ROSALIND FRANKLIN UNIVERSITY
HealthClinics

CATEGORY –COMPLIANCE AND RISK MANAGEMENT

HIPAA Privacy Rule

REVISED DATE 03-17-2017

INTRODUCTION & PURPOSE

All members of the Health Clinics workforce shall comply with the HIPAA Privacy Rule and the related Health Clinics policies and procedures, all of which are designed to protect the privacy and confidentiality of PHI that is either transmitted or maintained by the Health Clinics. Violations are prohibited and may result in sanctions, up to and including termination.

Any person seeking guidance or who becomes aware of any potential, known, or suspected violation of this policy shall contact the Privacy Officer, who shall take proper action to address the situation. The Privacy Officer shall document all reported violations of this policy using the Health Clinics Incident Report.

As an alternative, reports may be made to the Office of Compliance of RFUMS directly or through EthicsPoint, Inc. (by either going to the EthicsPoint website at http://rosalindfranklin.ethicspoint.com or dialing the toll-free telephone number of 1-800-254-0460) which allows anonymity, or to the U.S. Department of Health and Human Services. No person will be subjected to retaliation, retribution, or reprisal for making a good faith report of, seeking guidance regarding, or participating in the investigation or resolution of a potential, known, or suspected violation of this policy.

SCOPE & APPLICABILITY

This policy is applicable to all members of the Rosalind Franklin University Health Clinics workforce.

DEFINITIONS

Disclose. To disclose PHI means the release, transfer, provision of access to, or divulging in any manner PHI outside the Health Clinics (i.e. to someone other than a member of the Health Clinics workforce).

Genetic Information. *Information, other than sex or age, about (1) the individual's genetic tests; (2) the genetic tests of family members of the individual; (3) the manifestation of a disease or disorder in family members of such individual; or (4) any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by the individual or any family member of the individual.*

Note: For purposes of this definition, genetic information about an individual or family member includes genetic information of a fetus carried by the individual and of an embryo lawfully held by an individual or family member utilizing assisted reproductive technology.

Note: For purposes of this definition, genetic test means an analysis of human DNA, RNA, chromosomes, proteins, or metabolites, if the analysis detects genotypes, mutations, or chromosomal changes. Genetic test does not include an analysis of proteins or metabolites that is directly related to a manifested disease, disorder, or pathological condition.

Note: For purposes of this definition, genetic services means (1) a genetic test, (2) genetic counseling (including obtaining, interpreting, or assessing genetic information); or (3) genetic education.

PHI or protected health information - Information, including genetic information, whether oral or recorded in any form or medium that (1) was created or received by the Health Clinics, (2) identifies the individual (or is capable of identifying the individual), and (3) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual. The term does *not* include certain education records described in the Family Educational Rights and Privacy Act (FERPA), employment records held by the Health Clinics in its role as employer, or information regarding a person who has been deceased for more than 50 years.

Privacy Officer - The Health Clinics employee who is designated in writing as the Privacy Officer and will have authority to and is responsible for the development and implementation of procedures that promote compliance with this policy and the HIPAA Privacy Rule. The Privacy Officer will also be responsible to receive complaints and provide information relating to the HIPAA Privacy Rule as well as the Health Clinics Notice of Privacy Practices (NOPP).

Use. To use PHI means a member of the Health Clinics workforce either utilizes the PHI him/herself or shares the PHI with another member of the Health Clinics workforce.

Workforce - All employees of the Health Clinics, all volunteers of the Health Clinics, all trainees (including university students) that are engaged in training activities at the Health Clinics or under the cognizance of the Health Clinics, and all persons whose conduct is under the direct control of the Health Clinics.

PROCEDURES

OVERVIEW
(CONTENTS OF PROCEDURES SECTION)

Permitted Uses and Disclosures of Health Information
- Treatment, Payment, and Health Care Operations (TPO)
- Written Authorization
- Those Involved in Care or Payment ~or~ for Notification Purposes
- Child Abuse or Neglect

Victims of Abuse, Neglect, or Domestic Violence
Victims of Crime
Court Order, Subpoena, or Other Similar Written Demand
Identification of Locating Suspect, Fugitive, Material Witness, or Missing Person
Coroners and Medical Examiners
Crime on Premises of the Health Clinics
To Avert Threat to Health or Safety of Person or the Public
To Control Disease, Injury, or Disability
For Workers Compensation Purposes
Research Purposes - Waiver of Authorization
Research Purposes - Preparatory to Research
Research Purposes - Limited Data Set
Other Reasons

General Rules Applicable to Using and Disclosing Health Information
Role-Based Access
Minimum Necessary
Verification
Personal Representative

Safeguarding Health Information
General Rule
Incidental Uses or Disclosures
Medical Record Storage

Patient Rights
Notice of Privacy Practices (NOPP)
Right of Access to PHI
Right to Amend PHI
Right to Receive an Accounting of Disclosures of PHI
Right to Request Further Restrictions
Right to Request Alternate Confidential Communications

Administrative and Miscellaneous Provisions
Breach and Related Notification Procedures
Modifications to HIPAA Policies and Procedures
Document Retention
De-Identified Health Information
Business Associates and Business Associate Agreements (BAA)
Training for Workforce

PERMITTED USES AND DISCLOSURES OF HEALTH INFORMATION

Note: The HIPAA Privacy Rule is a law of general applicability and is the primary legal source for these provisions. Illinois laws may exist that impose greater limitations on the permissiveness of using or disclosing certain types of health information. One such law that is applicable to the Health Clinics is the Illinois Mental Health and Developmental Disabilities Confidentiality Act (740 ILCS 110). While efforts were made to identify areas of applicability of those laws in the main text of the manual, a copy of that law is also included in the appendix and members of the Health Clinics should refer to that when applicable.

Members of the Health Clinics workforce may *not* request PHI, use PHI, or disclose PHI *unless* that specific use or disclosure is permitted by these provisions, which are intended to reflect current federal and Illinois laws.

Treatment, Payment, and Health Care Operations (TPO).

1. Treatment.

   a. A member of the workforce of the Health Clinics may use or disclose PHI for "treatment activities" of the Health Clinics.

   b. A member of the workforce of the Health Clinics may use or disclose PHI for "treatment activities" of another health care provider.

   Treatment activities *mean activities related to the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.*

2. Payment.

   a. A member of the workforce of the Health Clinics may use or disclose PHI for "payment activities" of the Health Clinics.

   b. A member of the workforce of the Health Clinics may use or disclose PHI for "payment activities" of another health care provider or group health plan.

   Payment activities *mean activities of a health care provider or health plan to obtain or provide reimbursement for the provision of health care or activities of a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan. Examples include determinations of eligibility or coverage, adjudication of claims, risk adjusting, billing, claims management, collection activities, obtaining payment under a contract for reinsurance, and related health care data processing, medical necessity review, utilization review, and disclosure of certain limited information to consumer reporting agencies.*

3. Health Care Operations.

a. A member of the workforce of the Health Clinics may use or disclose PHI for health care operations activities of the Health Clinics.

b. A member of the workforce of the Health Clinics may use or disclose PHI for health care operations activities of another health care provider or a group health plan, so long as all of the following are fulfilled:

(1) the other health care provider or the group health plan has or had a relationship with the individual (*i.e.* the person about whom the PHI relates), and
(2) the PHI being requested pertains to that relationship, and
(3) the disclosure is only for those activities listed in paragraphs a. or b. of the definition of health care operations activities (see below).

c. When participating in an organized health care arrangement (OHCA) (as that concept is described in the HIPAA Privacy Rule), a member of the workforce of the Health Clinics may use or disclose PHI to another health care provider or group health plan that participates in that same OHCA for any health care operations activities of that OHCA.

Health care operations activities *mean any of the following activities to the extent it relates to the status of health provider or health plan:*

a. Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in 42 CFR 3.20); population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

b. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;

c. Underwriting (however, a health plan shall not use or disclose PHI that is genetic information for underwriting purposes), enrollment, premium rating, and other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of § 164.514(g) are met, if applicable;

d. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

e. Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

f. Business management and general administrative activities of the entity, including, but not limited to:

(i)Management activities relating to implementation of and compliance with the requirements of the HIPAA Privacy Rule;
(ii) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer.
(iii) Resolution of internal grievances;
(iv)The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and
(v)Consistent with the applicable requirements of §164.514, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.

Written Authorization.

1. Health Clinics Form. A member of the workforce of the Health Clinics may use or disclose PHI consistent with the terms of a properly completed Health Clinics Written Authorization Form.

2. Another's Form. A member of the workforce of the Health Clinics may use or disclose PHI consistent with the terms of a completed written authorization form, so long as the form, as submitted, contains all of the required elements of the Health Clinics Written Authorization Checklist.

3. Forms. The complete list of forms, templates, and checklists may be found in the appendix.

Note: Illinois law at 740 ILCS 110/5 provides for additional required contents of an authorization (termed "consent" by that law) when the information is mental health information. The Health Clinics has a form specifically tailored for mental health information. In such a case, use of another's form may be accomplished after utilization of the general HIPAA Privacy Rule Written Authorization Checklist along with reference to the law cited above.

Those Involved in Care or Payment -*or*- for Notification Purposes.

1. When the patient is present and has decisional capacity. If the patient is present and has decisional capacity, a member of the workforce of the Health Clinics may use or disclose to a family member, other relative, or a close personal friend of the patient, or to any other person identified by the patient, PHI that is directly relevant to such person's involvement with the patient's care or payment related to the patient's health care (or for notification purposes of location, general condition, or death of the patient), PROVIDED that either:

a. the patient agreed (may be an oral agreement); OR

b. the patient has been given the opportunity to object and did not expressly object and, based on professional judgment, it is reasonably inferred that the patient does not object.

2. When the patient either is not present or does not have decisional capacity. If the patient either is not present or does not have decisional capacity, a member of the workforce of the Health Clinics may use or disclose to a family member, other relative, or a close personal friend of the patient, or any other person identified by the patient, PHI that is directly relevant to such person's involvement with the patient's care or payment related to the patient's health care (or for notification purposes of location, general condition, or death of the patient), PROVIDED that, based on professional judgment and experience with common practice, it is determined that the use or disclosure is in the best interests of the patient.

3. Disaster Relief Entities. A member of the workforce of the Health Clinics may use or disclose PHI to a public or private entity authorized by law or by its charter to assist in disaster relief in order to coordinate notification of location, general condition, or death of the patient to a family member, a personal representative of the individual, or another person responsible for the care of the patient. The limitations of paragraphs 1 and 2 are applicable only to the extent that, in the exercise of professional judgment, those requirements do not interfere with the ability to respond to the emergency circumstances.

Child Abuse or Neglect. A member of the Health Clinics workforce may use and disclose PHI when all of the following are fulfilled:

1. There is reasonable cause to believe a child known to that member of the workforce in a professional or official capacity may be an abused child or neglected child pursuant to the Illinois Abused and Neglected Child Reporting Act (325 ILCS 5);

2. The disclosure is to a government agency authorized to receive reports of child abuse or neglect (*e.g.* for Illinois, it is the Illinois Department of Children and Family Services; http://www.state.il.us/dcfs/index.shtml; 1-800-25-ABUSE); and

3. An accounting log entry is made documenting the disclosure (see the provision in Section IV regarding right to receive an accounting of disclosures).

Per Illinois law (325 ILCS 5/3),

*"**Abused child**" means a child whose parent or immediate family member, or any person responsible for the child's welfare, or any individual residing in the same home as the child, or a paramour of the child's parent:*

(a) inflicts, causes to be inflicted, or allows to be inflicted upon such child physical injury, by other than accidental means, which causes death, disfigurement, impairment of physical or emotional health, or loss or impairment of any bodily function;

(b) creates a substantial risk of physical injury to such child by other than accidental means which would be likely to cause death, disfigurement, impairment of physical or emotional health, or loss or impairment of any bodily function;

(c) commits or allows to be committed any sex offense against such child, as such sex offenses are defined in the Criminal Code of 1961, as amended, and extending those definitions of sex offenses to include children under 18 years of age;
(d) commits or allows to be committed an act or acts of torture upon such child;
(e) inflicts excessive corporal punishment;
(f) commits or allows to be committed the offense of female genital mutilation, as defined in Section 12-34 of the Criminal Code of 1961, against the child; or
(g) causes to be sold, transferred, distributed, or given to such child under 18 years of age, a controlled substance as defined in Section 102 of the Illinois Controlled Substances Act in violation of Article IV of the Illinois Controlled Substances Act, except for controlled substances that are prescribed in accordance with Article III of the Illinois Controlled Substances Act and are dispensed to such child in a manner that substantially complies with the prescription.

A child shall not be considered abused for the sole reason that the child has been relinquished in accordance with the Abandoned Newborn Infant Protection Act.

*"**Neglected child**" means any child who is not receiving the proper or necessary nourishment or medically indicated treatment including food or care not provided solely on the basis of the present or anticipated mental or physical impairment as determined by a physician acting alone or in consultation with other physicians or otherwise is not receiving the proper or necessary support or medical or other remedial care recognized under State law as necessary for a child's well-being, or other care necessary for his or her well-being, including adequate food, clothing and shelter; or who is abandoned by his or her parents or other person responsible for the child's welfare without a proper plan of care; or who is a newborn infant whose blood, urine, or meconium contains any amount of a controlled substance as defined in subsection (f) of Section 102 of the Illinois Controlled Substances Act or a metabolite thereof, with the exception of a controlled substance or metabolite thereof whose presence in the newborn infant is the result of medical treatment administered to the mother or the newborn infant. A child shall not be considered neglected for the sole reason that the child's parent or other person responsible for his or her welfare has left the child in the care of an adult relative for any period of time. A child shall not be considered neglected for the sole reason that the child has been relinquished in accordance with the Abandoned Newborn Infant Protection Act. A child shall not be considered neglected or abused for the sole reason that such child's parent or other person responsible for his or her welfare depends upon spiritual means through prayer alone for the treatment or cure of disease or remedial care as provided under Section 4 of this Act. A child shall not be considered neglected or abused solely because the child is not attending school in accordance with the requirements of Article 26 of The School Code, as amended.*

*"**Person responsible for the child's welfare**" means the child's parent; guardian; foster parent; relative caregiver; any person responsible for the child's welfare in a public or private residential agency or institution; any person responsible for the child's welfare within a public or private profit or not for profit child care facility; or any other person responsible for the child's welfare at the time of the alleged abuse or neglect, or any person who came to know the child through an official capacity or position of trust, including but not limited to health care professionals, educational personnel, recreational supervisors, members of the clergy, and volunteers or support personnel in any setting where children may be subject to abuse or neglect.*

Victims of Abuse, Neglect, or Domestic Violence. A member of the Health Clinics workforce may use and disclose PHI when all of the following are fulfilled:

1. A member of the Health Clinics workforce reasonably believes an individual is a victim of abuse, neglect, or domestic violence;

2. The disclosure of the victim's PHI is to a government agency authorized by law to receive reports of such abuse, neglect, or domestic violence;

3. The disclosure of the victim's PHI is either:

a. required by law;

Per Illinois law (320 ILCS 20/4), it is required by law to report a suspicion of the abuse, neglect, or financial exploitation of a person 60 years of age or older to the Illinois Department on Aging; http://www.state.il.us/aging/; 1-866-800-1409; when there is reason to believe that the elder is unable to seek assistance for himself or herself.

Per Illinois law (320 ILCS 20/2),

"Abuse" means causing any physical, mental or sexual injury to an eligible adult, including exploitation of such adult's financial resources.

This does not mean that an eligible adult is a victim of abuse, neglect, or self-neglect for the sole reason that he or she is being furnished with or relies upon treatment by spiritual means through prayer alone, in accordance with the tenets and practices of a recognized church or religious denomination.

This does not mean that an eligible adult is a victim of abuse because of health care services provided or not provided by licensed health care professionals.

"Neglect" means another individual's failure to provide a person 60 years of age or older with or willful withholding from a person 60 years of age or older the necessities of life including, but not limited to, food, clothing, shelter or medical care. This subsection does not create any new affirmative duty to provide support to a person 60 years of age or older. This definition does not mean that a person 60 years of age or older is a victim of neglect because of health care services provided or not provided by licensed health care professionals.

"Eligible adult" means a person 60 years of age or older who resides in a domestic living situation and is, or is alleged to be, abused, neglected, or financially exploited by another individual or who neglects himself or herself.

The Illinois Domestic Violence Act does not have a mandatory reporting provision for health care providers. However, it does state that anyone authorized to administer health care "shall offer to a person suspected to be a victim of abuse immediate and adequate information regarding services available to victims of abuse." 750 ILCS 60/401.

b. necessary to prevent serious harm to the current victim or other potential victims,

c. when the victim is unable to agree (due to incapacity) and the government official represents that the PHI is not intended to be used against the victim and that an immediate enforcement activity depends upon the disclosure or else it would be materially and adversely affected by waiting until the victim is able to agree to the disclosure, -or-

d. when the victim agrees to the disclosure;

4. The victim is promptly notified that the disclosure has been or will be made UNLESS it is reasonably believed in the exercise of professional judgment that either:

a. informing the victim would place that victim at risk of serious harm or

b. a personal representative of the victim would receive the notification that that personal representative is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interests of the victim; and

5. An accounting log entry is made documenting the disclosure (see the provision in Section IV regarding right to receive an accounting of disclosures).

Victims of Crime. A member of the Health Clinics workforce may use and disclose PHI when all of the following are fulfilled:

1. The disclosure is to a government officer empowered to investigate or prosecute violations of law and in response to such official's request for information about an individual who is a victim of a crime or is suspected to be a victim of a crime;

2. Either the individual agrees to the disclosure -or-

a. The Health Clinics is unable to obtain the individual's agreement because of incapacity or other emergency circumstance,

b. The government official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim,

c. The government official represents that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure, and

d. The Health Clinics determines, in the exercise of professional judgment, that the disclosure is in the best interests of the individual; and

3. An accounting log entry is made documenting the disclosure (see the provision in Section IV regarding right to receive an accounting of disclosures).

Court Order, Subpoena, or Other Similar Written Demand.

[see notes at end of Illinois laws regarding mental health information, physician/patient privilege, and subpoenas]

1. Court Order. A member of the Health Clinics workforce may use or disclose PHI in compliance with a lawful order of a court or administrative tribunal (consultation should be made

with legal counsel of the Health Clinics). An accounting log entry will be made documenting the disclosure (see the provision in Section IV regarding right to receive an accounting of disclosures).

2. Subpoena (not accompanied by court order) (Option A). A member of the Health Clinics workforce may use or disclose PHI in response to a lawful subpoena, discovery request, or other lawful process that is not accompanied by an order of a court or administrative tribunal if:

a. The Health Clinics receives a written statement and supporting documentation from the requesting party demonstrating that:

(1) The party requesting such information has made a good faith attempt to provide written notice to the patient (or, if the patient's location is unknown, to mail a notice to the patient's last known address),

(2) The notice included sufficient information about the litigation or proceeding in which the PHI is requested to permit the patient to raise an objection to the court or administrative tribunal, and

(3) The time for the patient to raise objections to the court or administrative tribunal has elapsed, and either:

(a) No objections were filed or

(b) All objections filed by the patient have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with such resolution; and

b. An accounting log entry is made documenting the disclosure (see the provision in Section IV regarding right to receive an accounting of disclosures).

3. Subpoena (not accompanied by court order) (Option B). A member of the Health Clinics workforce may use or disclose PHI in response to a lawful subpoena, discovery request, or other lawful process that is not accompanied by an order of a court or administrative tribunal if:

a. The Health Clinics receives a written statement and supporting documentation from the requesting party demonstrating that: the party seeking the PHI has requested a qualified protective order from such court or administrative tribunal that:

(1) Prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which such information was requested and

(2) Requires the return to the Health Clinics or destruction of the PHI (including all copies made) at the end of the litigation or proceeding; and

b. An accounting log entry is made documenting the disclosure (see the provision in Section IV regarding right to receive an accounting of disclosures).

4. Other Written Demand. A member of the Health Clinics workforce may use or disclose PHI to a government officer empowered to investigate or prosecute violations of law if:

a. The Health Clinics receives and discloses consistent with either:
(1) a warrant, subpoena, or summons issued by a judicial officer,
(2) a grand jury subpoena, or
(3) an administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that:
(a) The information sought is relevant and material to a legitimate law enforcement inquiry,
(b) The written demand is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought, and
(c) De-identified information could not reasonably be used; and

b. An accounting log entry is made (see the HIPAA Privacy Rule policy on Right to Receive an Accounting).

Note about mental health information: Illinois law at 740 ILCS 110/10(d) provides that "No person shall comply with a subpoena for records or communications under this Act, unless the subpoena is accompanied by a written order authorizing the issuance of the subpoena or the disclosure of the records. Each subpoena duces tecum issued by a court or administrative agency or served on any person pursuant to this subsection (d) shall include the following language: 'No person shall comply with a subpoena for mental health records or communications pursuant to Section 10 of the Mental Health and Developmental Disabilities Confidentiality Act, 740 ILCS 110/10, unless the subpoena is accompanied by a written order that authorizes the issuance of the subpoena and the disclosure of records or communications.'" That law then provides some details about the court order. Accordingly, this statutory privilege to refuse to disclose should be asserted and consultation with legal counsel should be obtained before any disclosure is made in response to a court order, subpoena, or other written demand. 740 ILCS 110/10.

Note about physician/patient privilege: Illinois law at 735 ILCS 5/8-802 establishes a physician and patient privilege that permits disclosure only in certain types of cases. Those are: (1) in trials for homicide when the disclosure relates directly to the fact or immediate circumstances of the homicide, (2) in actions, civil or criminal, against the physician for malpractice, (3) with the expressed consent of the patient, or in case of his or her death or disability, of his or her personal representative or other person authorized to sue for personal injury or of the beneficiary of an insurance policy on his or her life, health, or physical condition, (4) in all actions brought by or against the patient, his or her personal representative, a beneficiary under a policy of insurance, or the executor or administrator of his or her estate wherein the patient's physical or mental condition is an issue, (5) upon an issue as to the validity of a document as a will of the patient, (6) in any criminal action where the charge is either first degree murder by abortion, attempted abortion or abortion, (7) in actions, civil or criminal, arising from the filing of a report in compliance with the Abused and Neglected Child Reporting Act, (8) to any department, agency, institution or facility which has custody of the patient pursuant to State statute or any court order of commitment, (9) in prosecutions where written results of blood alcohol tests are admissible pursuant to Section 11‑501.4 of the Illinois Vehicle Code, (10) in prosecutions where written

results of blood alcohol tests are admissible under Section 5‑11a of the Boat Registration and Safety Act, (11) in criminal actions arising from the filing of a report of suspected terrorist offense in compliance with Section 29D‑10(p)(7) of the Criminal Code of 1961, or (12) upon the issuance of a subpoena pursuant to Section 38 of the Medical Practice Act of 1987; the issuance of a subpoena pursuant to Section 25.1 of the Illinois Dental Practice Act; or the issuance of a subpoena pursuant to Section 22 of the Nursing Home Administrators Licensing and Disciplinary Act.

Note about subpoenas: Illinois law (Sup.Ct Rule 204(a)-(c) states the following:
Rule 204. Compelling Appearance of Deponent
(a) Action Pending in This State.

(1) Subpoenas. Except as provided in paragraph (c) hereof, the clerk of the court shall issue subpoenas on request. The subpoena may command the person to whom it is directed to produce documents or tangible things which constitute or contain evidence relating to any of the matters within the scope of the examination permitted under these rules.

(2) Service of Subpoenas. A deponent shall respond to any lawful subpoena of which the deponent has actual knowledge, if payment of the fee and mileage has been tendered. Service of a subpoena by mail may be proved prima facie by a return receipt showing delivery to the deponent or his authorized agent by certified or registered mail at least seven days before the date on which appearance is required and an affidavit showing that the mailing was prepaid and was addressed to the deponent, restricted delivery, return receipt requested, showing to whom, date and address of delivery, with a check or money order for the fee and mileage enclosed.

(3) Notice to Parties, et al. Service of notice of the taking of the deposition of a party or person who is currently an officer, director, or employee of a party is sufficient to require the appearance of the deponent and the production of any documents or tangible things listed in the notice.

(4) Production of Documents in Lieu of Appearance of Deponent. The notice, order or stipulation to take a deposition may specify that the appearance of the deponent is excused, and that no deposition will be taken, if copies of specified documents or tangible things are served on the party or attorney requesting the same by a date certain. That party or attorney shall serve all requesting parties of record at least three days prior to the scheduled deposition, with true and complete copies of all documents, and shall make available for inspection tangible things, or other materials furnished, and shall file a certificate of compliance with the court. Unless otherwise ordered or agreed, reasonable charges by the deponent for production in accordance with this procedure shall be paid by the party requesting the same, and all other parties shall pay reasonable copying and delivery charges for materials they receive. A copy of any subpoena issued in connection with such a deposition shall be attached to the notice and immediately filed with the court, not less than 14 days prior to the scheduled deposition. The use of this procedure shall not bar the taking of any person's deposition or limit the scope of same.

(b) Action Pending in Another State, Territory, or Country. Any officer or person authorized by the laws of another State, territory, or county to take any deposition in this State, with or without a commission, in any action pending in a court of that State, territory, or country may petition the circuit court in the county in which the deponent resides or is employed or transacts business in person or is found for a subpoena to compel the appearance of the deponent or for an order to compel the giving of testimony by the deponent. The court may hear and act upon the petition with or without notice as the court directs.

(c) Depositions of Physicians. The discovery depositions of nonparty physicians being deposed in their professional capacity may be taken only with the agreement of the parties and the subsequent consent of the deponent or under a subpoena issued upon order of court. A party shall pay a reasonable fee to a physician for the time he or she will spend testifying at any such deposition.

Unless the physician was retained by a party for the purpose of rendering an opinion at trial, or unless otherwise ordered by the court, the fee shall be paid by the party at whose instance the deposition is taken.

Identifying or Locating Suspect, Fugitive, Material Witness, or Missing Person. A member of the Health Clinics workforce may use or disclose PHI to a government officer empowered to investigate or prosecute violations of law if:

1. The disclosure is in response to such government official's request for information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person;

2. The disclosure only includes:
   a. Name and address;
   b. Date and place of birth;
   c. Social security number;
   d. ABO blood type and rh factor;
   e. Type of injury;
   f. Date and time of treatment;
   g. Date and time of death, if applicable; and
   h. A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos;

3. Other than that listed above, the disclosure does not include PHI related to the individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue; and

4. An accounting log entry is made documenting the disclosure (see the provision in Section IV regarding right to receive an accounting of disclosures).

Coroners and Medical Examiners. A member of the Health Clinics workforce may use or disclose PHI when all of the following are fulfilled:

1. The PHI is about a deceased person;

2. The disclosure is to a coroner or medical examiner;

3. The disclosure is for the purpose of identifying a deceased person, determining a cause of death, or other coroner/medical examiner duties as authorized by law;

4. An accounting log entry is made documenting the disclosure (see the provision in Section IV regarding right to receive an accounting of disclosures).

Crime on Premises of Health Clinics. A member of the Health Clinics workforce may use or disclose PHI when all of the following are fulfilled:

1. The disclosure is to a government officer empowered to investigate or prosecute violations of law;

2. The Health Clinics believes in good faith the disclosed PHI constitutes evidence of criminal conduct that occurred on the premises of the Health Clinics; and

3. An accounting log entry is made documenting the disclosure (see the provision in Section IV regarding right to receive an accounting of disclosures).

To Avert Threat to Health or Safety of Person or the Public. A member of the Health Clinics workforce may use or disclose PHI when all of the following are fulfilled:

1. A member of the Health Clinics workforce, in good faith, believes (through actual knowledge or through reliance on a credible representation from another with apparent knowledge or authority) that:

    a. Disclosure of the PHI is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public,

    b. The disclosure is made to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat, and

    c. The disclosure is consistent with the relevant professional ethical standards, and

2. An accounting log entry is made documenting the disclosure (see the provision in Section IV regarding right to receive an accounting of disclosures).

To Control Disease, Injury, or Disability. A member of the Health Clinics workforce may use or disclose PHI when all of the following are fulfilled:

1. A member of the Health Clinics workforce reasonably believes the disclosure of PHI is for preventing or controlling disease, injury, or disability;

2. The disclosure is to a government agency authorized by law to collect or receive such information; and

3. An accounting log entry is made documenting the disclosure (see the provision in Section IV regarding right to receive an accounting of disclosures).

For Workers Compensation Purposes. A member of the Health Clinics workforce may use or disclose PHI when all of the following are fulfilled:

1. The use or disclosure is in response to a subpoena or subpoena duces tecum that:

    a. was issued by the Illinois Workers' Compensation Commission (aka Illinois Industrial Commission) or an Arbitrator designated by the Illinois Workers' Compensation Commission (820 ILCS 305/16), and

    b. specifically requires the disclosure of PHI; and

2. The PHI disclosed is limited to that described in the subpoena; and

3. An accounting log entry is made documenting the disclosure (see the provision in Section IV regarding right to receive an accounting of disclosures).

Research Purposes - Waiver of Authorization. A member of the Health Clinics workforce may use or disclose PHI when all of the following are fulfilled:

1. The Health Clinics obtains documentation that an alteration to or waiver, in whole or in part, of a written authorization has been approved by an Institutional Review Board (IRB) established by the *Common Rule*;

2. The documentation of such approval consists of at least:

    a. A statement identifying the IRB and the date on which the alteration or waiver of authorization was approved;

    b. A statement that the IRB has determined that the alteration or waiver, in whole or in part, of authorization satisfies the following criteria:

        (1) The use or disclosure of PHI involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements;
            (a) An adequate plan to protect the identifiers from improper use and disclosure,
            (b) An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law, and
            (c) Adequate written assurances that the PHI will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of PHI would be permitted by the HIPAA Privacy Rule,

        (2) The research could not practicably be conducted without the waiver or alteration, and

(3) The research could not practicably be conducted without access to and use of the PHI;

c. A brief description of the PHI for which use or access has been determined to be necessary by the IRB;

d. A statement that the alteration or waiver of authorization has been reviewed and approved by the IRB under either normal or expedited review procedures as established by the *Common Rule*; and

e. The signature of the chair or other member as designated by the chair of the IRB; and

3. An accounting log entry is made documenting the disclosure (see the provision in Section IV regarding right to receive an accounting of disclosures).

Note: The Privacy Officer should notify the Office of Compliance of RFUMS prior to release of PHI under this provision.

Research Purposes - Preparatory to Research. A member of the Health Clinics workforce may use or disclose PHI when all of the following are fulfilled:

1. The Health Clinics obtains from the researcher a written statement certifying that:

a. the use or disclosure is sought solely to review PHI as necessary to prepare a research protocol or for similar purposes preparatory to research;

b. no PHI is to be removed from the designated component by the researcher in the course of the review; and

c. the PHI for which use or access is sought is necessary for the research purposes; and

2. An accounting log entry is made documenting the disclosure (see the provision in Section IV regarding right to receive an accounting of disclosures).

Research Purposes - Limited Data Set. A member of the Health Clinics workforce may use or disclose PHI when all of the following are fulfilled:

1. The disclosed PHI consists only of a limited data set, as defined by the HIPAA Privacy Rule;

2. The purpose of the use or disclosure is for research;

3. The Health Clinics and the researcher enter into a written agreement that:

a. establishes the only permitted uses and disclosures is for research purposes and that the researcher is not authorized to use or disclose the information in a manner that would violate the requirements of the HIPAA Privacy Rule, if done by the Health Clinics;

b. identifies the research who is permitted to use or receive the limited data set; and

c. provides that the researcher will:

(1) not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;
(2) use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;
(3) report to the designated component any use or disclosure of the information not provided for by its data use agreement of which it becomes aware;
(4) ensure that any agents, including a subcontractor, to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and
(5) not identify the information or contact the individuals; and

4. The Health Clinics is not aware of a pattern of activity or practice of the researcher that constituted a material breach or violation of the data use agreement, unless the Health Clinics took reasonable steps to cure the breach or end the violation, as applicable (Note: if such steps to cure the breach or end the violation were unsuccessful, the Health Clinics must discontinue disclosure of PHI to the recipient and report the problem to the Department of HHS).

*"**Limited Data Set**" means PHI that excludes the following direct identifiers of the patient or of relatives, employers, or household members of the patient:*
1. Names;
2. Postal address information, other than town or city, State, and zip code;
3. Telephone numbers;
4. Fax numbers;
5. Electronic mail addresses;
6. Social security numbers;
7. Medical record numbers;
8. Health plan beneficiary numbers;
9. Account numbers;
10. Certificate/license numbers;
11. Vehicle identifiers and serial numbers, including license plate numbers;
12. Device identifiers and serial numbers;
13. Web Universal Resource Locators (URLs);
14. Internet Protocol (IP) address numbers;
15. Biometric identifiers, including finger and voice prints; and
16. Full face photographic images and any comparable images.

Other Reasons. A member of the Health Clinics workforce may use or disclose PHI after and upon approval by the Privacy Officer, who will have assessed the proposed use or disclosure for compliance with the HIPAA Privacy Rule.

GENERAL RULES APPLICABLE TO

USING AND DISCLOSING HEALTH INFORMATION

Role-Based Access. The Health Clinics limits access to PHI to those whose role requires access to complete assigned duties or functions. Examples are as follows:

1. Computer Records (e.g. health, billing, appointments). Access to these computer record systems is controlled through user names and passwords, which are overseen by RFUMS Information Technology Services and in the cases of the Advanced MD and Athena Electronic Health Record Systems, the Health Clinics and its designees directly. The Health Clinics Privacy Officer will coordinate with RFUMS ITS to ensure only those with proper roles have access to the electronic records (including terminating access when no longer needed). Only those with role-based access may access the electronic records.

2. North Chicago - Health Records Room. The Health Records Room is to be locked at all times. Access to that room is controlled through use of the person's identification card, which is overseen by RFUMS Campus Security. The Health Clinics Privacy Officer will coordinate with RFUMS Campus Security to ensure only those with proper roles have such access to the Health Records Room (including terminating access when no longer needed). Only those with role-based access may enter to the Health Records Room.

3. North Chicago - Archive Health Records Room. The Archive Health Records Room is to be locked at all times. Access to that room is controlled through use of a key held in the custody of the Health Clinics Privacy Officer.

4. North Chicago - Building. The main door to the building is locked after normal working hours and other doors are locked preventing access at all times. Access through locked doors is controlled through use of the person's identification card, which is overseen by RFUMS Campus Security. The Health Clinics Privacy Officer will coordinate with RFUMS Campus Security to ensure only those with proper roles have such access to enter through locked doors (including terminating access when no longer needed). Only those with role-based access may enter through locked doors.

5. Vernon Hills - Clinic Suite. The clinic suite is locked after normal working hours. Access through locked doors is controlled through use of keys issued by RFUMS Campus Security. The Health Clinics Privacy Officer will coordinate with RFUMS Campus Security to ensure only those with proper roles have such access to enter through locked doors (including terminating access when no longer needed). Only those with role-based access may enter through locked doors.

6. Vernon Hills - Health Records Room. The health records room is locked after normal working hours and access is controlled through use of a key held in the custody of the Health Clinics Privacy Officer. Duplicate keys may be authorized by the Privacy Officer to be possessed by those with role-based access. Only those with role-based access may enter that health records room.

Minimum Necessary. Members of the Health Clinics workforce will limit the PHI used or disclosed to that which is the minimum necessary to accomplish the permitted reason (with a few exceptions).

1. The General Rule. When requesting, using, or disclosing PHI, the Health Clinics and its workforce must make reasonable efforts to limit PHI to the minimum necessary to accomplish the permitted reason for the request, use, or disclosure. For example, do not request, use, or disclose an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the permitted reason for request, use or disclosure.

2. When These Requirements are NOT APPLICABLE. These requirements do not apply to:
   a. disclosures to or requests by a health care provider for treatment purposes;
   b. uses or disclosures made to the patient;
   c. uses or disclosures made pursuant to a valid written authorization;
   d. disclosures made to HHS in relation to HIPAA compliance and enforcement;
   e. uses or disclosures that are required by law; and
   f. uses or disclosures that are required for compliance with the HIPAA Privacy Rule.

3. Complying with the Minimum Necessary Requirements.

   a. The minimum necessary rule may be deemed satisfied when:
      (1) the PHI is requested by another health care provider or health plan that is itself bound by the HIPAA Privacy Rule);

      (2) the PHI is requested by a professional member of the Health Clinics or of a business associate of the Health Clinics and the professional states that the PHI requested is the minimum necessary for the stated purpose.

   b. For all requests, uses, or disclosures to which the minimum necessary requirements apply, do not request, use, or disclose an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the permitted reason for request, use or disclosure.

4. Incidental Uses or Disclosures. A use or disclosure of PHI that occurs as a consequence or was incident to activities associated with a permitted use or disclosure of PHI is not considered a violation of the HIPAA Privacy Rule or this Manual if:

   a. the minimum necessary requirements were fulfilled; and

   b. reasonable safeguards were implemented and utilized.

Verification. Members of the Health Clinics workforce will use reasonable verification procedures before disclosing PHI.

1. The General Rule. Reasonable efforts must be made to verify the existence or truth of the required or relevant circumstances prior to disclosing PHI.

2. Compliance with the Verification Requirements.

a. When identity or authority of a particular person is required or is a relevant factor in the decision whether to disclose PHI, then members of the Health Clinics workforce must verify the identity of a person requesting PHI and the authority of that person, if not already known.

(1) The Health Clinics may rely (if reasonable under the circumstances), on any of the following to verify identity when the disclosure of PHI is to a public official or a person acting on behalf of the public official:

(a) If the request is made in person, then presentation of an agency identification badge, other official credentials, or other proof of government status;

(b) If the request is in writing, then the request is on the appropriate government letterhead; or

(c) If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

(2) The Health Clinics may rely (if reasonable under the circumstances), on any of the following to verify authority when the disclosure of PHI is to a public official or a person acting on behalf of the public official:

(a) A written statement of the legal authority under which the PHI is requested, or, if a written statement would be impracticable, an oral statement of such legal authority;

(b) If a request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority.

b. When certain a document, statement, or assertion is a required or is a relevant factor in the decision whether to disclose PHI, then members of the Health Clinics workforce must verify and obtain the documentation, statement, or assertion (oral or written), from the person requesting the PHI.

(1) The Health Clinics may rely (if reasonable under the circumstances), on documentation, statements, or assertions that, on their face, meet the applicable requirements.

(2) Section III of this Manual has special guidance for situations involving an administrative request for law enforcement purposes and a waiver of authorization in research.

Personal Representative. Members of the Health Clinics workforce will comply with the following provisions in order to determine whether a patient has a personal representative and, if so, the identity of that personal representative.

1. The General Rule. With limited exceptions, a personal representative must be treated as the patient for purposes of the HIPAA Privacy Rule.

2. How to Identify Who is a Personal Representative.

a. Adults and emancipated minors. If, under applicable law, a person has authority to act on behalf of a patient who is an adult or an emancipated minor in making decisions related to health care, the Health Clinics must treat such person as a personal representative under the HIPAA Privacy Rule, with respect to PHI relevant to such personal representation.

Note: Per Illinois law:

1. A court-appointed guardian of the person of the patient has authority to act on behalf of that patient in making decisions related to health care if such court appointment so authorizes the guardian and the guardian acts consistent with that court appointment.

2. An "agent" identified in a written Power of Attorney for Health Care document created pursuant to the Illinois Power of Attorney for Health Care Law (755 ILCS 45/Art. IV) has authority to act on behalf of the principal (otherwise known as the "patient") in making decisions related to health care during periods in which the patient lacks decisional capacity but only to the extent the agent is complying with the written Power of Attorney for Health Care document and Illinois Power of Attorney for Health Care Law.

3. A "surrogate decision maker" for the patient that is identified by the attending physician pursuant to the Illinois Health Care Surrogate Act (755 ILCS 40) has authority to act on behalf of that patient in making decisions relating to health care during periods in which the patient lacks decisional capacity but only to the extent the surrogate decision maker is complying with the Illinois Health Care Surrogate Act.

b. Unemancipated minors.

(1) If, under applicable law, a parent, guardian, or other person acting in loco parentis has authority to act on behalf of a patient who is an unemancipated minor

in making decisions related to health care, the Health Clinics must treat such person as a personal representative under the HIPAA Privacy Rule, with respect to PHI relevant to such personal representation.

(2) However, the person described above may not be a personal representative of an unemancipated minor (and the minor has the authority to act) with respect to PHI pertaining to a health care service, if:

(a) The minor consents to such health care service; no other consent to such health care service is required by law, regardless of whether the consent of another person has also been obtained; and the minor has not requested that such person be treated as the personal representative;

(b) The minor may lawfully obtain such health care service without the consent of a parent, guardian, or other person acting in loco parentis, and the minor, a court, or another person authorized by law consents to such health care service; or

(c) A parent, guardian, or other person acting in loco parentis assents to an agreement of confidentiality between the Health Clinics and the minor with respect to such health care service.

(3) However,

(a) to the extent permitted or required by applicable law, the Health Clinics may disclose, or provide access in accordance with the right of access to PHI about an unemancipated minor to a parent, guardian, or other person acting in loco parentis;

(b) to the extent prohibited by applicable law, the Health Clinics may not disclose, or provide access in accordance with the right of access to PHI about an unemancipated minor to a parent, guardian, or other person acting in loco parentis; and

(c) where the parent, guardian, or other person acting in loco parentis, is not the personal representative as defined above and where there is no applicable access provision under applicable law, the Health Clinics may provide or deny access under the right of access to a parent, guardian, or other person acting in loco parentis, if such action is consistent with applicable law, provided that such decision must be made by a licensed health care professional, in the exercise of professional judgment.

Per Illinois law, an unemancipated minor has authority to consent to health care as follows:

1. The patient is married, a parent, or a pregnant women and the health care consists of any medical or surgical procedures by a licensed professional (410 ILCS 210/1).

2. The patient is a victim of criminal sexual assault or criminal sexual abuse and the health care consists of medical care or counseling related to the diagnosis or treatment by a licensed professional of any disease or injury arising from that criminal offense (410 ILCS 210/3(b)).

3. The patient has attained at least 12 years of age and came in contact with a sexually transmitted disease, is an addict or alcoholic, or has a family member who abuses alcohol or drugs and the health care consists of medical care or counseling related to the diagnosis or treatment of that disease (410 ILCS 210/4).

4. The patient has attained at least 12 years of age and the treatment or procedures consist of mental health counseling services or psychotherapy on an outpatient basis when there is not more than 5 sessions and no session will last more than 45 minutes (405 ILCS 5/3-501(a)).

5. The patient has attained at least 16 years of age; is a "voluntary recipient" admitted into a mental health facility; the person's parent, guardian, or person in loco parentis has been informed of the admission into the facility; and the health care consists of treatment of the mental illness (405 ILCS 5/3-502).

c. Deceased individuals. If, under applicable law, an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate, the Health Clinics must treat such person as a personal representative under this subchapter, with respect to PHI relevant to such personal representation.

d. Abuse, neglect, endangerment situations. Notwithstanding any law or any requirement of the HIPAA Privacy Rule to the contrary, the Health Clinics may elect not to treat a person as the personal representative of a patient if:

(1) The Health Clinics has a reasonable belief that:
(a) The patient has been or may be subjected to domestic violence, abuse, or neglect by such person; or
(b) Treating such person as the personal representative could endanger the patient; and

(2) The Health Clinics, in the exercise of professional judgment, decides that it is not in the best interest of the patient to treat the person as the patient's personal representative.

SAFEGUARDING HEALTH INFORMATION

The General Rule. The Health Clinics will have in place and its workforce must utilize appropriate administrative, technical, and physical safeguards to:

1. Protect the confidentiality of PHI from inappropriate uses or disclosures;

2. Promote compliance with this Manual and the HIPAA Privacy Rule; and

3. Limit incidental uses or disclosures made pursuant to an otherwise permitted use or disclosure.

Examples of reasonable safeguards include these administrative policies and procedures (e.g. this Manual), standard practices and tools (e.g. checklists and template forms), training, computer username and password systems, secured cabinets and locked doors, etc.

Incidental Uses or Disclosures. A use or disclosure of PHI that occurs as a consequence or was incident to activities associated with a permitted use or disclosure of PHI is not considered a violation of the HIPAA Privacy Rule or this Manual if:

1. the minimum necessary requirements were fulfilled; and

2. reasonable safeguards were implemented and utilized.

Administrative Safeguards – Medical Records Storage

1. All medical records shall remain within the building. No records shall be removed from the premises except for the planned purpose of transferring to other qualified storage space under direct control of the Health Clinics.

2. Records shall be kept locked up in the medical records storage areas; current and archived. Records that are removed from these areas for business purposes during the day shall remain in non-public areas (areas only accessible by Health Clinics workforce) and secured in filing cabinets, placed face down on desks, or other reasonable measures to avoid incidental disclosures of PHI. All records shall be returned to their secured storage area when finished.

3. Records shall be classified as current for a minimum of six years or until patient is inactive, which ever is longer. These records shall be maintained in designated medical record rooms.

4. Inactive records shall be archived and maintained for the period of time as applicable by state and federal law and business purposes. These records shall be maintained in designated medical records rooms.

PATIENT RIGHTS

Notice of Privacy Practices (NOPP).

1. With limited exceptions, a patient has the right to adequate notice of the uses and disclosures of PHI that may be made by the Health Clinics and of the patient rights and the Health Clinics legal duties with respect to PHI.

2. The Health Clinics will create a NOPP consistent with the requirements of the HIPAA Privacy Rule and accomplish the following:

a. provide a written copy of the NOPP on or before the date of the first delivery of service and obtain a written acknowledgment of receipt;

b. have available written copies of the NOPP upon request;

c. display the NOPP prominently in the patient waiting area; and

d. electronically post the NOPP on the Health Clinics website.

Right of Access to PHI.

1. With limited exceptions, a patient has a right of access to inspect and obtain a copy of PHI about the patient that is contained in a designated record set for as long as the PHI is maintained in that designated record set.

> ***Designated record set****. "Designated record set" means the health records of patients, billing records of patients, and other designated groups of records about patients that are maintained by or for the Health Clinics and used by the Health Clinics to make decisions about patients.*

2. If the patient's request for access directs the Health Clinics to transmit the copy of PHI directly to another person designated by the patient, the Health Clinics must provide the copy to the person designated by the patient. The patient's request must be in writing, signed by the individual, and clearly identify the designated person and where to send the copy of PHI. These requirements relating to a writing may not be waived by the Health Clinics.

3. To exercise this right of access, the patient must make the request in writing (the Health Clinics has a form to be used for this purpose). Except for a request described in paragraph 2, this requirement of a writing may be waived. In all cases, further discussions with the patient may be made to arrange for a convenient time and place to inspect or obtain a copy of the PHI, or mailing the copy of the PHI at the patient's request. The Health Clinics may discuss the scope, format, and other aspects of the request for access with the patient as necessary to facilitate the timely provision of access.

4. Within 30 days of receiving the written request, an authorized workforce member of the Health Clinics shall either:

a. provide access if the situation does not meet the definition of "grounds for denial" or

b. notify the patient of the decision to deny access if the situation meets the definition of "grounds for denial."

Note: A 30-day extension is allowed if the Health Clinics notifies the patient of the reasons for the delay and the expected completion date. This notice must be sent prior to expiration of the initial 30-day period. Only one extension is allowed.

***Grounds for denial**. A request for access will be denied when the request relates to any of the following:*
a. Psychotherapy notes;
b. Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and
c. Situations where access is prohibited per the Clinical Laboratory Improvements Amendments of 1988 (42 U.S.C. § 263a) or where the information is exempt from the Clinical Laboratory Improvements Amendments of 1988 (42 CFR § 493.3(a)(2)).
d. Situations in which the Health Clinics is acting under the direction of a correctional institution and an inmate's obtaining requested access would jeopardize the health, safety, security, custody, or rehabilitation of the patient or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate.
e. Situations in which the PHI was created or obtained by a health care provider in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress, provided that the patient has agreed to the denial of access when consenting to participate in the research that includes treatment, and the covered health care provider has informed the patient that the right of access will be reinstated upon completion of the research.
f. Situations in which the PHI was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.
g. Situations in which a licensed health care professional has made one of the following decisions in the exercise of professional judgment (a "right of review" will apply):

(1) that the access requested is reasonably likely to endanger the life or physical safety of the patient or another person;
(2) that the access requested is reasonably likely to cause substantial harm to a person referenced in the record (other than a health care provider); or
(3) that the access to a personal representative of the patient is reasonably likely to cause substantial harm to the patient or another person.

5. <u>When the Decision is to Deny Access</u>.

a. The notification to the patient shall be in writing and shall discuss:
(1) the basis for the denial;
(2) if applicable, the "right of review" and how to exercise that right; and
(3) the right to file a complaint to the Health Clinics or HHS and how to exercise that right.

b. If the individual desires to exercise the right of review, the Health Clinics shall follow the steps listed in the definition of right of review, comply with the decision of the designated reviewing official, and send a written letter to the patient discussing:
(1) the basis for the denial and
(2) the right to file a complaint to the Health Clinics or HHS and how to exercise that right.

***Right of review**. This right of review is only applicable when the ground for denial is based on subparagraph g of that definition and the individual has requested a review of that denial. The*

right of review involves the Health Clinics designating a licensed health care professional, who was not directly involved in the initial denial determination, to review the initial denial decision.

The designated reviewing official will deny access only when, through the exercise of professional judgment, he or she determines one of the following:
a. that the access requested is reasonably likely to endanger the life or physical safety of the patient or another person;
b. that the access requested is reasonably likely to cause substantial harm to a person referenced in the record (other than a health care provider); or
c. that the access to a personal representative of the patient is reasonably likely to cause substantial harm to the patient or another person.

6. When the Decision is to Provide Access.

a. The access to be provided shall be in the form and format requested by the patient, if it is readily producible. Otherwise, it may be provided in either:

(1) a readable hard copy form or
(2) any other format as agreed to by the Health Clinics and patient.

Note: If the PHI that is the subject of a request for access is maintained in one or more designated record sets electronically and if the patient requests an electronic copy of such information, the Health Clinics must provide the patient with access to the PHI in the electronic form and format requested by the patient, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by the Health Clinics and the patient.

b. Reasonable, cost-based fees may be charged, but not in excess of the maximum fees established by Illinois law. Fees may be for:

(1) Labor for copying the PHI requested by the patient, whether in paper or electronic form;
(2) Supplies for creating the paper copy or electronic media, if the patient requests that the electronic copy be provided on portable media; and
(3) Postage, when the patient has requested the copy to be mailed.

Note: Illinois law at 735 ILCS 5/8-2001(d) and 8-2006 provides that charges for copying may not exceed the amount determined annually by the Illinois Comptroller as published on the Comptroller's website, which is:
http://www.ioc.state.il.us/office/fees.cfm

Although Illinois law permits a handling fee, the HIPAA Privacy Rule does not. Accordingly, handling fee may not be charged.

** Records retrieved from scanning, digital imaging, electronic information or other digital format do not qualify as microfiche or microfilm retrieval for purposes of calculating charges.*

** For electronic records, retrieved from a scanning, digital imaging, electronic information or other digital format in a electronic document, a charge of 50% of the per page charge for paper copies listed above. This per page charge includes the cost of each CD Rom, DVD, or other storage media.*

** Records already maintained in an electronic or digital format shall be provided in an electronic format when so requested. If the records system does not allow for the creation or transmission of an electronic or digital record, then the facility or practitioner shall inform the requester in writing of the reason the records can not be provided electronically.*

Note: Illinois law at 740 ILCS 110/4(b) provides that while "a reasonable fee may be charged for duplication of a record" containing mental health information, " when requested to do so in writing by any indigent recipient, the custodian of the records shall provide at no charge to the recipient.. one copy of any records in its possession whose disclosure is authorized under this Act."

Right to Amend PHI.

1. With limited exceptions, a patient has the right to have the Health Clinics amend PHI or amend a record about the patient that is contained in a designated record set for as long as the PHI is maintained in the designated record set.

> ***Designated record set****. "Designated record set" means the health records of patients, billing records of patients, and other designated groups of records about patients that are maintained by or for the Health Clinics and used by the Health Clinics to make decisions about patients.*

2. To exercise this right, the patient must make the request in writing (the Health Clinics has a form to be used for this purpose).

3. Within 60 days of receiving the written request that includes a reason to support the requested amendment, an authorized member of the Health Clinics workforce shall:

a. grant the requested amendment to the extent it does not meet the definition of "grounds for denial" and/or

b. deny the requested amendment to the extent it meets the definition of "grounds for denial."

Note: A 30-day extension is allowed if the University notifies the individual of the reasons for the delay and the expected completion date. This notice must be sent prior to expiration of the initial 30-day period. Only one extension is allowed.

Grounds for denial*. A request for amendment will be denied when the PHI or record that is the subject of the request is any of the following:*
1. was not created by the Health Clinics; unless the patient provides a reasonable basis to believe that the originator of PHI is no longer available to act on the requested amendment;
2. is not part of the designated record set;
3. would not be available for inspection under the right of access; or
4. is accurate and complete.

4. When Amendment is Granted (in whole or in part). If the Health Clinics grants the requested amendment, in whole or in part, it must:

a. make the appropriate amendment to the PHI or record that is the subject of the request for amendment by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment.

b. timely inform the patient that the amendment is granted and obtain the patient's identification of and agreement to have the Health Clinics make reasonable efforts to inform and provide the amendment within a reasonable time to:

(1) persons identified by the patient as having received PHI about the patient and needing the amendment; and

(2) persons, including business associates, that the Health Clinics knows have the PHI that is the subject of the amendment and that may have relied, or could foreseeably rely, on such PHI to the detriment of the patient.

5. When the Amendment is Denied (in whole or in part). If the Health Clinics denies the amendment, in whole or in part:

a. The Health Clinics must provide the patient with a written letter using plain language that contains:

(1) the basis for the denial;

(2) the patient's right to submit a written statement disagreeing with the denial and how the patient may file such a statement;

(3) a statement that, if the patient does not submit a statement of disagreement, the patient may request that the Health Clinics provide the patient's request for amendment and the denial with any future disclosures of the PHI that is the subject of the amendment; and

(4) a description of how the patient may complain to the Health Clinics [including providing the telephone number of the Privacy Officer] or to the Department of HHS [including a reference to 45 C.F.R. § 160.306].

b. The Health Clinics must permit the patient to submit a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. The length of this statement is limited to two pages.

c. The Health Clinics may prepare a written rebuttal to the patient's statement of disagreement. Whenever such a rebuttal is prepared, the Health Clinics will provide a copy to the patient who submitted the statement of disagreement.

d. The Health Clinics will identify the record or PHI in the designated record set that is the subject of the disputed amendment and append or otherwise link the patient’s request for an amendment, the Health Clinics denial of the request, the patient’s statement of

disagreement, if any, and the Health Clinics rebuttal, if any, to the designated record set.

e. For future disclosures of the PHI:

(1) If a statement of disagreement has been submitted by the patient, the Health Clinics will include the amendment-related material that was appended to the record (or an accurate summary of that information) with any subsequent disclosure of the PHI to which the disagreement relates.

(2) If the patient has not submitted a written statement of disagreement, the Health Clinics will include the amendment-related material that was appended to the record (or an accurate summary of that information) with any subsequent disclosure of the PHI only if the patient has requested such action.

6. Receiving Notices of Amendment. When the Health Clinics is informed by another health care provider or health plan of an amendment to an individual's PHI, it must amend the PHI in its designated record set as provided in the above paragraph entitled "When Amendment is Granted (in whole or in part)."

Right to Receive an Accounting of Disclosures of PHI.

1. With limited exceptions, a patient has the right to receive an accounting of disclosures of PHI about that patient made by Health Clinics in the six years prior to the date on which the accounting is requested.

2. The Health Clinics will create an "accounting log" to document certain disclosures of PHI, as required by the HIPAA Privacy Rule. This requirement does not apply to:

a. disclosures made for TPO (treatment activities, payment activities, or health care operations activities);
b. disclosures made to that patient;
c. disclosures that occurred incident to a permitted use or disclosure;
d. disclosures made pursuant to a valid written authorization;
e. disclosures to persons involved in the individual's care or other notification purposes; and/or
f. any disclosure occurring over 6 years ago.

Accounting log. *An accounting log documents certain disclosures of PHI. The log includes:*
1. the date of the disclosure;
2. the name of the entity or person who received the PHI and, if known, the address of such entity or person;
3. a brief description of the PHI disclosed; and
4. a brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure.

Note 1. In certain circumstances, if, during the period covered by the accounting, the Health Clinics has made multiple disclosures of PHI to the same person or entity for a single purpose, the accounting may, with respect to such multiple disclosures, provide (i) the above information for the first disclosure during the accounting period; (ii) The frequency, periodicity, or number of the disclosures made during the accounting period; and (iii) The date of the last such disclosure during the accounting period.

Note 2. If, during the period covered by the accounting, the Health Clinics has made disclosures of PHI for a particular research purpose for 50 or more individuals, the accounting may, with respect to such disclosures for which the PHI about the patient may have been included, provide:
(a) the name of the protocol or other research activity;
(b) a description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records;
(c) a brief description of the type of PHI that was disclosed;
(d) the date or period of time during which such disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period;
(e) the name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and
(f) a statement that the PHI of the patient may or may not have been disclosed for a particular protocol or other research activity.

If the University provides an accounting for research disclosures per Note 2, the Health Clinics shall, at the request of the patient, assist the patient to make contact with the entity that sponsored the research and the researcher.

Note 3: Illinois law at 740 ILCS 110/13 provides that whenever mental health information is disclosed without consent, "a notation of the information disclosed and the purpose of such disclosure or use shall be noted in the recipient's record together with the date and the name of the person to whom disclosure was made or by whom the record was used."

3. To exercise this right, the patient must make the request in writing (the Health Clinics has a form to be used for this purpose).

4. Within 60 days of receiving the written request, the Health Clinics shall grant the request by providing a copy of the accounting log regarding certain disclosures of that patient's PHI occurring within the past 6 years unless there has been a "temporary suspension of the right to an accounting."

Temporary Suspension of Right to an Accounting *shall occur as follows:*

a. Disclosures to a health oversight agency or law enforcement official (as provided in the HIPAA Privacy Rule § 164.512(d) or (f)), during the time period specified by such agency or official, if such agency or official provides the Health Clinics with a written statement that such an accounting to the patient would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required.

b. If the agency or official statement described above is made orally, the Health Clinics shall:

(1) document the statement, including the identity of the agency or official making the statement;

(2) temporarily suspend the patient's right to an accounting of disclosures subject to the statement; and

(3) limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement is submitted during that time.

Right to Request Further Restrictions.

1. A patient has the right to request that the Health Clinics restrict:

a. uses or disclosures of PHI about the patient for TPO (treatment, payment, or health care operations activities);

b. disclosures of PHI to persons directly involved in the patient's care or payment; and/or

c. disclosures of PHI to notify persons responsible for individual's care.

2. To exercise this right, the patient must make the request in writing (the Health Clinics has a form to be used for this purpose).

3. An authorized member of the Health Clinics workforce shall review the request and make a determination using the applicable standard in paragraphs 4 or 5 below.

4. Specific Circumstances.

a. If the request meets all of the criteria in this paragraph 4.a, then the Health Clinics must agree to the request to not disclose certain PHI. : The criteria are:

(1) the request is to restrict disclosure of certain PHI,
(2) to a health plan,
(3) for purposes of carrying out payment or health care operations,
(4) the disclosure of that PHI is *not* required by law, and
(5) that PHI only pertains to a health care item or service for which the Health Clinics has been paid in full from a source other than the health plan

b. The following guidance shall be used to apply paragraph 4.a:

(1) If a purported payment is dishonored (e.g. check does not clear) or if a promised payment is not tendered, after making reasonable efforts to obtain payment, then the Health Clinics may bill the health plan due to the lack of fulfillment of criteria of 4.a(5). Normally, the Health Clinics will require payment at the time the request for the restriction is made.

(2) While separate records systems need not be created to segregate the PHI covered by this agreed-to restriction, some method must be used to flag that PHI to ensure such PHI is not inadvertantly disclosed to the health plan (e.g. due to a later audit by the health plan).

(3) The required-by-law criterion includes a requirement of law to disclose information to Medicare or other Federal health plan to comply with conditions of participation. Regarding mandatory claim submission requirements, if there is a recognized exception to that requirement, that exception must be used when applicable.

(4) If the requested restriction relates to PHI that is only part of a bundled billing code, the Health Clinics must determine whether the law permits unbundling.

(a) If so, then the patient will be counseled about the potential ability of the health plan to determine the restricted PHI and provide the opportunity for the patient to modify (if desired) the request to not restrict any PHI or restrict more PHI.

(b) If not, then the patient will be counseled that the request cannot be agreed to because the Health Clinics is not able to unbundle the billing code and then provide the patient the opportunity to make another request to restrict PHI relating to the entire billing code.

(5) The Health Clinics will counsel the patient that:

(a) the agreed restriction does not extend to restricting the disclosure to other health care providers for treatment purposes and those other health care providers might seek reimbursement from the health plan for services or items rendered, and

(b) if the patient desires those other health care providers to restrict disclosures to the health plan, then the patient would need to make that request directly with the other health care provider.

(6) In the event a prior restriction is in place and then, subsequently, the patient obtains additional health services or items that are themselves billable to the health plan but the Health Clinics needs to disclose PHI that is subject to the prior restriction (e.g. to support medical necessity or other billing criteria for the subsequent billing code), then the Health Clinics will provide the opportunity for the patient to request a restriction relating to the subsequent additional health services or items, consistent with paragraph 4.a. If the patient declines to request the additional restriction (consistent with paragraph 4.a), then the Health Clinics may disclose to the health plan the information that was subject to the original restriction to the extent determined to be minimum necessary to comply with the billing code criteria.

5. All Other Circumstances. If paragraph 4 does not apply, then the Health Clinics is not required to agree to the request and may deny the request without providing a reason.

a. If the Health Clinics agrees to the requested restriction, then it shall document its agreement and then shall not use or disclose PHI in violation of such restriction, except that,

(1) if the patient who requested the restriction is in need of emergency treatment and the restricted PHI is needed to provide the emergency treatment, the Health Clinics may use the restricted PHI, or may disclose such PHI to a health care provider, to provide such treatment to the patient;
(2) if the restricted PHI is disclosed to a health care provider for emergency treatment as described above, the Health Clinics must request that such health care provider not further use or disclose the PHI;
(3) a restriction agreed to by the Health Clinics is not effective to prevent uses or disclosures required to be made to HHS or as described in 45 C.F.R. § 164.512.

b. The Health Clinics may terminate its agreement to a restriction, if:

(1) the patient agrees to or requests the termination in writing;
(2) the patient orally agrees to the termination and the oral agreement is documented; or
(3) the Health Clinics informs the patient that it is terminating its agreement to a restriction, except that such termination is only effective with respect to PHI created or received after it has so informed the patient.

Right to Request Alternate Confidential Communications.

1. A patient has the right to request to receive communications of PHI from the Health Clinics by alternative means or at alternative locations.

2. To exercise this right, the patient must make the request in writing (the Health Clinics has a form to be used for this purpose).

3. The Health Clinics shall accommodate reasonable requests by the patient but may require the following information or statement prior to granting the request:

a. how payment, if any, will be handled; and

b. specification of the desired alternative means or location(s).

Note: The Health Clinics may <u>not</u> require an explanation from the patient as to the basis for the request as a condition of providing communications on a confidential basis.

ADMINISTRATIVE AND MISCELLANEOUS PROVISIONS

<u>Breach and Related Notification Procedures</u>. Certain notifications must be made following a "breach" of PHI.

1. Definitions.

a. Breach means the acquisition, access, use, or disclosure of PHI that:

* is in violation of the HIPAA Privacy Rule and

* compromises the security or privacy of the PHI.

except the following is *<u>not</u>* considered a breach::

* Any unintentional acquisition, access, or use of PHI by a member of the Health Clinics workforce or person acting under the authority of the Health Clinics or its business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the HIPAA Privacy Rule; or.

* Any inadvertent disclosure by a person who is authorized to access PHI at the Health Clinics or its business associate to another person authorized to access PHI at the Health Clinics or business associate, and the PHI received as a result of such disclosure is not further used or disclosed in a manner not permitted by the HIPAA Privacy Rule; or

* A disclosure of PHI where the Health Clinics or its business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

in determining whether a violation of the HIPAA Privacy Rule has compromised the security or privacy of the PHI, the following analysis shall be used:

* It is presumed to have been comproismed (and therefore a breach);

* that presumption may be overcome when the Health Clinics or its business associate demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

(i) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

(ii) The unauthorized person who used the PHI or to whom the disclosure was made;

(iii) Whether the protected health information was actually acquired or viewed; and

(iv) The extent to which the risk to the PHI has been mitigated.

Note: It is relevant to determine whether the PHI is secured in a manner that the PHI is rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111–5.

2. Internal Notification to Privacy Officer. Any person in the Health Clinics workforce that discovers or suspects a breach of PHI must immediately notify the Health Clinics Privacy Officer.

3. Determinations and Actions of Privacy Officer. Upon notification of a discovered or suspected breach of PHI, the Privacy Officer will:

a. determine whether the situation meets the definition of breach;

b. and if so, implements the proper external notifications along with other mitigating actions;

c. and then document those determinations made and any notifications and other mitigating actions taken.

4. External Notifications to Each Individual.

a. Timing. External notifications must be made without unreasonable delay and in no case longer than 60 days from the first discovery of the breach. However, if a law enforcement official states to the Health Clinics that a notification of breach would impede a criminal investigation or cause damage to national security, then:

(1) If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or
(2) If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement is submitted during that time.

b. Content. External notifications use plain language and contain the following:

(1) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
(2) A description of the types of unsecured PHI that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
(3) Any steps individuals should take to protect themselves from potential harm resulting from the breach;
(4) A brief description of what the Health Clinics is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
(5) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

c. Form.

(1) Written notice.

(a) Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as information is available.

(b) If the covered entity knows the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by first class mail to either the next of kin or personal representative of the individual. The notification may be provided in one or more mailings as information is available.

(2) Substitute notice. In the case in which there is insufficient or out-of-date contact information that precludes written notification to the individual, a substitute form of notice reasonably calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual under paragraph 4.c.(1)(b).

(a) In the case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then such substitute notice may be provided by an alternative form of written notice, telephone, or other means.

(b) In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice shall:

(i) Be in the form of either a conspicuous posting for a period of 90 days on the home page of the Web site of the covered entity involved, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and

(ii) Include a toll-free phone number that remains active for at least 90 days where an individual can learn whether the individual's unsecured PHI may be included in the breach.

(3) Additional notice in urgent situations. In any case deemed by the Health Clinics to require urgency because of possible imminent misuse of unsecured PHI, the Health Clinics may provide information to individuals by telephone or other means, as appropriate, in addition to the required notice provided.

5. External Notifications to Media. For a breach of unsecured PHI involving more than 500 residents of a State, the Health Clinics will notify prominent media outlets serving the State or jurisdiction by directly delivering a press release (mere posting of a general release on the Health Clinics website is not sufficient for external notification to media. The timing and content of this notification are the same as described in paragraphs 4.a and 4.b. The Health Clinics is not obligated to incur any cost of any media broadcast regarding the breach. Any choice by the media to not publish or any failure by the media to publish does not render the notice provided by the Health Clinics insufficient.

6. External Notifications to HHS.

a. Breaches involving 500 or more individuals. For breaches of unsecured PHI involving 500 or more individuals, the Health Clinics shall, contemporaneously with other required external notifications, provide notification to HHS in the manner specified on the HHS Web site.

b. Breaches involving less than 500 individuals. For breaches of unsecured PHI involving less than 500 individuals, the Health Clinics shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide notification to HHS for breaches occurring during the preceding calendar year, in the manner specified on the HHS Web site.

Modifications to HIPAA Policies and Procedures. These policies and procedures are subject to continuous review and improvement. Any recommendation for improvement should be submitted to the Privacy Officer.

1. Modifications that are required due to a change in the law will be implemented immediately; then promptly followed by a revision of the Notice of Privacy Practices (NOPP), if warranted.

2. Other modifications that would alter the contents contained in the Notice of Privacy Practices may be implemented only after revision of the NOPP. Implementation of the modification will include appropriate training for the members of the workforce affected by the modification.

Document Retention. The Privacy Officer will retain for six years from the date it was last in effect a copy (either in paper or electronic form) of the following:

1. Any written Health Clinics policy, procedure, or similar document that is designed to promote compliance with the HIPAA Privacy Rule by the Health Clinics (e.g. this Manual).

2. Any document, form, or other writing that was created or used as a basis to comply with the provisions of this Manual or the HIPAA Privacy Rule (e.g. BAAs, valid written authorization forms, etc).

De-Identified Health Information.

1. General Rule. Health information that is de-identified is not PHI and is, therefore, not subject to the requirements of this Manual or the HIPAA Privacy Rule.

2. Criteria for De-Identified Health Information. The Health Clinics may determine that health information is de-identified only if:

a. A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:

(1) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an patient who is a subject of the information; and

(2) Documents the methods and results of the analysis that justify such determination; or

b. The Health Clinics does not have actual knowledge that the information could be used alone or in combination with other information to identify a patient who is a subject of the information and all of the following identifiers of the patient or of relatives, employers, or household members of the patient, are removed:

(1) Names;

(2) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:

(a) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and

(b) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

(3) All elements of dates (except year) for dates directly related to an patient, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

(4) Telephone numbers;

(5) Fax numbers;

(6) Electronic mail addresses;

(7) Social security numbers;

(8) Medical record numbers;

(9) Health plan beneficiary numbers;

(10) Account numbers;

(11) Certificate/license numbers;
(12) Vehicle identifiers and serial numbers, including license plate numbers;
(13) Device identifiers and serial numbers;
(14) Web Universal Resource Locators (URLs);
(15) Internet Protocol (IP) address numbers;
(16) Biometric identifiers, including finger and voice prints;
(17) Full face photographic images and any comparable images; and
(18) Any other unique identifying number, characteristic, or code, except as permitted below in the paragraph entitled "Re-Identification."

3. Re-Identification. The Health Clinics may assign a code or other means of record identification to allow information de-identified under this section to be re-identified by the Health Clinics, provided that:

a. Derivation. The code or other means of record identification is not derived from or related to information about the patient and is not otherwise capable of being translated so as to identify the patient; and

b. Security. The Health Clinics does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

4. The HIPAA Privacy Rule Applies. The requirements of this Manual and the HIPAA Privacy Rule would apply if:

a. de-identified information is re-identified; or

b. there is a disclosure of a code or other means designed to enable the de-identified information to be re-identified.

Business Associates and Business Associate Agreements (BAAs).

1. The General Rule. Members of the Health Clinics workforce may disclose PHI to a business associate of the Health Clinics and may allow a business associate to create or receive PHI on its behalf, if satisfactory assurances are obtained that the business associate will appropriately safeguard the information.

Business associate means, with respect to the Health Clinics, a person who:
(i) On behalf of the Health Clinics or of an organized health care arrangement in which the Health Clinics participates, but other than in the capacity of a member of the workforce of the Health Clinics or arrangement, creates, receives, maintains, or transmits PHI for a function or activity regulated by the HIPAA Privacy Rule, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety

activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing; or

(ii) Provides, other than in the capacity of a member of the workforce of the Health Clinics, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of PHI from the Health Clinics or arrangement, or from another business associate of the Health Clinics or arrangement, to the person.

A covered entity may be a business associate of another covered entity.

Business associates include:

(i) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to PHI to the Health Clinics and that requires access on a routine basis to such PHI.

(ii) A person that offers a personal health record to one or more individuals on behalf of the Health Clinics.

(iii) A subcontractor that creates, receives, maintains, or transmits PHI on behalf of the business associate.

Business associates do not include:

(i) A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual.

(ii) A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of § 164.504(f) of the HIPAA Privacy Rule apply and are met.

(iii) A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting PHI for such purposes, to the extent such activities are authorized by law.

(iv) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (i) of the main definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (ii) of the main definition to or for such organized health care arrangement by virtue of such activities or services.

2. Documentation of the Business Associate Agreement (BAA). The Health Clinics must document the satisfactory assurances through a written contract or other written agreement or arrangement with the business associate that is compliant with the HIPAA Privacy Rule. These are often termed business associate agreements or BAAs. Guidance on BAA requirements is contained in the appendix.

3. Violation of Terms of Agreement. If the Health Clinics knows of a pattern of activity or practice of the business associate that constituted a material breach or violation of the BAA, the Health Clinics must take reasonable steps to cure the breach or end the violation, as applicable, and, if such steps are unsuccessful, then either:

a. terminate the contract or arrangement, if feasible; or

b. if termination is not feasible, reported the problem to HHS.

4. Review of BAAs. The Privacy Officer will review all proposed BAAs for compliance with this Manual and the HIPAA Privacy Rule. A BAA checklist is The Privacy Officer will also maintain a copy of current BAAs.

Training for Workforce.

1. Initial. All members of the Health Clinics workforce shall complete training within a reasonable period after joining the workforce (typically 30 days). The specifics of the training will be determined by the Privacy Officer and will consist of at least an introductory level of information about the HIPAA Privacy Rule and this Manual. The Privacy Officer will retain documentation of the completion of this training.

2. Annual Refresher. Members of the Health Clinics workforce who routinely request, use, or disclose PHI will normally complete refresher training on an annual basis. The specifics of the training will be determined by the Privacy Officer and will consist of at least an introductory level of information about the HIPAA Privacy Rule and this Manual. The Privacy Officer will retain documentation of the completion of this training.

3. Changes in this Manual or Law. Upon implementing a modification of practices or procedures due to a change in this Manual or applicable law, persons whose duties are affected by that modification are required to complete training specific to that modification as soon as practicable. The Privacy Officer will retain documentation of the completion of this training.

4. Additional Training for Mental Health Information. Due to the additional requirements imposed by the Illinois Mental Health and Developmental Disabilities Confidentiality Act (740 ILCS 110), additional training on that law will occur for personnel involved with mental health information.