2. Enforcement Action Trends
3. Additional Hot Topics

3

HIPAA Overview

4

What Is HIPAA

- Health Insurance Portability and Accountability Act of 1996
- Privacy Rules and Security Rules – Regulations found at 45 C.F.R. Parts 160 and 164
  - Focus on privacy aspects in training
- Strengthened and expanded by the Health Information Technology for Economic and Clinical Health ("HITECH") Act

5

Who Is Directly Covered By HIPAA?

"Covered Entities"

- Healthcare providers: persons or entities who furnish, bill or are paid for health care services in the normal course of business. (Examples include: physician practices, hospitals, skilled nursing facilities, surgery centers, home health agencies, pharmacies, and durable medical equipment providers)
- Health plans: individual or group plans that provide or pay the cost of medical care. (Examples include: HMOs, private health insurers, group health plans, and employee welfare benefit plans)
- Health care clearinghouses: entities that process protected health information in a non-standard HIPAA format or containing non-standard data into a standard format. (Examples include: health care billing companies)

6

Where Is Protected Health Information Found?

- Medical Records
- Health Plan Claims
- Practice Management System
- E-mails
- Texts
- Word Documents
- Apps
- Faxes

7

What Information Is Not Protected Under HIPAA?

- De-Identified Health Information. There are no restrictions on the use or disclosure of de-identified health information. De-identified health information neither identifies nor provides a reasonable basis to identify an individual. There are two ways to de-identify information; either: (1) a formal determination by a qualified statistician; or (2) the removal of specified identifiers of the individual and of the individual's relatives, household members, and employers.
- PHI in employment records that a covered entity maintains in its capacity as an employer.
- Education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g.
- Records involving a person who has been deceased for more than 50 years.

8

HIPAA Compliance Plan

- Each covered entity should have a HIPAA Compliance Plan that addresses the permitted uses and disclosures of PHI.
- Make accessible to everyone impacted.
- Review and update periodically.
- Train workforce on policies and procedures.
- Appoint Privacy and Security Officer

9

What Does the HIPAA Compliance Plan Address?

- Manner in which PHI may be used or disclosed by a Covered Entity (Privacy Rules):
  1. To the individual (or personal representative)
  2. For treatment, payment and health care operations ("TPO")
  3. After opportunity by the individual to agree/object
  4. "Public policy" purposes
  5. With Written Authorization
  6. With a Business Associate Agreement

10

What Does the HIPAA Compliance Plan Address?

- Manner in which individuals may exercise their patient rights:
  1. Right to Access
  2. Right to Amend
  3. Right to Accounting
  4. Right to Request Restrictions
  5. Right to NPP

11

What Does the HIPAA Compliance Plan Address?

- Manner in which PHI must be secured by a Covered Entity (Security Rules)
  - Access Controls
  - Device Controls
  - Audit Controls
  - Security Management
  - Security Controls
  - Security Evaluation
  - Security Training
  - Incident Responses

12

Enforcement Actions and Trends

13

HIPAA Enforcement In General

- Enforced by the HHS Office for Civil Rights
- Investigations initiated based on filed complaints, HIPAA breach reports, referrals from other agencies, and OCR's own initiative
  - 794 cases under investigation by OCR
- Penalties can encompass no action, written technical guidance, corrective action, monetary penalties, and criminal penalties

14

Recent HIPAA Enforcement Actions

- $135,223,772.00 in civil monetary penalties imposed for HIPAA violations
- In 2024, 725 breach reports affecting more than 500 individuals were filed
- Number of HIPAA complaints increasing each year

15

Topics From Recent Enforcement Actions

1. Cyberattacks
2. Risk Analysis
3. Right to Access
4. Unauthorized Access

16

Cyberattacks Enforcement Actions

17

Image from The New Yorker

18

Cyberattacks Enforcement Action

- Comstar, LLC (May 30, 2025)
  - 13th ransomware enforcement action
  - Business Associate (billing and coding)
  - Ransomeware attack impacted 585,621 individuals (Occurred in March, 2022, detected a week later).
    - How quickly must you detect?
  - No risk analysis conducted
  - Enter into CAP and pay $75,000 fine
    - Conduct risk analysis
    - Develop risk management plan
    - Revise policies and procedures
    - Conduct training

19

Cyberattacks Enforcement Action

- Vision Upright MRI (May, 2025)
  - 21,778 individuals impacted
  - Failed to conduct risk analysis and notify of breach
  - CAP and $5,000
    - Provide breach notification
    - Conduct risk analysis
    - Develop risk management plan
    - Develop written policies and procedures
    - Provide training

20

Cyberattacks Enforcement Action

- PIH Health (health network) (April 23, 2025)
  - Reported breach in January, 2020 (incident occurred in June, 2019)
  - Impacted 45 employees accounts
  - 189,763 individuals impacted
  - Failed to use/disclose PHI only as permitted, failed to conduct a risk analysis, failed to notify individuals
  - CAP and $600,000 penalty
    - Conduct risk analysis
    - Develop risk management plan
    - Revise policies and procedures
    - Train

Cyberattack Enforcement Action

- Guam Memorial Hospital Authority (April, 2025)
  - 2 complaints concerning a ransomware incident impacting 5,000 patients
  - Failed to conduct risk analysis
  - CAP and $25,000 penalty
    - Conduct risk analysis
    - Develop risk management plan
    - Develop process to review records of system activity
    - Develop and revise policies and procedures
    - Revise training program
    - Enhance workforce security and information access management and review all access credentials that have been granted
    - Conduct breach risk assessments and provide breach notice

Cyberattack Enforcement Action

- Warby Parker (February 20, 2025)
  - Breach report received in December, 2018
  - Unauthorized access achieved by using usernames and passwords from other unrelated websites that were breached. "Credential Shuffling"
  - 197,986 individuals impacted
  - $1,500,000 penalty
  - Failed to conduct risk analysis, failed to implement security measures, and failed to implement processes to review information system activity.

Cyberattacks: In General

- Phishing e-mails
- Brute force attack
- Credential Shuffling
- Business e-mail compromise
- Ransomware

Why Cyberattacks?

- Cyberattacks are the cause of the majority of breaches
  - 70% of the U.S. population has been affected by at least 1 data breach
- 52% of small businesses (less than 100 employees) have experienced a cyberattack in the previous year
- Change impacted 190 million individuals
- Ransomware hit 141 hospitals in 2023. Average ransom was $1.5 million
- Targeted smaller hospitals, rural health clinics, and physician practices
  - Don't have the resources or funds to address, so easy targets
  - Smaller staff
  - Vulnerability for patient care—no where else to go if rural

25

Why Cyberattacks?

- Why?
  - Records are valuable
    - Breached healthcare information is 50 times more valuable than financial information.
  - Records contain vast amount of personal information that can be used for blackmail, identity theft, fraudulent insurance claims, obtaining drugs.
  - Data takes many forms in multiple databases
  - Oftentimes remain undeleted for weeks/months

26

Preventing Cyberattacks & Related Penalties

- Training
- 2-factor authentication on all remote and admin access
- Strong firewalls, anti-virus, and spam detection systems
- Timely patching and updates
- Encryption and mobile device management
- Strong passwords and change frequently and in response to an event; auto lock-out
- Audit logs and security measures
- Risk analysis & management
- Incident Response

27

Cyberattack Response and Aftermath

- OCR Notices (covered entity or business associate)
  - Patient
  - Website
  - Media
  - OCR
- State Regulatory Notices
- Litigation (including class actions)
- Cyber-Liability Insurance
- PR
- Malpractice Implications. 36% of facilities report increased medical complications from ransomware attacks.

28

Breach Response – Documentation

- Breach Assessment: who, what, when, where and why?
- Summary of mitigation efforts and operational changes
- Logs, reports, etc.
- IT reports
- Consultant report
- Attorney summary
- Insurance policy/coverage correspondence
- Notification documents: individuals, AG, media, OCR
- FBI report/disclosure
- Police report

OCR Guidance Document—CyberSecurity

- https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html
- Video on How to Defend Against Cyberattacks
  - OCR Breach and Investigation Trends
  - Common Attacks
  - Weaknesses that Led to Attacks
  - How Security Rule Compliance Can Assist
  - Cybersecurity Checklist
  - Steps to Respond to an Attack

OCR Guidance Document—CyberSecurity Continued

- Ransomware Guidance
  - What is ransomware?
  - How to respond to an attack.
  - What is reportable?
- Cybersecurity Newsletters
  - Quarterly
  - Sign-up at https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/cybersecurity-newsletter-archive/index.html

31

OCR Guidance Document—CyberSecurity Continued

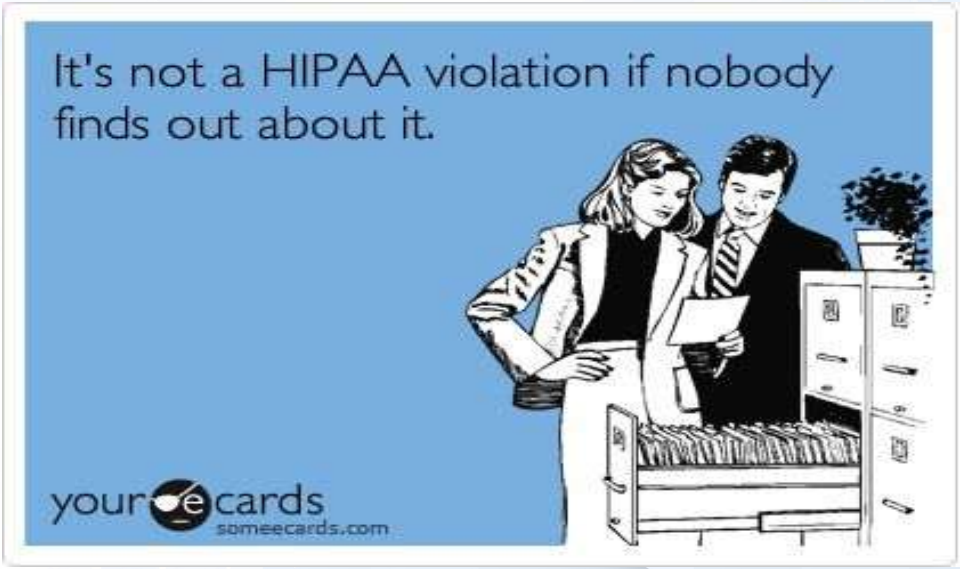
- OCR Audits (issued December, 2024)
  - Auditing 50 entities. Voluntary, but with some risk.
  - Focused on responding to cyberattacks.
  - Do you have written policies? Are they reviewed and updated? Are they implemented?

32

Cyberattacks—OCR Recommendations

- Identify where PHI is located, how it enters, flows through, and leaves the system
- Conduct risk analysis and risk management as part of business processes
- Enact audit controls
- Implement regular reviews of information system activity
- Utilize mechanisms to authenticate information to ensure only accessed by authorized users
- Encrypt PHI in transit and at rest to guard against unauthorized access
- Incorporate lessons learned from incidents into security management process
- Provide regular training specific to entity and job responsibilities

33



34

Risk Analysis Enforcement Actions

35

Risk Analysis Enforcement Action

- Comprehensive Neurology, PC (April, 2025)
  - Ransomware attack impacting 6800 patients (occurred in 2020)
  - Investigated following a breach report of ransomware
  - 1 physician practice
  - No risk analysis
  - CAP and $25,000 penalty
    - Conduct Risk Analysis
    - Develop Risk Management Plan
    - Revise Policies and Procedures
    - Train

36

Risk Analysis Enforcement Action

- Northeast Radiology, P.C. (April 10, 2025)
  - Breach report filed in March, 2020
  - Unauthorized access to images on system
  - 298,532 patients
  - Failed to conduct risk analysis
  - CAP and $350,000 penalty
    - Conduct risk analysis
    - Develop risk management plan
    - Develop process to review records of information system activity
    - Revise policies
    - Train

37

Risk Analysis Enforcement Action

- Health Fitness Corporation (March 21, 2025)
  - Business Associate
  - 4,304 individuals
  - 3 reports filed concerning breaches of PHI between 2018 and 2019
  - PHI exposed on the internet and exposed to search engines
  - Failed to conduct risk analysis
  - CAP and $227,816 penalty
    - Review and update risk analysis
    - Develop risk management plan
    - Implement process to evaluate environment and operational changes
    - Develop policies

38

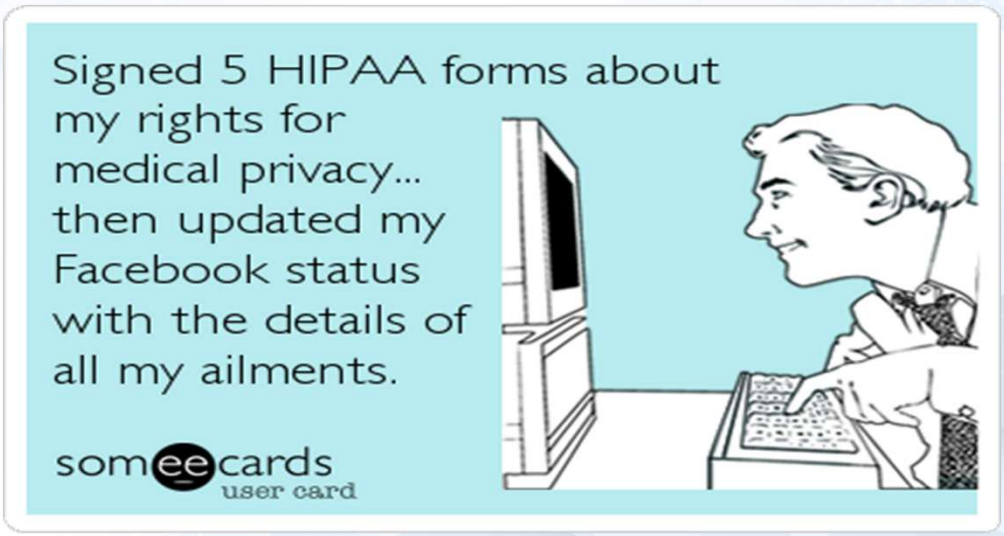
Risk Analysis

- Must have an updated, thorough risk analysis on file—in writing.
- Anytime a new system or new software is added, you should update the risk analysis.
- Anytime a procedure is changed materially, you should update the risk analysis.
- Can do internally or can hire third-party.
- OCR and ONC (Office of National Coordinator) have issued a security risk analysis tool for small and medium size providers. https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html?language=es
- Oftentimes requested in OCR investigation.
- Need to review and address risky areas that result from analysis.

39

Right to Access Enforcement Actions

40



41

Right to Access Enforcement Actions

- Oregon Health & Science University (March 6, 2025)
  - 53rd Decision under Right to Access Initiative (22 in 2024)
  - Complaint in January, 2021 from patient that records were not timely provided
  - $200,000 penalty

42

Right To Inspect And Copy PHI

- An individual has a right of access to inspect and/or copy PHI in a Covered Entity's "designated record set."
- Includes right to inspect, obtain a copy, and direct the Covered Entity to transmit a copy to a designated person or entity of the individual's choice.
- Must provide the individual with access to the PHI in the form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable hard copy form or such other form and format as agreed to by us and the individual.
- Limited on what you can charge for the information.
- 30 days to respond (one 30-day extension)

43

Right To Inspect And Copy PHI

- Fees - If a patient requests a copy of their PHI, you may impose a reasonable cost-based fee, provided that the fee includes only the cost of:
  - Labor for copying the PHI requested, whether in paper or electronic form;
  - Supplies for creating the paper copy or electronic media if the patient requests that the electronic copy be provided on portable media;
  - Postage, when the individual has requested that the copy, summary or explanation be mailed.

44

Right To Inspect And Copy PHI: Copy Charges

- Flat fee of up to $6.50 (electronic) or reasonable, cost-based fee.
- Two Options when calculating labor costs for cost-based fee.
  - Actual Costs. A covered entity may calculate actual labor costs to fulfill the request, as long as the labor included is only for copying and the labor rates used are reasonable for such activity.
  - Average costs. In lieu of calculating labor costs individually for each request, a covered entity can develop a schedule of costs for labor based on average labor costs to fulfill standard types of access requests, as long as the types of labor costs included are permitted (*e.g.*, labor costs for copying but not for search and retrieval) and are reasonable.

Right To Inspect And Copy PHI: Copy Charges For Labor Costs

- Labor for copying includes only labor for creating and delivering the electronic or paper copy in the form and format requested or agreed upon by the individual, once the PHI that is responsive to the request has been identified, retrieved or collected, compiled and/or collated, and is ready to be copied.
- Labor for copying does not include costs associated with reviewing the request for access; or searching for and retrieving the PHI, which includes locating and reviewing the PHI in the medical or other record, and segregating or otherwise preparing the PHI that is responsive to the request for copying, even if by state law.

Right To Inspect And Copy PHI: Copy Charges When Outsourcing

- Administrative and other costs associated with outsourcing the function of responding to individual requests for access cannot be the basis for any fees charged to individuals for providing that access.
- Business associates responding on your behalf are limited to the charges you are allowed to charge.

47

Right To Inspect And Copy PHI: Copy Charges For Electronic Copies

- For any request from an individual for electronic copies, a covered entity may calculate the allowable fees for providing individuals with copies of their PHI:
  1. by calculating actual allowable costs to fulfill each request; or
  2. by using a schedule of costs based on average allowable labor costs to fulfill standard requests, or;
  3. by charging a flat fee not to exceed $6.50 (inclusive of all labor, supplies, and postage).
- Charging a flat fee not to exceed $6.50 per request is an option available to entities that do not want to calculate actual or average allowable costs for requests for electronic copies of PHI maintained electronically.
- Per page fees are not allowed if the PHI is maintained electronically.
- No fee for using View, Download, and Transmit function of EMR.

48

Right To Inspect And Copy PHI: Miscellaneous

- OCR recommends not charging fees at all. (Encouraged, but not required.)
- Need to inform individual upfront about estimated fees charged.
- Cannot create a barrier to access or unreasonably delay.
- Only send unencrypted e-mail containing PHI if inform individual of risk and individual still requests such form of delivery.

49

50

Improper Access Enforcement Actions

51

Improper Access Enforcement Actions

- Deer Oaks – The Behavioral Health Solution (July, 2025)
  - Patient complained that patient discharge summaries were available online publicly
  - December, 2021 – May, 2023
  - Due to coding error with patient portal.
  - 35 patients.
  - Second incident involvoing ransomware and impacting 171,871 individuals
    - Agreed to CAP and pay $225,000
    - Risk analysis
    - Risk management plan
    - Revise policies and procedures
    - Train workforce

52

Improper Access Enforcement Actions

- BayCare Health System (May 28, 2025)
  - Patient complained in October, 2018 after unknown person contacted her and had copies of her medical records (video and photos)
  - Accessed by former employee of medical staff member
  - Failed to implement policies and procedures for authorized access, failing to reduce risks and vulnerabilities, failing to regularly review records for system activity.
  - Agreed to CAP and pay $800,000
    - Conduct risk analysis
    - Develop risk management plan
    - Revise policies and procedures
    - Train workforce

Improper Access Enforcement Actions

- Office for Civil Rights Settles Disclosure of PHI to News Reporter (11/20/2023)
  - Disclosure of COVID-related PHI to media outlet
    - Article included photographs and information about patients
    - No authorization obtained
  - $80,000 penalty and agree to CAP

Access Takeaways

- Terminate credentials immediately upon termination
- No media in practice/onsite
- Marketing authorizations obtained
- Social media woes

55

Hot Topics & Updates

56

Hot Topics & Updates

1. Reproductive Health
2. Tracking Technologies
3. Business Associate Agreements
4. Regulatory Guidance
5. Age of Consent

57

Reproductive Health Rules

- The Final Rule became effective on June 25, 2024, with a December 23, 2024 compliance date.
- PHI concerning reproductive healthcare shall not be used or disclosed to:
  - Criminally, civilly, or administratively investigate or impose liability on anyone who seeks, obtains, provides or facilitates reproductive healthcare that is lawful; or
  - Identify persons engaged in lawful reproductive healthcare-related activities.

58

Disclosure Of Reproductive Health Information - Attestation

- If a request for PHI potentially related to reproductive healthcare is received for the following purposes, a valid, signed attestation form must also be received from the requester:
  - Health oversight activities;
  - Judicial and administrative proceedings;
  - Law enforcement purposes; or
  - Disclosures to coroners or medical examiners.
- New attestation form is required for each disclosure.
- Also required revisions to policies and procedures, as well as Notice of Privacy Practices

Reproductive Health Rules Vacated

- On June 18, 2025, a federal district court in Texas vacated the Reproductive Health Rules nationwide.
  - Unlawfully limits state public health
  - Impermissibly defines person and public health in contravention of federal law and in excess of statutory authority
  - Was adopted without authority delegated by Congress
  - Nullified the rule effective immediately. No need to comply and no longer subject to enforcement. OCR confirmed attestation no longer needed.
  - Applies nationwide
  - TBD if an appeal will be filed or if intervention allowed. Could also have a circuit split.

Tracking Technologies

A tracking technology is used to collect information about how online users interact with websites or mobile applications (*e.g.*, Google Analytics). Can include collection or disclosure to vendors or PHI.

- OCR Issued Guidance Regarding Tracking Technologies – twice.
- Enter in a Business Associate Agreement ("BAA") with the vendor, or obtain patient authorization for such use and/or disclosure.
    - Disclosing PHI to tracking technology vendors based solely on informing individuals of such use in the website's privacy policy or terms of use is not sufficient, nor is merely accepting or rejecting cookie use.
- Use of PHI must be permissible. Think about marketing and authorization requirement
- Individually identifiable information "collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the [information] does not include specific treatment or billing information like dates and types of healthcare services."

61

Tracking Technologies

Guidance Resulted in Class Actions Against Healthcare Providers

- Can cookies tied to computer in another state subject you to that state's laws?

Guidance Vacated by a Court Order.

- The U.S. District Court for the Northern District of Texas issued an order declaring unlawful and vacating a portion of this guidance document.
- Specifically, the Court vacated the guidance to the extent it provides that HIPAA obligations are triggered in "circumstances where an online technology connects (1) an individual's IP address with (2) a visit to a[n] [unauthenticated public webpage] addressing specific health conditions or healthcare providers."
    - Unauthenticated means no log-in
    - Tracking on authenticated webpages is still prohibited unless in compliance with HIPAA
- HHS is evaluating its next steps in light of that order.

62

Business Associate Agreements

- Must enter into Business Associate Agreements with any business associate prior to disclosing PHI
- Sets out permitted uses and disclosures of our PHI
- Topics covered include minimum access to PHI, how to respond to a breach incident, access/amendment/accounting, indemnity, use and disclosure, de-identification, safeguards, and subcontractors.
- Several OCR penalties recently for not getting a BAA or for having a BAA that has not been updated.
- OCR recommends reviewing to make sure breach notification is properly addressed

63

Regulatory Initiatives

- Proposed Cybersecurity Rule
  1. Issued December 27, 2024
  2. Response to Increasing Number of Cyberattacks
     1. Between 2018-2023, large breaches reports increased by 102% (namely from cyber incidents).
     2. OCR noticed common deficiencies
     3. Align with other cybersecurity best practices
     4. Transitioned how care is received, delivered, and documented
  3. Strengthen security protections for PHI
  4. More Specific Requirements

64

Regulatory Initiatives

- HITECH Request for Information
  1. Issued April 6, 2022
  2. Two Areas of Interest
     - Recognized Security Practices When Determining Fines, Penalties, Etc.
     - CMP and Settlement Sharing with Harmed Individuals

65

Age of Consent in Alabama

- Ala. Code 22-8-4 amended to increase the age of consent in Alabama from 14 to 16.
- Effective October 1, 2025.
- Parents have access to minors records and health information if they request such records or information until the child reaches the age of 19. Few exceptions.
- Interplay with HIPAA.

66

How to Avoid a HIPAA Violation/Enforcement Action

- Implement HIPAA Policies and Procedures
- Train Employees Periodically
- Follow Appropriate Privacy and Security Safeguards
- Pay Attention to Trends From OCR
- Instill a Culture of Compliance from Top Down
- Put HIPAA on Forefront of Everyone's Mind
- Think Before You Act

67

Our Footprint

Atlanta	Jackson
Birmingham	Jacksonville
Bluffton	Mobile
Charleston	Montgomery
Charlotte	Myrtle Beach
Chicago	Nashville
Columbia	Orlando
Daniel Island	Raleigh
Ft. Lauderdale	Tampa
Greenville	Washington, D.C.
Hilton Head	Wilmington

BURR & FORMAN

68