KU THE UNIVERSITY OF KANSAS

2024

Clinic Policies & Procedures Regarding Privacy & Security of Patient Information

The University of Kansas

6/2024

CLINIC POLICIES AND PROCEDURES
REGARDING PRIVACY & SECURITY
OF PATIENT INFORMATION

Table of Contents

PART I. GENERAL INFORMATION

I. Introduction

This document is intended to provide University Clinics operating on (or pursuant to the control of) the KU Lawrence Campus (KUL) with general guidance and standards regarding the handling of health information in any form or format. Because Clinic activities vary and Clinics are subject to numerous laws pertaining to the handling of health information, no document can address every question or circumstance. **Questions pertaining to the information contained in this document may be addressed to the HIPAA Privacy Officer at (913) 588-0940 or the Information Security Office at (785) 864-9003.**

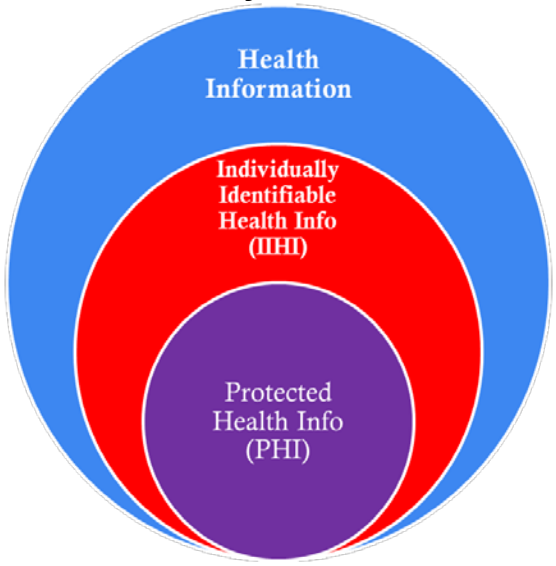
As a general matter, efforts have been made to provide information that is generally consistent with the many state and Federal laws relating to the privacy of health information, including the Health Insurance Portability and Accountability Act of 1996 ("HIPAA")[1]. In many cases, these state and Federal laws are consistent. There may be circumstances, however, where conflicts arise. At KU, we endeavor to address information privacy holistically rather than segmented by the various laws or regulations. The focus is on personally identifiable information (PII) used in our teaching, research and service, and its status as public or non-public, rather than financial, health, consumer, etc.

A. Health Information Privacy.

1. US Coverage. Most Health information privacy is considered to be addressed by HIPAA. Under HIPAA, the privacy of individually identifiable health information (IIHI) is addressed by the HIPAA Privacy Rule; the HIPAA Security Rule provides standards for the privacy and security of electronic health information; and the Breach Notification Rule requires both Covered Entities and Business Associates to notify following a breach of unsecured protected health information.[2]

2. KU Coverage. This Clinic Handbook generally addresses two (2) areas of health information privacy in Part I and Part II of this Handbook: 1) Part I will deal with "***Uses and Disclosures***" of Individually identifiable health information in the Clinics; and 2) Part II will address "***Patient Rights***" regarding the IIHI in the Clinics. These are the areas that are commonly referred to when dealing with HIPAA and apply well to FERPA/student treatment records. Part III of the Clinic Handbook addresses information Security, an integral part to ensuring Privacy, and Part IV addresses Additional Administrative Requirements.

B. University Clinics.



A common area of confusion is surrounding the application of law to health information. There are actually 3 levels of "health information" that are referred to by law and as referenced in the Handbook Glossary.

1. HIPAA *only* applies to PHI, which is a specifically defined term under the statute that means individually identifiable health information that relates to a person's past, present or future health condition or the provision of health care, but only where the information is ***created, received, maintained, or transmitted*** by a "Covered Entity." See 45 CFR 160.103.

C. FERPA.

1. Where HIPAA and FERPA Intersect[3]. HIPAA does not apply to health information that is subject to FERPA (that means, health information maintained by the University in student education records, including student health clinic records). Where student records[4] are involved, Clinics must take steps to ensure that their practices are consistent with the requirements of state and Federal laws pertaining to such records, including the Family Educational Rights and Privacy Act of 1974 as Amended. See 20 USC 1232g; 34 CFR Part 99.

2. Treatment Record. If a Clinic discloses a KU student's "treatment records" (as that term is used in FERPA and as further defined by KU's Student Records Policy) for purposes other than treatment, the treatment records are no longer excluded from the definition of "education records" and are subject to all other *FERPA* requirements, including the right of the eligible student to inspect and review the records. In order to use or disclose the student treatment records for reasons other than treatment, the student must provide written authorization to the disclosure.[5] Once the treatment record is disclosed for purposes other than treatment, the record changes to a standard "education record" and FERPA principles apply.

3. Clinic. While the health records of students at the University Clinic may be subject to *FERPA*, KU is a *HIPAA* covered entity with designated health care components (i.e. Clinics) that may provide health care to *non*students. When those Clinics are providing health care to non-students or clients of the University, the resulting IIHI of the clinic's *non*student patients is subject to the *HIPAA* Privacy Rule. Thus, for example, postsecondary institutions that are subject to both *HIPAA* and *FERPA* and that operate clinics open to students, staff, or the public, are required to comply with *FERPA* with respect to the health records of their student patients, and with the *HIPAA* Privacy Rule with respect to the health records of their *non*student patients. See Joint Guidance, Page 7, and Example 7.

D. Applicable Laws.

Although this guidance is not subject to only one Federal or State law on privacy and security of health information, it does recommend the adoption of the most stringent levels of data management when such data is identifiable.

II. Hybrid Entity Status

A University may be a "Covered Entity" which must comply with the HIPAA Privacy Rule when dealing with non-student patients and clients in certain areas of the institution. As such, the University may designate itself as a "Hybrid Entity"[7] meaning that only "Healthcare Components" (Covered Components) must comply with all aspects of the HIPAA Privacy Rule; those units not designated as Covered Components, but that may have individually identifiable health information are not subject to HIPAA[8], but may be subject to FERPA, GLBA, state breach laws or University policy and should comply accordingly.

A. Covered Components. The following health care components are designated as "Covered Components" on the KUL, for purposes of HIPAA, including:

1. The Schiefelbusch Speech-Language-Hearing clinic (SLH).
2. Child and Family Services Clinic (CLAS).
3. Little Steps at the Edna A. Hill Child Development Center.
4. The Counseling and Psychiatric Services clinic (CAPS) (to the extent treatment services are provided to non-students.)

B. Other clinics. These units will be required to comply with the Clinic Policies and Procedures as set forth in this minimum standard (or floor), including:

1. Center for Psychoeducational Services (CPS) (Education) / Outcomes, Assessment Services, and Intervention Supports (OASIS)
2. The Counseling and Psychiatric Services clinic (CAPS) (to the extent treatment services are provided to students.)
3. Achievement and Assessment Institute (AAI) (Education)
4. Educational Testing Services (CLAS/CAPS)
5. Energy and Weight Balance Clinic
6. Department of Athletics, Training Services
7. KU Psychological Clinic
8. School of Music, Music Therapy Department

C. Supporting Units/Services.

Units within the University that perform functions or services on behalf of a Covered (healthcare) Component or clinic will be treated as "covered"

for purposes of providing private and secure resources to the Covered Components.

These service units include at least the following units:

1. Information Technology (Computing Services, Customer Support Services, Network Operations, IT Security Office)
2. Controller's Office
3. Office of the General Counsel
4. Office of Audit, Risk & Compliance
5. Provost's Office (Provost & Vice Provosts)
6. KU Police Department (investigations and monitoring of units)
7. Office of Research (payment to subjects)
8. Office of the University Registrar
9. Life Span Institute (Information Technology Services)
10. Institutional Review Board Office
11. Research Integrity Office
12. CRMDA (Center for Research Methods and Data Analysis) (REDCap Service)

These Supporting Units may be required to follow this manual or more specific unit procedures, prior to addition or update of this manual, and thus may not be identified above.

D. Safeguards. All Covered Components, clinics and Supporting Units should develop and incorporate appropriate safeguard procedures that correspond to the needs and/or function of the component to assure compliance with the health information privacy regulations or university policies, including accountability.

1. Updates. All components are responsible for updating component- specific procedures as needed to comply with changes in the law or university policy.
2. Reporting & Documenting. All components are responsible for reporting and documenting violations and for providing appropriate mitigation procedures within their unit.

3. Enforcement & Mitigation. All components are responsible for implementing disciplinary measures for violations of information protection policies in accordance with clinic standard operating procedures and university policy.

E. Training. All staff and faculty, volunteers, and student employees of all Covered Components and Supporting Units will be considered members of the "workforce" of the University for purposes of training requirements.[9] As such, these Components and Units must successfully complete and document training on at least an annual basis for existing workforce members and introductory training for new workforce members.

PART II. USE AND DISCLOSURE OF IIHI

I. General Rules Governing Use and Disclosure of IIHI

The goals of HIPAA, FERPA and other health information laws or policies is to assure that an individual's identifiable health information remains private and secure through reasonable and appropriate standards and safeguards while not stopping or hindering the necessary information flow to provide excellent care or services. Although not every clinic is a covered component, University clinics with identifiable health information need good practices to meet other laws and the University goal: balance clients' needs, legal requirements, and institution missions for teaching, research and service to provide the best possible service.

A. General Standard. Under HIPAA, a Covered Entity (CE) may only use or disclose PHI as permitted or required by the Privacy Rule or Individual authorization. Non-covered units of the University similarly need to use/disclose IIHI with care and scrutiny.

1. Permitted Uses & Disclosures for PHI. The designated CEs are permitted to use or disclose PHI in any of the following six (6) ways:

    a. To the individual;

    b. For treatment, payment, or health care operations (typically referred to as "TPO")[10];

    c. For a use or disclosure otherwise permitted or required by HIPAA[11]

    d. Pursuant to and in compliance with a valid authorization (from individual/patient)[12];

    e. Pursuant to an agreement for individual opportunity to agree/object is not required[13]; and

f. As permitted by and in compliance with HIPAA, such as de-identification.[14]

2. Required Uses & Disclosures for PHI. The University as a CE is required to disclose PHI when:

   a. To an individual, when requested under, and required by Access of Individuals to PHI or Accounting of Disclosures[15]; and

   b. When required by the HHS Secretary to investigate or determine the covered entity's compliance with HIPAA.

B. Minimum Necessary Standard. The minimum necessary standard is a **central principle** of the Privacy Rule addressing the need to have limits on use and disclosure of IIHI. The CE's workforce should only use and disclose the minimum amount of information necessary to satisfy the job-related task at hand or to provide continuity of care for the patient or client.

1. Access and uses. The minimum necessary standard is based on good business practices, and standards of confidentiality in use today for Clinics and health care providers to limit unnecessary access to and disclosure of individual's private health information.

   a. *Role-based access.* As part of the Minimum Necessary standard protocols, the Clinic should develop role-based access policies and procedures that limit the PHI access to workforce members to the degree necessary for them to perform their respective duties.

   b. *Reasonable Efforts.* The standard is to make reasonable efforts to meet the Minimum necessary standard. As such, Clinics should consider from the outset the use or disclosure of the information in the context of the need of information, and consider factors to limit the use and disclosures of IIHI, such as limit the workforce members that access the information, limit what is collected, retained, accessed or used. These minimum standards must be tailored to the needs of and implemented by Clinics.

2. Disclosures and Requests for Disclosures. Outside requests for a copy of the ***entire medical record*** is common but such disclosures should be avoided unless specifically authorized by the patient or client. A reasonable exception is when an outside provider is requesting the entire record for continuity of care.

   a. *Routine Requests or Disclosures.* For routine or recurring requests or disclosures, a Clinic must develop and

implement standard protocols that limit the IIHI requested or disclosed to the amount minimally (reasonably) necessary to achieve the purpose of the Disclosure for Payment or Operations. The protocols should address identification of the types of IIHI to be disclosed, the types of persons who would receive the IIHI, and the conditions that would apply to such access.

b. *Non-Routine Requests or Disclosures.* For all other requests or Disclosures, a Clinic must develop criteria designed to limit the IIHI requested or disclosed to the information reasonably necessary to accomplish the purpose for which the request or Disclosure is sought and review each request for Disclosure on an individual basis in accordance with such criteria.

3. Reasonable Reliance. Clinic Workforce members may assume that a request for IIHI is for the minimum necessary information when:

   a. Making Disclosures to public officials who claims that the information requested is the minimum necessary for the stated purpose;

   b. The information is requested by an entity that is covered under HIPAA;

   c. The information is requested by a professional who is a member of Clinic's Workforce, or is a Business Associate for the purpose of providing professional services to the Clinic, if the professional claims that the information requested is the minimum necessary for the stated purpose(s) (i.e. minimum necessary reflects and is consistent with professional judgment and standards); or

   d. The information is requested for Research purposes and the Clinic has been provided with the documentation required to permit Disclosure of the information for Research purposes, as outlined below.

4. Exceptions. The Minimum Necessary Standard outlined in this Section is not required where the use/disclosure of PHI is as follows:

   a. Uses or Disclosures made to, or requested by, a healthcare provider for Treatment purposes;

   b. Disclosures made to the Individual/Patient about him or herself;

   c. Uses or disclosures required by law;

d. Uses or disclosures made pursuant to an Authorization initiated by the patient or client;

e. Disclosures to the U.S. Department of Health and Human Services (DHHS), when disclosure of information is required under the Privacy Rule for enforcement purposes; or

f. Uses or disclosures required for compliance with applicable laws.

Please contact the Office of the General Counsel regarding questions where uses and disclosures required by law may not require an Authorization.

C. Incidental Disclosures. Privacy laws, such as HIPAA, are not intended to impede customary and essential communications and practices and thus do not require that all risk of incidental Use or Disclosure be eliminated. These rules permit certain incidental Uses and Disclosures that occur as a by-product of another permissible or required Use or Disclosure, as long the Clinic has applied "reasonable safeguards" and "minimum necessary" policies and procedures to protect an individual's privacy. For example, it is acceptable to call-out a person's first name or last name in the waiting area but it should be unnecessary to call-out the person's first AND last name.

D. Safeguards. Reasonable safeguards will vary from Clinic to Clinic. Therefore, a Clinic should analyze its own needs and circumstances, such as the nature of the Patient information (IIHI) it creates, receives, transmits or maintains, and **assess** the potential risks to patients' privacy. The units should also take into account the potential effects on patient care and may consider other issues, such as the financial and administrative burden of implementing particular safeguards. HIPAA does not require the elimination of all possible risks because that would be an impossible goal and financially unattainable.

Examples of reasonable safeguards to avoid inappropriate disclosures may include, but are not limited to:

- Speaking quietly when discussing a Patient's condition with family members in a waiting room or other public area;
- Avoiding use of individual's full name in public areas;
- Isolating and/or locking file cabinets or record storage rooms;
- Providing additional security, such as passwords, password protected screensavers, and timed log-outs on computers storing or accessing personal information; or
- Regular updates and reminders to the workforce in staff meetings, newsletters, etc.

E. Personal Representatives. The rights of a Personal Representative of a Patient are limited only by the scope of the Personal Representative's legal authority (e.g., Guardianship or a Durable Power of Attorney for Healthcare.) State or other law must be consulted to determine the authority of a Personal Representative to receive or access the Patient's IIHI.

The following additional guidelines apply when dealing with a Personal Representative:

1. General Rule. Incapacitated Patients must have a Personal Representative identified in order to make decisions regarding the Patient's IIHI. Clinics must treat a Patient's Personal Representative as the Patient for purposes relating to the Use and Disclosure of IIHI, consistent with the scope of the Personal Representative's legal authority. Thus, if the representative has broad authority of a living individual to make decisions related to health care, then that representative is usually treated as the individual for all purposes under the Privacy Rule, unless an exception applies. If, however, the authority is limited or specific to only specific health care decisions, the representative is to be treated as the individual only with respect to the IIHI involved in the representation.

2. Minors Who Are Not KU Students. Ordinarily, Kansas' law regarding the confidentiality of information pertaining to minors should be followed. In most cases, a parent is the Personal Representative of a Minor child and can exercise the Minor's rights with respect to the minor's information. Regardless of whether a parent is the Personal Representative, a Clinic may disclose to a parent or provide the parent with access to, a Minor child's information when and to the extent it is permitted or required by State or other laws. Conversely, a parent is not the Personal Representative of the Minor, and does not have the ability to exercise the Minor's rights regarding Use and Disclosure of IIHI when:

    a. State or other law expressly prohibits the parent from accessing such information;

    b. State or other law does not require the consent of a parent or other person before a Minor can obtain a particular health care service, and the Minor Consents to the health care service (e.g. diagnosis and Treatment of a sexually transmitted disease/illness, family planning services and/or alcohol/drug abuse Treatment). In these circumstances the Minor is permitted to acknowledge receipt of the Clinic's Notice of Privacy Practice and to authorize Use and

Disclosure of their IIHI specific to the services to which they are Consenting;

c. A court determines or other law authorizes someone other than the parent to make Treatment decisions for the Minor; or

d. A parent agrees to a confidential relationship between the Minor and the physician. If the Clinic has a practice of entering into such agreements with parents, documentation of the agreement must be placed in the Patient's medical record.

e. If it is believed that a Patient, including an emancipated Minor, has been or may be subjected to domestic violence, abuse or neglect by the Personal Representative, or that treating a person as a Patient's Personal Representative could endanger the Patient, the Clinic may choose not to treat that person as the Personal Representative, if doing so (in the professional judgment of a licensed health care professional) would not be in the best interests of the Patient.

3. Minors Who ARE KU Students. It is and has been the practice at KU to extend the rights of controlling their own IIHI to all KU-enrolled students regardless of their age. Therefore, even enrolled students who are below the age of majority in Kansas (18 years of age) are entitled to authorize the use and disclosure of their medical information. An exception to this practice would be where the information is part of the Student Education Record and is therefore subject to FERPA.

4. Deceased Patients. PHI created during the life of a Patient continues to be protected from Use and Disclosure after death of the Patient for at least 50 years, unless otherwise permitted by law. IIHI that is subject to FERPA as part of the Student Education Record is subject to University policy.

F. Verification. Clinic Workforce members must verify the identity of all persons requesting IIHI and the authority of that person to have access, unless the identity and the authority of such person is known. If state or Federal law requires certain documentation to be presented prior to a Disclosure, Clinic Workforce members may rely on documentation, statements or representations that on their face meet the applicable requirements. The following additional guidelines apply:

1. Patients. Verification of Patients requesting their own IIHI should include asking to see a photo ID and asking appropriate questions

to verify the identity of the person, e.g., date of birth, social security number, place of birth, etc.

2. Personal Representatives. Verification of Personal Representatives should include asking for a photo ID and a copy of the documentation supporting his or her legal authority. If there is no formal documentation, reliance upon professional judgment to determine whether the appropriate relationship exists is permissible.

3. Public Officials. The identity of public officials may be verified by presentation of an agency identification badge, other official credentials, other proof of government status, or by provision of a written request on appropriate government letterhead. The authority of a public official may be verified by a written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority.

4. Imminent Threats to Safety. Verification is not required if there is an imminent threat to health or safety and the Disclosure is made to a person reasonably able to prevent or lessen the threat. In such emergencies, reasonable reliance on verbal representations is appropriate.

5. Note Red Flags Requirement. The University has adopted the Identity Theft Prevention Plan (aka "Red Flags Rule") for clinics or areas that collect identifiable information on customers and that bill for services.[16]

    a. Requirements include adopting procedures to identify and address Identity Theft of Covered Accounts by 1) Identifying relevant events that may occur in the clinic that would cause the workforce to suspect that someone's identity has been compromised and is being used by someone other than the individual; these are referred to as "Red Flags;" 2) Documenting how to detect and respond to Red Flags in unit policies & procedures; 3) Responding to any detection of Red Flags; 4) Updating of unit procedures regularly; 5) training of staff; and 6) reviewing oversight on Service provider agreements.

    b. *Designate Privacy Liaison*. Each unit or clinic should have a designated Privacy Liaison to coordinate activities. This may be the Privacy Officer or another person as available.

    c. *Security Procedures.* The unit must implement appropriate security procedures as well, such as 1) Asking the client or patient for a photo ID card, 2) Obtaining university approval

to store student ID photos within the system used to document care rendered and then using those photos to positively identify the individual.

G. Designated Record Sets (DRS). Federal and in some cases state laws provide a Patient with the right to access or amend his or her medical information. See sections XII and XIII below. These rights are limited to IIHI contained in the Clinic's DRS, as identified by the Clinic. The DRS includes any record containing medical, billing, enrollment, or Payment information used by or for the Clinic to make decisions about Patients, including such information specifically created, received, stored and/or transmitted by Business Associates of the Clinic when acting on behalf of the Clinic. Clinics must document the type of records to be included in the DRS, the basic content of the DRS, the location of the DRS and a description of any information in the DRS that Patients will not have a right to access or amend.

The following are examples of information that should <u>not</u> be considered part of the Designated Record Set (DRS) including:

1. Health information that is not used to make decisions about Patients or information that the Patient does not have a right to access based on state or federal law;
2. Psychotherapy Notes;
3. Quality improvement or risk management records;
4. Research documentation; (Note: When IIHI is created or obtained by the Clinic/Researcher for a Clinical trial, the Patient's access rights can be suspended while the Clinical trial is in progress, provided the Research participant agreed to this denial of access when Consenting to participate in the Clinical trial. Certain limitations/restrictions may apply.)
5. Appointment schedules;
6. Information compiled in reasonable anticipation of, or for Use in civil, criminal or administrative action or proceeding, e.g., incident reports used to identify problems and implement correction action;

H. Disclosures to Other Components of the University.

1. <u>General Rule.</u> Disclosures to other University Clinics/components from a Covered Component/Clinic should be treated as disclosures to a legally separate entity. In other words, unless law expressly permits such Disclosure, the transfer of IIHI between such areas should be allowed only to the same extent such a Disclosure is permitted to an outside entity. An exception is allowed where two units have a written agreement to share such

information for continuity of care and where this is stipulated in the Notice of Privacy Practices for those units.

2. Supporting Units/Services. In some cases, Clinics may need to Disclose IIHI to other departments or units of the University who provide Business Associate - type support services to the Clinic.

    a. Where such support services involve the disclosure of IIHI, the University department involved in providing the support service must identify those individuals (or units) who require access to the IIHI stored by the Clinic.

    b. The University department or component that receives the information must take appropriate steps to limit:

        1) The sharing (disclosure) of IIHI beyond the individuals identified,

        2) The information that is disclosed to the minimum necessary, and

        3) Ensure that such individuals receive education regarding the requirements of applicable state and Federal privacy laws.

    c. The University departments providing such support services to Clinics may not Use or Disclose IIHI that they create, receive, store, or transmit from, or on behalf of, a Clinic in a way prohibited by these guidelines, or state or Federal law.

    d. Support services that fail to properly use or disclose IIHI are subject to required sanctions under University policy and procedures.

    e. Support services are also subject to risk analysis on a regular basis.

    f. Supporting units/services should adopt policies and procedures as required by this Handbook, or other laws and regulations, train their employees accordingly and comply with any Breach reporting or notification requirements.

I. Disclosures to Insurers/Health Plans. Clinics should take into account the "minimum necessary" standard in disclosing information to health insurers, limiting the information as appropriate. However, clinics must also work with insurers reasonably and in a business relationship to facilitate the processing of claims.

J. Business Associates. A Business Associate (BA) is typically a person or entity other than a workforce member, who performs a function or activity on behalf of the CE. Clinics may disclose IIHI to a Business Associate that is not affiliated with the University, and may allow such a

Business Associate to create, receive, store, view or transmit IIHI on its behalf, ***only if*** the Clinic (University) obtains prior satisfactory written assurances that the Business Associate will appropriately safeguard the information. This includes all of the following steps:

1. Contracts, aka Business Associate Agreements (BAA).

    a. Such contracts must be in the format approved for such purposes by the University's General Counsel, and in the case of HIPAA Covered Components of the University, must comply with the requirements of HIPAA. Such contracts must be updated when associated regulations are modified by the U.S. Department of Health and Human Services.

    b. If a contract or relationship changes during the term of the agreement or you are made aware of any legal or regulatory changes regarding Business Associates, you should contact the Office of the General Counsel to discuss if updating the agreements is needed.

    c. Clinics acting as a Business Associate or that contract with third parties as a Business Associate must obtain review of the agreement by the appropriate reviewing counsel at KUCR or KUL Office of the General Counsel.

2. Violations.

    a. If a Clinic becomes aware of a violation by the Business Associate and it is unable to correct the problem, the Clinic should discuss terminating the BAA with KU General Counsel. The violation should also be reported to the KUL HIPAA Privacy Officer.

    b. Any report of breach of PHI or IIHI by the Clinic acting as a Business Associate must be reported to the KUL HIPAA Privacy Officer and the Information Security Officer for assistance prior to notification of the Covered Entity or Business Associate that is contracting with the Clinic.

K. Subcontractor. Business Associates will include any third party or subcontractor that is performing the function or services of a Business Associate on behalf of a Covered Entity or another Business Associate, whether or not the term "Business Associate" or "BA" is specifically stated in the agreement. The Subcontractor must do the following:

1. Immediately report breaches of privacy/security to the CE and to the KUL HIPAA Privacy Officer and the Information Security Officer;

2. Comply with Administrative, Physical and Technical safeguards of HIPAA security rule and maintain policies, procedures and documentation of security activities;
3. Only use or disclose IIHI as specified by the agreement, and only the minimum necessary amount;
4. BA's who violate HIPAA security standards are now subject to civil and criminal penalties as if they were the Covered Entity; and
5. Maintain records of workforce training, policies & procedures, and documentation of any incident.

II. Use and Disclosure of IIHI Pursuant to Consent---Treatment, Payment or health care Operations (TPO)

A. Clinics must obtain a Patient's written Consent to Use and Disclose information about him or her for purposes relating to **Treatment, Payment or health care Operations.** This should be done in concert with the patient having an opportunity to read the Notice of Privacy Practices.

B. Clinics have discretion to design a Consent process that works best for their own operations and patients/clients, ***provided that*** the Consent process and Consent document are consistent with state and federal laws applicable to the Clinic.

C. Depending upon the information contained in the "Consent" document used by the Clinic, the Consent document may not be sufficient valid permission to Use or Disclose IIHI in certain specific contexts, e.g., releases of certain records pertaining to students, releases of certain information pertaining to alcohol/drug abuse or HIV/AIDS, etc. Such situations may require a more detailed or specific "Authorization" (See section V below), or where other requirements or conditions may exist for the Use or Disclosure of IIHI (e.g., the patient's Right to Request a Privacy Protection).

D. Consent documents generally differ from Authorizations to use or disclose IIHI under the Privacy Rule (45 CFR § 164.508).

III. Use and Disclosure of IIHI Pursuant to Written Individual Authorizations

Written Authorizations, in the form outlined in section V.E. below, are required *prior to* Disclosure of IIHI in the circumstances set forth below. A Patient may revoke an Authorization at any time, provided the revocation is in writing. A revocation is not valid for Disclosures made prior to receipt of the revocation. A copy of the Authorization and a revocation, if any, must be given to the Patient and a copy retained in the Patient's Designated Records Set (DRS).

As identified, special Authorizations are required prior to Disclosure of IIHI for these situations:

A. Psychotherapy Notes. Use or Disclosure of Psychotherapy Notes generally requires a prior written Authorization. Exceptions include Use or Disclosure to carry out the following Treatment, Payment or health care Operations: 1) Use by the originator of the Psychotherapy Notes for Treatment; 2) Use or Disclosure by the Clinic for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family or individual counseling; or 3) Use or Disclosure for defense in a legal action or other proceeding brought by the Patient.

B. Marketing & Sale.

1. Marketing is defined as a communication about a product or service that encourages recipients of the communication to purchase or use the product or service. Marketing also includes the sale of information so that the purchaser of the information may make a communication about its own product or service.

2. Not Marketing. A communication is **not** considered "marketing" if it is in the form of a face-to-face communication by a Clinic to the Patient (or other individual) or if it consists of a promotional gift of nominal value provided by the Clinic. Additionally, a communication is not considered "marketing" if it is made for Treatment of the Patient, case management or care coordination of the Patient, or to recommend alternative treatments, therapies, healthcare providers or settings of care to the Patient.

3. Use or Disclosure of IIHI for marketing purposes generally requires a prior written Authorization of the Individual/patient to receive such communications.

4. Remuneration. The Clinic/CE cannot receive "remuneration" for making non-marketing communications, except where the communication:

    a. Describes only a drug/biologic currently prescribed for individual and payment is reasonable for communication;

    b. Made by Clinic under valid authorization of individual;

    c. Communication made by Business Associate for a Covered Entity/Clinic and consistent with the Business Associate Agreement; and

    d. The Written communication from the clinic must provide individual/patient an opportunity to elect not to receive further such communication ("Opt Out" option.)

5. No Sale of PHI[17] or IIHI.

    a. Clinics (whether acting as a Covered Component or a Business Associate) are prohibited from selling PHI. This includes the direct or indirect receipt of remuneration in exchange for any PHI without a valid authorization from individual that includes a specification of whether PHI may be sold by entity receiving the PHI;

    b. Exceptions to prohibition of Sale of PHI may include:

        1) Public health activities;

        2) Research (if price reflects cost of preparation and transmittal of data for such purpose);

        3) Treatment of individual

        4) Sale, transfer, merger, consolidation of Clinic with another CE

        5) Remuneration from CE to BA for activities that BA performs involving the PHI at the specific request of CE; or

        6) Providing individual copy of their PHI pursuant to request; As otherwise determined,

    NOTE: Prior to a Sale of PHI or IIHI, the Clinic or Business Associate must review this plan with the KUL HIPAA Privacy Officer and/or KUL General Counsel.

6. Communication Exceptions.

    a. *Refill Exception*. To fall within the refill exception under marketing, there are two requirements to review:

        1) Is the communication about a currently prescribed drug/biologic? And

        2) Does the communication involve financial remuneration, and if so, is it reasonable?

    Please consult the KUL HIPAA Privacy Officer for more information on these exceptions.

    b. *Appointment reminders* are not marketing communications. However, the patient or client *should* authorize the communication prior to receiving such reminders. At the very least, Clinics should adopt a process and include this in the NPP.

C. Research. Use or Disclosure of IIHI for Research activities requires a written Authorization, unless one of the exceptions to individual Authorization for Research is met. Research Uses and Disclosures are addressed more fully below (see Section VIII).

D. HIV/AIDS. Use or Disclosure of IIHI pertaining to Human Immunodeficiency Virus / Acquired Immunodeficiency Syndrome (HIV/AIDS) generally requires prior written Authorization, unless one of the exceptions to state statutes regarding confidentiality of HIV/AIDS information is met. See K.S.A. 65-6001 et seq.

E. Alcohol or Drug Abuse Treatment. Use or Disclosure of IIHI pertaining to substance abuse patients generally requires a written Authorization. The requirements of the Federal statute pertaining to records of substance abuse patients maintained in connection with the performance of any federally assisted specialized alcohol or drug abuse program must be followed. See 42 U.S.C. 290dd-2 and 42 C.F.R. Part 2.

F. Treatment Facilities. Use or Disclosure of IIHI by a treatment facility such as a state licensed community mental health center, community service provider for the developmentally disabled, psychiatric hospital or state institution for the mentally retarded, generally requires use of a written Authorization, unless one of the exceptions to the state statutes regarding "treatment facilities" is met. See K.S.A. 65-5601 et seq.

G. Other Disclosures. Unless the Disclosure is permitted or required by law without an Authorization, an Authorization must be obtained from the Patient prior to the Disclosure. Examples requiring an Authorization include (but are not limited to) Disclosures of IIHI to an employer or life insurance company (where IIHI is provided by someone other than the patient directly to the recipient).

H. Authorization Content and Format. Authorizations must be written in plain language and must contain the core elements below. An Authorization is not valid if it has not been completed in accordance with these requirements (and this procedure), or if any material information in the Authorization is known by the Clinic to be false.

1. Information Description. A description of the information to be Used or Disclosed that identifies the information in a specific and meaningful fashion;

2. Names. The name or other specific identification of the person(s), or class of persons, authorized to make the requested Use or Disclosure;

3. Identification. The name or other specific identification of the person(s), or class of persons, to whom the Clinic may make the requested Use or Disclosure;

4. Description of each purpose of the requested Use or Disclosure. The statement "at the request of the individual" is a sufficient description of the purpose when a Patient initiates the Authorization and does not, or elects not to, provide a statement of the purpose;

5. Expiration date or an expiration event that relates to the Patient or the purpose of the Use or Disclosure. An Authorization is not valid if the expiration date has passed or the expiration event has occurred. (Typically, 1 year is the maximum time frame.)

6. Signature of the Patient and date. If the Authorization is signed by the Patient's Personal Representative a description of such representative's authority to act for the Patient must be provided.

7. Revocation Language. Statements adequate to place the Patient on notice of his or her right to revoke the Authorization in writing. The document must also include: 1) information regarding any exceptions to the right to revoke or a reference to the Clinic's Notice of Privacy Practices ("NPP"); 2) a description of how the Patient may revoke, and if applicable, the ability or inability to condition treatment on the Authorization; and 3) a statement regarding the potential for the information to be subject to re-disclosure by the recipient (and no longer subject to legal protection).

8. Compound Authorizations. Generally speaking, Authorizations may not be required as a Condition of Treatment. The purpose of the limit on compound authorizations was to enable patients to decline actions described in an authorization, yet still receive treatment, services or benefits outlined in the Authorization. An Authorization for Use or Disclosure of IIHI may not be combined with any other document to create a compound Authorization, except as follows:

    a. *Research*. An Authorization for the Use or Disclosure of IIHI for Research may be combined with any other type of written permission for the same Research, including another Authorization for the Use or Disclosure of IIHI for such Research or Consent to participate in such Research; certain restrictions may apply and other specific requirements for research Authorizations must be met. See 45 CFR Sec. 164.508(b)(3)(iii). The Authorization, however, must be specific in detailing the research studies (including future uses or storage for databases or repositories) to sufficiently notify the participant in the Study.

        1) **Compound Authorization.** The compound Authorization for Patient participation however,

cannot be used when treatment or intervention is involved. See "Research Repositories, Databases and the HIPAA Privacy Rule," http://privacyruleandresearch.nih.gov/research_repositories.asp

2) ***Future* research use and disclosure of PHI** no longer has to be study-specific. The authorization for use and disclosure of PHI for future research must describe the purposes in a manner such that the individual may expect that his/her PHI could be used or disclosed for such future research. The IRB is appropriate for additional guidance in this area.

3) **Decedent's PHI** is still covered by the Privacy Rule after their death in the same manner and under the same Authorization requirements as a living individual or patient. The PHI privacy period of coverage ceases 50 years after the individual's death. 45 CFR 160.201.

b. *Psychotherapy Notes*. An Authorization for a Use or Disclosure of Psychotherapy Notes may be combined only with another Authorization for a Use or Disclosure of Psychotherapy Notes.

c. *Other*. An Authorization, other than an Authorization for the Use and Disclosures of Psychotherapy Notes, may be combined with another Authorization, except when an Authorization has been required as a condition for Treatment.

9. Conditioning Authorizations. A Clinic may not condition Treatment on the signing of a privacy Authorization, except in the context of the provision of Research-related Treatment or for health care that is solely for the purpose of creating IIHI for Disclosure to a third party (e.g., employer drug testing).

I. Fundraising. Any CE that performs "fundraising" must have a policy and procedure limiting the IIHI that will be used without an authorization in these efforts (e.g. demographic information, dates that health care was provided), and how individuals will be provided an opportunity to opt-out of receiving future fundraising communications.

IV. Use and Disclosure of IIHI without Written Consent or Authorization

The following are examples of additional Uses and Disclosures that are permitted or required by law **without** written Consent or Authorization of the Individual, including:

A. Health Oversight Activities. A Clinic may disclose IIHI to a health oversight agency for oversight activities that are authorized by law. Health oversight agencies include, but are not limited to, agencies of the U.S. Government or the State of Kansas~~,~~ that are authorized by law to oversee the health care system or government programs in which health information is necessary to determine eligibility or compliance. Examples of oversight activities include audits, inspections, licensure or disciplinary actions, and oversight of entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards.

B. Public Health Activities.

1. Clinics may Disclose PHI, without Authorization, to public health authorities who are legally authorized to receive such reports for the purpose of preventing or controlling disease, injury, or disability, e.g. the reporting of a disease or injury and conducting public health surveillance, investigations, or interventions. Further, Clinics may disclose PHI to a person subject to FDA jurisdiction, for public health purposes related to the quality, safety or effectiveness of an FDA-regulated product or activity for which that person has responsibility. Examples include but are not limited to, collecting or reporting adverse events, product defects or problems, tracking FDA-regulated products, enabling product recalls, repairs or replacement or look-back and conducting post-marketing surveillance. See 45 CFR §164.512(b)(1)(iii).

2. Disclosure of treatment records of a student to an agency, however, may be a disclosure subject to FERPA (the Family Educational Rights and Privacy Act of 1974, as amended) and should ***first*** be cleared through the KUL General Counsel's Office prior to any release of information.

C. Abuse, Neglect or Domestic Violence Reporting. Clinics may disclose IIHI to report known or suspected abuse or neglect, if the report is made to a public health authority or other appropriate governmental authority that is authorized by law to receive such reports. All Kansas state laws that apply to the reporting of abuse and neglect must be followed. The Clinic should promptly inform the Patient that such a report has been or will be made **unless** the victim is a child, or the Clinic Workforce member believes that informing the Patient would place the Patient at risk of serious harm, **or** the Clinic Workforce member would be informing a Personal Representative believed to be responsible and as such would not be in the best interests of the Patient.

D. Judicial and Administrative Proceedings. Requests for IIHI in response to an order of a court or administrative tribunal, or in response to a subpoena, discovery request, or other legal process, must be

referred immediately to the University General Counsel's Office for assistance. Time is of the essence in handling these matters.

E. Threat to Health and Safety. A Clinic may Use or Disclose IIHI if it is believed that the Use or Disclosure is necessary to prevent or lessen a serious and imminent threat to the health and safety of a person or the public and the Disclosure is made to a person who can reasonably prevent or lessen the threat, including the target of the threat. An eligible student's *treatment records* may be disclosed for purposes other than the student's treatment under the Health and Safety exceptions to written consent under 34 *CFR* § 99.31(a) or with the student's written consent under 34 *CFR* § 99.30.

F. Disclosures for Law Enforcement Purposes. Clinics may Disclose IIHI to comply with laws that require the reporting of certain types of wounds or other injuries. In addition, Clinics may Disclose IIHI to address emergency situations or threats to health and safety as outlined in section E above. In other contexts, requests for IIHI by law enforcement authorities should be referred to the KUL General Counsel's Office for assistance. If the Clinic is the first point of contact with an investigative agent who is delivering a subpoena, search warrant, or other court order, the Clinic Workforce member should ask the agent for permission to contact a supervisor and the KUL General Counsel to assist with reviewing the paperwork. The KUL General Counsel should be contacted immediately for assistance. If the agent refuses to wait before executing the instructions detailed in a search warrant or court order, the KUL General Counsel should still be contacted immediately, but the Clinic should not inhibit the progress of the investigation.

G. Disclosures for Workers' Compensation. Clinics may disclose IIHI as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs. Remember, that PHI excludes IIHI in employment records held by a covered entity in its role as employer (e.g., workers' compensation records, sick leave records, etc.) For questions or concerns consult the KUL HIPAA Privacy Officer as other laws may apply.

H. Cooperation with DHHS. The Privacy Rule requires that Covered Entities cooperate with efforts by the Department of Health and Human Services (HHS), Office for Civil Rights (OCR), to investigate complaints or otherwise ensure compliance. Any requests for information or investigation by HHS/OCR should immediately involve the KUL General Counsel and the KUL HIPAA Privacy Officer.

I. KU Student Records with Health Information. FERPA, not HIPAA, directs the requirements of handling KU student IIHI in the "Education Record" that is contained in a clinic or non-clinic record set. See Section VIII of this Policy Manual; or see the Joint Guidance on the Application of the Family Educational Rights and Privacy Act (FERPA) and the Health

Information Portability and Accountability Act of 1996 (HIPAA) to Student Health Records, US Department of Health and Human Services & US Department of Education.

V. Use and Disclosure of IIHI Requiring an Opportunity for the Patient to Agree or to Object

A. Individuals involved in the Patient's Care.

1. When the Patient is Present. Clinics may Disclose IIHI without written Consent or Authorization to a family member, close personal friend of the Patient, or any other person identified by the Patient, who is involved in the Patient's care or Payment for the Patient's care if the Clinic has provided the Patient with an opportunity to agree or object to the person's involvement in their care and access to their IIHI. An account of the discussion must be recorded in the Patient's medical record. It is not necessary to verify the identity of a person when the person accompanies a Patient. The Patient's act of involving the other person(s) in his or her care is sufficient evidence of their involvement in the Patient's care.

2. When the Patient is not present. If the Patient is not present, or cannot agree or object because of the Patient's incapacity or emergency circumstances**,** then **a Clinic physician or other authorized healthcare provider** may disclose the patient's IIHI to a family member or personal friend, **when in their professional judgment** such Disclosure is in the patient's best interest and the IIHI which is disclosed is limited to the minimum necessary and relevant to the person's involvement with the patient's care. If there is any uncertainty that a patient desires to have a particular family member or personal friend involved in his or her medical care, treatment, or payment of medical services, Clinic Workforce Members should either verify the identity and authority of that person's status as a Personal Representative, or obtain and appropriately document the patient's agreement that the patient does in fact desire his or her IIHI to be Disclosed to this individual.

B. Disaster Relief Activities.

Clinics may disclose IIHI to Federal, state, or local government agencies engaged in disaster relief activities, as well as to private disaster relief or disaster assistance organizations (such as the Red Cross) authorized by law or by charter to assist in disaster relief efforts. However, except in emergency situations, disclosures to disaster relief agencies cannot be made without informing the Patient and giving him or her an opportunity to agree or object. (e.g. Hurricane Katrina 2005)

C. **Victims of a Crime.** Clinics may disclose IIHI about a Patient who is suspected of being a victim of a crime, **in response to a law enforcement request**, if the Patient agrees to the Disclosure. The Patient's agreement must be noted in the Patient's DRS. If the Clinic is unable to obtain the Patient's agreement, the Clinic should not release such information without first consulting the University General Counsel's Office for assistance, unless the Disclosure is necessary to respond to an emergency situation or to prevent or lessen a serious and imminent threat to the health and safety of a person or the public.

D. **Payment in Full at time of Service.** Patients have a right to make a payment in full at time of service and to also request that no further disclosure of the IIHI be made for payment purposes. The Clinic is obligated to abide by this request.

VI. Use and Disclosure for Educational Purposes

Clinics are permitted to use and disclose IIHI to carry out educational activities and training programs in which students, trainees, and/or health care practitioners learn under supervision to practice or improve their skills as health care providers, to the extent such uses and disclosures are permitted by law. If applicable, such uses and disclosures must be described in the Clinic's Notice of Privacy Practices (NPP). Students, residents and fellows are permitted to access and use IIHI on a need-to-know basis and may have full access for Patients with whom they are clinically involved during their education and training.

A. **Use on Clinic Premises.** Information obtained through the course of treatment and used beyond the scope of the Patient's treatment for the Clinic's educational/training purposes, must be stripped of direct identifiers (e.g. name, address, phone) whenever practicable.

B. **Removal from Clinic Premises.** IIHI may not be removed from the Clinic premises for educational purposes or otherwise included in classroom presentations or discussions outside the Clinic unless approved by the Clinic ***and*** the actual information is de-identified in one of two methods. Contact the KUL HIPAA Privacy Officer for a discussion of this topic before such actions are taken.

C. **Disposal.** All Patient information used or disclosed for educational purposes must be returned to the medical record or destroyed in accordance with the procedures developed by the Clinic to provide for Patient privacy (e.g. placed in the secure shredding bin designated by the Clinic for this purpose). Placing such materials in trash receptacles or other publicly accessible containers (including publicly accessible recycling) is never acceptable. Similarly, use of electronic records for educational purposes should never be retained on a hard drive, portable or mobile device (e.g. laptops, Smartphones, tablets, USB devices, etc.), in "cloud" storage or other location not approved by the KUL Information

Security Officer. Simple deletion of the electronic file (e-file) is **not** sufficient. For more information on "wiping" or "sanitizing" electronic devices, please consult the I.T. Help Desk for assistance at 785-864-8080.

D. **Unaffiliated students and other health care professionals.** Unaffiliated students (including those admitted or visiting but not yet "in attendance" at the University) and/or community health care professionals may participate in the training/education activities of the Clinic in accordance with University and unit or Department policies and procedures. An affiliation agreement or other appropriate agreement between the University and the group that sponsors the individual must be in place. Such individuals shall be required to sign a confidentiality agreement and complete or demonstrate satisfactory HIPAA training.

E. **External Rotations.** Students/trainees who are on external rotations are required to follow the specific policies and procedures of the training site. IIHI regarding Patients/clients of the external training facilities may not be removed unless approved by the facility. Students/trainees are not Business Associates of KU, nor are KU students on external rotations Business Associates of the Medical Facility/Hospital. Send any agreements to the KUL Office of the General Counsel for review and approval prior to signature.

F. **Accreditation Activities.** Students/trainees should consult with the Unit's Privacy Liaison or KUL HIPAA Privacy Officer if they are asked to disclose identifiable information about Patients to document a training experience. Clinics must maintain Business Associate Agreements with any external organizations that require use or disclosure of PHI to accredit the Clinic's educational programs.

VII. Business Associates (BA).

A Business Associate is typically a person or entity other than a workforce member, who performs a function or activity on behalf of the Clinic involving the creation, receipt, maintaining, viewing, use and/or disclosure (transmission) of PHI, or who provides services to or for the Clinic involving the disclosure of PHI. Included as Business Associates are entities that Creates, Receives, Maintains, Views or Transmits PHI, or an entity that performs those functions on behalf of BA, such as a subcontractor to the BA.[18]

A. **Clinics as BAs.** From time to time, a clinic of the University or a Researcher may serve as a Business Associate of a Covered Entity (or of another Business Associate) in the performance of certain activities or research. When the Clinic or PI is a Business Associate, the unit must comply with all aspects of the Business Associate Agreement (BAA) or other arrangement as provided to the University. This will include at minimum following the standards set forth in this manual.

1. When the Clinic is a BA, the clinic must use or disclose PHI only as permitted by the agreement and by the law

    a. When required by the HHS Secretary to investigate or determine the business associate's compliance with HIPAA

    b. To the covered entity, individual, or individual's designee, as necessary to satisfy a covered entity's obligations under § 164.524(c)(2)(ii) and

    c. With respect to an individual's request for an electronic copy of protected health information.

2. Clinics may disclose IIHI to a Business Associate that is not affiliated with the University, and may allow such a Business Associate to create, receive, store, or transmit IIHI on its behalf, ***only if*** the Clinic obtains prior satisfactory written assurances in the form of a BAA or other Agreement with confidentiality provisions reviewed and approved by the General Counsel's Office.

B. Business Associate Agreement from Clinic to third party.

1. Approved format and content. Business Associate Agreements (BAA) from the University to external parties must be in the format approved for such purposes by the General Counsel's Office. The General Counsel's Office should also be consulted regarding content of each BAA.

2. Compliance with HIPAA. Where a HIPAA Covered Component of the University needs a BAA with another party, the agreement must comply with HIPAA and include at least the following:

    - Limitations on the Use and Disclosure of such information
    - Reasonable and appropriate Safeguards
    - Breach handling and reporting to the University requirements, and
    - Flow down terms from agreements that the University must comply with from funding or other sources.

C. Purchase or Use of product or service by KU/Clinic. KU clinics should have procedures for the purchase or obtaining of any service or function that may touch, access, use, or potentially disclose IIHI.

1. Purchasing. Although the purchase of a system or service may not reach the threshold required by KU Purchasing for an RFP (Request for Proposal), an agreement involving the creation, use,

transmission or storage of IIHI (including service of a program, software, or hardware that stores or accesses IIHI) must have proper review prior to execution. The review should be performed by the General Counsel's Office to ensure minimum controls are in place to comply with law or University policy.

2. Agreements for "free" products, tools, or services.
   The fact that a service or product does not have a fee attached does not mean that such product is compliant with law or KU policy.

3. All agreements (funded or not) should be reviewed and approved by the General Counsel's Office for use of any system capable of the creation, use/access, disclosure, transmission, or storage of IIHI.

D. Compliance.

1. Regular Review of Existing Contracts. Clinics should maintain documentation of all Business Associates or other arrangements. Such agreements should be reviewed regularly for currency or changes that may have occurred under the law or University policy requiring amendment.

2. Accounting for Disclosures. Similarly, Clinics must include the requirements for Accounting of Disclosures for the BAs, as necessary.

3. Breach of Contract by Business Associate. If a Clinic becomes aware of a material violation of the agreement by the Business Associate, and the Clinic is unable to correct the problem, the contract should be terminated or, if termination is not possible, the violation should be reported to the Privacy Officer for the Lawrence Campus and the Office of the General Counsel for further consultation. Reasons for immediate contract termination may include the:

   a. failure of a BA to notify KU of a Breach/security incident or failing to provide either the CE or the individual access to the ePHI where required by law;

   b. failure to disclose PHI to HHS Secretary in investigations or failure to account for disclosures or otherwise comply with the Security Rule.

4. Breach or Loss of IIHI by KU, where KU is Business Associate. Each Clinic as a Business Associate, and that experiences inappropriate use/disclosure by a BA or subcontractor must be reported and managed through KU. **Immediate notification** of

the KUL HIPAA Privacy Officer or Security Officer should occur. See also Reporting Section in Part IV.

E. Business Associate for Research. (see next section).

VIII. Use and Disclosure of IIHI for Research

In order for a Clinic to conduct Research using IIHI or to Disclose IIHI to a Researcher for Research purposes, at minimum **one** of the conditions outlined in sections A through F of this section must be met. Additional information may be obtained by contacting the Institutional Review Board (IRB) Office - Lawrence Campus.

A. Individual Authorization. Written, signed privacy Authorization from the Patient has been obtained. HIPAA Covered Components of the University must comply with the HIPAA Privacy Rule's authorization requirements for use/disclosure of Protected Health Information for research. Additional or alternative requirements may apply in other contexts (e.g. use of student treatment records). Additionally, prior to any release of information, the Clinic must receive documentation that Institutional Review Board (IRB) Office - Lawrence Campus has approved the study.

B. De-identified Data. Certain Research may be accomplished through the Use of de-identified data. HIPAA Covered Components of the University must comply with the HIPAA standards for de-identification of Protected Health Information by utilizing either the Safe Harbor Method or the Expert Determination Method described in Section VII above. Alternative requirements for de-identification of data may apply in other contexts.

Note: Research involving de-identified data may be considered human subjects Research, and subject to corresponding regulations and IRB approval.

C. Limited Data Sets. A Limited Data Set ("LDS") is one in which the direct identifiers have been removed, but certain potential identifiers of the individual or of relatives, employers or household members of the individual remain.

1. HIPAA Covered Components of the University must comply with HIPAA Privacy Rule requirements for use and disclosure of Protected Health Information in a Limited Data Set (including use of a Data Use Agreement). Additional or alternative requirements may apply in other contexts.

2. Research employing a Limited Data Set <u>is</u> subject to human subjects' regulations. The project must be approved by the IRB prior to initiation.

3. The Data Use Agreement (DUA) is a legally binding agreement and must minimally have the following elements:

a. Establish the permitted uses and disclosures of the limited data set by the recipient, consistent with the purposes of the research, and which may not include any use or disclosure that would violate the Rule if done by the covered entity;

b. Limit who can use or receive the data; and

c. Require the recipient to agree to the following:

1) Not use or disclose the information, **other than as permitted by the data use agreement** or as otherwise required by law;

2) Use **appropriate safeguards** to prevent the use or disclosure of the information, other than as provided for in the data use agreement;

3) **Report** to the covered entity any use or disclosure of the information not provided for by the data use agreement of which the recipient becomes aware;

4) Ensure that any agents, including a subcontractor, to whom the recipient provides the limited data set agrees to the same restrictions and conditions that apply to the recipient with respect to the limited data set; and

4. Not to identify the information or contact the individual.
For use of a Data Use Agreement (or DUA), consider the following steps:

a. *Identify* – Identify the need for a DUA;

b. *Document* – Document the fields/systems that will be exchanged;

c. *Consistency* – Ensure that data-use-agreements are consistent with the contents and format of KU agreements that KUCR has reviewed and approved;

d. *Develop Agreement* – Engage KUCR/RGS for assistance;

e. *Review* – Review the DUA for completeness, accuracy and requirements;

f. *Submit* – Submit the DUA to KUCR/RGS for formal review and approval.

D. Reviews Preparatory to Research. In some cases, a Clinic may wish to provide a Researcher with access to IIHI to formulate hypotheses, determine feasibility of Research, or determine availability of data or Research subjects. A HIPAA Covered Component of the University must

comply with HIPAA requirements for review of Protected Health Information preparatory to research. In these situations, the Covered Component must obtain the appropriate written representations from the researcher prior to any release or access to PHI by the Researcher. A sample form for this purpose may be obtained by contacting the IRB Office. Additional or alternative requirements may apply in other contexts. Approval by the IRB may be required.

E. Waiver of Individual Authorization. A HIPAA Covered Component of the University may disclose PHI to a Researcher, without Patient Authorization from the Research subjects, ***if*** the Researcher provides the Clinic with a copy of a waiver approval form from an IRB or Privacy Board (as defined by HIPAA), waiving the HIPAA Authorization requirements. In some cases, an IRB may waive or partially waive the requirement for written authorization for Research recruitment. Waivers of authorization for use/disclosure of Protected Health Information may not be granted in cases where more stringent state or federal laws apply. Alternative requirements may apply in other contexts.

F. Research on Decedents. A HIPAA Covered Component of the University must comply with HIPAA requirements for use/disclosure of PHI of decedents for Research, including obtaining from the researcher the appropriate written representations. A sample form for this purpose may be obtained by contacting the HSCL Coordinator. Additional or alternative requirements may apply in other contexts.

1. Threshold. As of 2013, the Privacy Rule explicitly excludes from the definition of "protected health information," individually identifiable health information regarding a person who has been deceased for more than 50 years.[19] Please consult the IRB for further privacy or research requirements on decedents.

    a. During the 50-year period of protection, the Privacy Rule generally protects a decedent's health information to the same extent the Rule protects health info of living individuals.

    b. There are provisions permitting the Covered Component to disclose a decedent's health information for research purposes that are solely on the PHI of decedents, that the PHI sought is necessary for research, and at the request of the Covered Component, documentation of the death of the individuals about whom the info is sought. (45 CFR §164.512(i)(1)(iii)).

2. Student decedents. Any student education record is covered by University policy on the use and disclosure of their IIHI. See below.

G. Study Recruitment. Healthcare professionals involved in the Treatment of a Patient are allowed to provide information to the Patient regarding Research or Clinical trials without obtaining a privacy Authorization. However, if the health care professional intends to disclose the Patient's information to a third party for recruitment purposes (including Disclosure of the Patient's name to Researchers in other Clinics, units or departments of the University), a written Authorization or an IRB waiver of Authorization (if applicable) is required. The written authorization or the waiver allows the Researcher to view the Patient's IIHI in order to make a determination about study eligibility. Posting of IRB approved flyers and advertisements, so that eligible Patients may contact the Researchers directly, is acceptable.

H. Student Records. Research involving the Use or Disclosure of the IIHI and/or the educational records of students is subject to additional requirements imposed by state or Federal law, including FERPA. *Education or treatment records as provided under FERPA, 20 USC 1232g are excluded from HIPAA. See 45 CFR 160.103.* Please consult the Lawrence Campus Registrar's Office for more guidance on the use and/or disclosure of Student Education Records (e.g., treatment records) prior to the use/disclosure.

PART III. PATIENT RIGHTS

I. Patient Right to Notice of Privacy Practices

A Clinic designated as a HIPAA Covered Component of the University must provide a Notice of Privacy Practices (NPP) to its Patients at the first date of service delivery. For recurring Patients, the NPP may be provided at the initial interaction.

A. Posting. A copy of the NPP must be posted in a clear and prominent location where it is reasonable to expect Patients seeking service to read the NPP. In addition, the NPP must be prominently posted on the Clinic's website (if any) and made available for printing from the website.

B. Electronic Delivery. If the first service delivery to a Patient is delivered electronically (through the internet, through e-mail, or otherwise electronically e.g., telemedicine), the provider should send an electronic notice automatically and contemporaneously to the individual's first request for service. A Clinic may e-mail the notice to an individual if the individual agrees to receive an electronic notice and the clinic has a method to retain such documentation of that agreement. See 45 CFR 164.520(c) for the specific requirements for providing the notice. The KUL HIPAA Privacy Officer should be contacted for more information if the NPP is delivered electronically, as special rules apply.

C. Acknowledgement. Except in an emergency Treatment situation, a Clinic must make a good faith effort to obtain a written acknowledgement of receipt of the NPP. Documentation of the written acknowledgement must be retained in the DRS. If written acknowledgement cannot be obtained from the patient, the Clinic must document good faith efforts to obtain such acknowledgement and the reason why the acknowledgement was not obtained. In an emergency Treatment situation, the NPP must be provided as soon as reasonably practicable after the emergency Treatment situation.

D. NPP Content. The NPP must be written in plain language and must include certain standard elements as required by law. **The KUL HIPAA Privacy Officer prior to implementation must review NPPs.**

1. NPP content will **minimally** include:

    a. How the Clinic Uses & Discloses PHI about the individual;

    b. Individual's (Patient's) Rights with respect to the information and the individual's exercise of those rights (access, amendment, complaint);

    c. The legal duty of the component with respect to the information;

d. Whom the individual can contact about the NPP, privacy policies or complaints;

e. Effective dates of notices and revision dates (on “material changes” to the NPP);

f. A statement that certain uses and disclosures of PHI require an authorization from the subject individual, specifically 1) psychotherapy notes (if recorded or maintained by the Covered Entity), 2) PHI for marketing purposes and 3) PHI in instances constituting the sale of PHI;

g. A statement that uses and disclosures not addressed within the NPP requires a written authorization;

h. An acknowledgment that the individual may revoke any authorization granted for uses and disclosures requiring such authorization; and

i. A notice of the individual’s rights following a breach of unsecured PHI, which can be sufficiently accomplished with a statement that the individual has a right to or will receive notification of a breach of his or her unsecured PHI; and

j. A statement notifying the individual of the individual’s right to restrict—and a health care provider’s affirmative obligation to agree to restrict—disclosures of PHI to the individual’s health plan where the individual has paid for the items or services out-of-pocket and in full;

2. Special Circumstances. Clinics that seek to contact individuals to raise funds for themselves must also include a notice of such intentions and of the individual’s right to opt-out of such communications. However, the mechanism for opting out of fundraising communications does not need to be included in the NPP.

3. Summary Notice Option. NPPs must be available at the care delivery site/Clinic, but health care providers may choose to post a summary of the policy with copies of the entire policy readily available at the patient’s request. This exception cannot apply to new patients, who must be given a complete copy of the NPP and must return a good faith acknowledgment of receipt.

E. Documentation. In addition to retaining evidence of the Patients’ acknowledgment of receipt of the NPP (and good faith efforts to obtain such written acknowledgements), the Clinic must document compliance by retaining copies of any version of the NPP issued. The prior versions

should be noted by version date on the current version of the NPP and all versions retained in the Clinic Documentation.

F. **Revisions to NPP.** The Clinic must revise the NPP to reflect material changes in privacy practices. A material change may not be implemented prior to the effective date of the NPP in which a material change is reflected. The Clinic is not required to mail a revised NPP to existing patients. Rather, the Clinic must post the revised NPP in a clear and prominent location and make it available upon request to patients or other persons on or after the effective date of the revision.

II. Patient Right to Request Privacy Restriction

Patients have the right to request a restriction on Uses and Disclosures of their IIHI for Treatment, Payment or Operations. Exceptions to this right include Psychotherapy Notes, information compiled for Use in civil, criminal or administrative actions, and information that is subject to prohibition by the Clinical Laboratory Improvements Amendments (CLIA).

A. **In Writing.** A Clinic should require such requests to be made in writing.

B. **Designated Individual.** A Clinic should designate an appropriate individual to agree to any such restriction. Written requests should be routed to that individual. A Clinic is not required to act immediately and should investigate its ability to meet the request prior to agreeing to any restriction. Care must be taken to ensure that a request can be met and that the DRS is flagged per Clinic procedure.

C. **Denial of Request.** The Clinic may deny any request. The Patient must be notified of a denial. If the Clinic agrees to a restriction, the Patient must be informed that the restriction will not apply in emergency Treatment situations where the information is required to treat the Patient.

D. **Required Documentation.** The Clinic must retain documentation of the DRS that is subject to restriction; the titles of the persons or offices responsible for receiving and processing requests for restrictions, and all correspondence and associated documentation related to Patient requests, including denials.

E. **Terminating a Restriction.** A Clinic may terminate its agreement to a restriction if the Patient agrees to or requests the termination in writing or if the Patient orally agrees to the termination and the oral agreement is documented. A Clinic may unilaterally terminate the restriction if it informs the Patient that it is terminating its agreement to the restriction, however, such termination is only effective with respect to IIHI created, received, stored, or transmitted ***after*** the Clinic has informed the Patient.

F. Restriction on Disclosure to Health Plan/Payment in Full. A Clinic has the obligation to agree to restrict disclosures of PHI to the individual's health plan where the individual has paid or agrees to pay for the items or services out-of-pocket and in full. Such request should be made in writing on a form developed and used by the Clinic in the regular course of their duties.

III. Patient Right to Request Confidential Communications

Patients have the right to request to receive communications of IIHI by 1) alternative means or 2) at alternative locations. Patients may make such requests at the time of registration, at the time of a visit, or at any time during the course of care.

A. Request in Writing. A Clinic should require that Patient requests be made in writing. A Clinic may not require that Patients provide a reason for their requests.

B. Granting a Request. A Clinic must accommodate Patient requests that are reasonable. The determination of whether a request is "reasonable" must be based solely on the administrative difficulty of accommodating the request. Appropriate staff must be informed of the communication requirements so that the request can be honored.

C. Denying a Request. A Clinic may deny a request that is not reasonable, for example, but not limited to, if the Patient does not specify an alternative method of contact, that such alternative method may endanger the individual, or that such alternative method does not provide for payment methods or handling.

D. Required Documentation. The Clinic must retain documentation of the titles of the persons or offices responsible for receiving and processing requests for access by Patients, and if the Clinic grants a Patient's request, documentation of the decision by maintaining a written or electronic record of the action taken.

IV. Patient Right of Inspect and Copy of Records

A Patient (or his Personal Representative) has a general right to inspect (access) and obtain a copy of IIHI about the Patient that is contained within the Designated Record Set (DRS) maintained by the Clinic. 164.524

A. Requests in Writing. A Clinic should require requests for access to be in writing.

B. Timely Action.

1. Paper Records. A Clinic must act on a request for access no later than 30 days after receipt of the request. The Clinic may extend the time for such actions by no more than 30 days if, within the

initial 30 days, it provides the Patient with a written statement of the reasons for the delay and the date by which the Clinic will complete its action on the request. The Clinic may have only one such extension of time for action on a request for access.

2. Electronic Records. A Clinic must act on a request for access to Electronic Health Records within a reasonable time.

C. Granting a Request for Access in Whole or in Part.

1. If the IIHI is maintained in more than one location, the Clinic need only produce the IIHI once in response to a request for access.
2. The Clinic must provide the Patient with access to the IIHI in the form or format requested by the Patient, *if it is readily producible in such form or format*. For example, if the Clinic utilizes an EHR, then it should comply with reasonable requests to provide electronic records in response to the patient request. If it is not readily producible in such form or format, it must be produced in a format agreed to by the Clinic and the Patient. This does not include allowing a patient or requestor to attach any peripheral or storage device (e.g., flash drive, smartphone, etc.) to the Clinic records or computers; the Clinic controls the transfer of the data process and devices.
3. The Clinic may provide the Patient with a summary in lieu of providing access, or an explanation of the IIHI requested, if the Patient agrees in advance to such a summary or explanation.
4. The Clinic must provide the access as requested by the Patient in a timely manner, including arranging for the Patient for a convenient time and place to inspect or obtain a copy of the IIHI, or mailing the copy of the IIHI at the Patient's request. If the Patient is requesting on-site access as opposed to copies, the clinic must have a staff person present to present the PHI and to protect it from alteration, destruction or removal. A cost-based fee may be charged for the staff time required to accommodate such a request for on-site access.
5. If the Patient requests a copy of the IIHI or agrees to a summary or explanation of such information, the Clinic may impose a reasonable, cost-based fee. A fee may be charged for preparing an explanation or summary of the IIHI, if the Patient agrees to the fee in advance. State laws regarding maximum fees for copying healthcare records must be followed.

D. Denying a Request for Access in Whole or in Part.

1. Acceptable Grounds for Denial of Access WITHOUT Opportunity for Review of the Decision.

    a. *Psychotherapy Notes*. The Patient is not authorized by law to access the information, if for example, the information consists of Psychotherapy Notes or information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

    b. *Correctional Institution/Inmate*. The Clinic is acting under the direction of a correctional institution, and obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the Patient or other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate.

    c. *Research*. The information was obtained in the course of Research that includes Treatment, provided that the Patient has agreed to the denial of access when consenting to participate in the Research.

    d. *Privacy Act of 1974*. The information contained in the records is subject to the Privacy Act of 1974, as amended, if the denial of access would meet the requirements of that law.

    e. *Records of another provider*. The IIHI 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.

    f. *No information maintained*. The Clinic does not maintain the information.

2. Acceptable Grounds for Denial of Access WITH Opportunity for Review of the Decision.

    a. *Endangerment*. A licensed healthcare professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the Patient or another person;

    b. *Substantial Harm to other*. The IIHI makes reference to another person (unless such other person is a healthcare provider) and a licensed health care professional has

determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person;

c. *Substantial harm to patient*. The request for access is made by the Patient's Personal Representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such Personal Representative is reasonably likely to cause substantial harm to the Patient or another person.

3. Access to Other IIHI Requested Unless Restricted. The Clinic must, to the extent possible, give the Patient access to any other IIHI requested, after excluding the IIHI as to which the Clinic has a ground to deny access.

4. Timely Written Denial. The Clinic must provide a timely, written denial to the Patient. The denial must be in plain language and contain the basis for the denial, a statement of the Patient's right to have the decision reviewed, and, if applicable, a description of how the Patient may exercise such review rights. The letter must contain a description of how the Patient may complain to the Clinic, the Lawrence Campus HIPAA Privacy Officer, and the Secretary of the U.S. Department of Health and Human Services. In addition, if the Clinic does not maintain the IIHI, and the Clinic knows where the requested information is maintained, the Clinic must inform the Patient where to direct the request for access.

5. Review of Denial. If the Patient exercises his or her right to review of a decision to deny access, the Clinic must designate a licensed healthcare professional who was not directly involved in the denial to review the decision to deny access. The Clinic must promptly refer the request for review to such individual for review and such individual must determine, within a reasonable period of time, whether or not to deny the access requested based on the applicable standards. The Clinic must promptly provide written notice to the Patient of the official's determination, and take other action as requested to carry out the determination.

E. Documentation. The Clinic must retain documentation of the DRS that is subject to access by Patients, the titles of the persons or office responsible for receiving and processing requests for access by Patients, and all correspondence and associated documentation related to Patient requests, including denials and reviews of denials.

V. Patient Right to Request an Amendment of Records

Patients have the right to request to amend (i.e., add to or append information to) their IIHI that is contained within the DRS of a Clinic, for as long as the information is maintained by the Clinic.

A. Requests in Writing. A Clinic must require requests for amendment to be presented in writing.

B. Timely Action. A Clinic must act on a request to amend no later than 60 days after receipt. A Clinic may extend the time for such action by no more than 30 days, provided that the Clinic, within the initial 60-day period, provides the Patient with a written statement of the reasons for the delay and the date by which the Clinic will complete its action on the request.

C. Denying a Request for Amendment.

1. Grounds for Denial. The Clinic may deny a Patient's request for amendment, if it determines that the IIHI that is the subject of the request:
    a. Was not created by the Clinic (unless the Patient provides a reasonable basis to believe that the originator of the IIHI is no longer available to act on the requested amendment);
    b. Is not part of the DRS;
    c. Would not be available for access by the Patient under state or Federal law; or
    d. Is accurate and complete.
2. Written Denial. The Clinic must provide the Patient with a timely written denial that outlines the reason for the denial. The denial must contain the basis for the denial, a statement of the Patient's right to submit a written disagreement and how the Patient may file such a disagreement. The denial must also include a statement that the Patient may request that the Clinic include the request and denial with any future Disclosures of the IIHI that is the subject of the amendment; and a description of how the Patient may discuss the denial with the Clinic, the KUL HIPAA Privacy Officer (including title and telephone number), and the Secretary of HHS**. In the case of a denial involving student records protected by FERPA, additional requirements regarding review of the decision to deny the amendment may apply.**

3. Statement of Disagreement. The Clinic must permit the Patient to submit a written statement disagreeing with the denial of all or part and the basis of such disagreement. The Clinic may prepare a written rebuttal for inclusion in the DRS if a copy is provided to the Patient. The Clinic must identify the record or IIHI in the DRS that is the subject of the disputed amendment and append, or otherwise link it to, the Patient's request for an amendment, the Clinic's denial of the request, the Patient's statement of disagreement if any, and the Clinic's rebuttal if any.

4. Effect on Future disclosures. If a statement of disagreement has been submitted by the Patient, the Clinic must include the appended material, or at the election of the Clinic, an accurate summary of any such information, with any subsequent Disclosure of the IIHI to which the disagreement relates. If the Patient has not submitted a written statement of disagreement, the Clinic must include the Patient's request for amendment and its denial, or an accurate summary of such information, with any subsequent Disclosure of the IIHI **only if** the Patient has requested such action.

D. Granting a Request for Amendment.

1. The Clinic must make the appropriate amendment to the IIHI by identifying the records in the DRS that are affected and appending or otherwise providing a link to the location of the amendment. In the case where the information is stored in another medium (e.g., microfilm, microfiche) a record of the link must be filed.

2. The Clinic must inform the Patient in a timely fashion that the amendment has been accepted and obtain the Patient's identification of an agreement to have the Clinic notify the relevant persons with whom the amendment needs to be shared, as required in subsection 3 immediately below.

3. The Clinic must make reasonable efforts to inform and provide the amendment in a reasonable time to persons identified by the Patient as needing the amendment, and persons, including Business Associates, whom the Clinic knows have the un-amended information and who may have relied or could foreseeably rely on such information to the detriment of the Patient.

E. Accepting Forwarded Amendments. A Clinic that is informed by another entity of an amendment made pursuant to the requirements of state or Federal law, must accept the amendment into its DRS.

F. Required Documentation. The Clinic must retain documentation of the DRS that is subject to amendment by Patients, the titles of the persons or offices responsible for receiving and processing requests for amendment by Patients, and all correspondence and associated documentation related to Patient requests for amendment.

VI. Patient Right to an Accounting of Disclosures

A Patient has a right to receive an accounting of Disclosures (not uses) of IIHI made by a Clinic in the six (6) years prior to the date on which the accounting is requested (or for a shorter period, if requested). An accounting is generally a listing or tracking record of the disclosures made by the Covered Component regarding the patients' IIHI.

A. Exceptions. A Clinic does not have to account for Disclosures:

1. To carry out Treatment, Payment and health care Operations (TPO);
2. To Patients about themselves or their own IIHI;
3. Pursuant to an individual (patient) authorization;
4. To persons involved in the patient's care, such as a patient's Personal Representative;
5. As part of Limited Data Set (Note: must have Data Use Agreement)
6. For the Clinic's directory (if applicable) or to persons involved in the Patient's care;
7. For national security or intelligence purposes;
8. To correctional institutions or law enforcement about an inmate;
9. That occurred prior to the April 14, 2003.

B. Accounting Content. For each Disclosure, the accounting must have at least the following (or as amended by HHS) information including:

1. date of the Disclosure,
2. name of the entity or person who received the IIHI
3. address, if known, of the entity or person who received the IIHI,
4. a brief description of the IIHI disclosed, and
5. a brief statement of the purpose of the Disclosure that reasonably informs the Patient of the basis for the Disclosure.

C. Multiple Disclosures to Same Entity. If, during the period covered by the accounting, the Clinic has made multiple Disclosures of IIHI to the same person or entity for a single public policy or compliance investigation purpose, or pursuant to a single Authorization, the accounting may, with respect to such multiple Disclosures, provide the following:

1. information required under subsection B above for the first Disclosure during the accounting period;
2. frequency, periodicity, or number of the Disclosures made during the accounting period; and
3. date of the last such Disclosure during the accounting period.

D. Timely Action. A Clinic must act on the request no later than 60 days after receipt of the request for an accounting. A Clinic may extend the time to provide the accounting by no more than 30 days, provided that the Clinic, within the initial 60-day period, provides the Patient with a written statement of the reasons for the delay and the date by which the Clinic will provide the accounting. A Clinic may have only one such extension of time for action on a request for accounting. See information on Electronic Health Records below for timeliness.

E. Cost. The Clinic must provide the first accounting to a Patient in any 12-month period without charge. A reasonable cost-based fee may be charged for each subsequent request within the 12-month period, provided the Clinic informs the Patient in advance of the fee and provides the Patient with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

F. Documentation. A Clinic must retain documentation of the titles of the person(s) or office responsible for receiving and processing requests for an accounting, the information needed to appropriately track disclosures, and copies of the written accountings provided to the Patients.

G. Suspension of Accounting. A Clinic must exclude from an accounting Disclosures to a health oversight agency or law enforcement official, for the time specified by that agency or official, *if* including the Disclosures in an accounting to the Patient would be reasonably likely to impede the agency or official's activities. In such a case, the health oversight agency or law enforcement official should provide the Clinic with a written statement that such an accounting would be reasonably likely to impede the agency's activities and specifying the time for which a suspension is required. If such statement is made orally, the Clinic must document the statement, including the identity of the agency or official making the statement, temporarily suspend the Patient's right to an accounting of Disclosures subject to the statement, and 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.

H. Examples of Disclosures that must be accounted for include:

1. Disclosures required by law;
2. Disclosures for public health activities such as reporting of disease, injury or vital events;
3. Disclosures about victims of abuse, neglect or domestic violence;
4. Disclosures for health oversight activities such as audits, investigations, inspections, licensure and criminal proceedings;
5. Disclosures for judicial and administrative proceedings;
6. Disclosures for law enforcement activities;
7. Disclosures to coroners, medical examiners, funeral directors or organ procurement agencies;
8. Disclosures for research purposes with IRB or Privacy Board Waiver of authorization requirements;
9. Disclosures to avert a serious threat to health or safety;
10. Disclosures for certain government functions;
11. Disclosures for workers' compensation and workplace surveillance (for work-related injuries).

I. Electronic Health Record (EHR).

Clinics that adopt Electronic Health Records must comply with a request for an accounting of disclosures from a patient. The accounting procedures where an EHR is used include the following:

1. individuals have a right to receive accounting of disclosures for Treatment, Payment or healthcare Operations (TPO) for 3-year period prior to request if in an EHR;
2. CE that uses/maintains EHR with PHI, individual has right to obtain a copy of his/her record in an electronic format;
3. Reasonable fees may be imposed for this processing; and
4. Only charges for reasonable *labor* are applied (not for the electronic product);
5. There is no requirement for the Clinic to allow the individual to directly access the record/accounting. Rather, this is appropriately handled by designated Clinic staff; and

6. Requestors do not have the right to demand use of a USB or other material/media that that may cause harm to the records or systems (e.g., individual may not require that you use their USB drive for this purpose).

J. Individual Privacy Restrictions.

Clinics should comply with requests from individuals to restrict the disclosure of PHI that relates to TPO disclosures. The Clinic **must** comply when the:

1. Restriction relates to disclosure to a health plan for purposes of carrying out payment or health care operations
2. Restriction does not relate to disclosure to health plan for purposes of carrying out treatment; and
3. PHI pertains solely to health care item/service that Clinic/provider was already paid in full out of pocket by the individual.

K. Research Accounting.[20] The Privacy Rule grants a patient the right to request an Accounting of Disclosures for some of the "disclosures" not "uses" of patient PHI, but not for all of the disclosures.

1. The clinic need not account for disclosures during a research study if the:
    a. Disclosure was made pursuant to a patient authorization;
    b. Disclosure is of a Limited Data Set (with a Data Use Agreement);
    c. Disclosure is of De-Identified information (as defined by this handbook or law); or
    d. The IRB found the study exempt under the Common Rule because the existing information recorded cannot be identified (directly or through indirect identifiers linking to the research subject).[21] (Note that disclosures for research operating under a waiver of authorization are not exempt from the accounting requirement, however disclosures made under a patient's authorization for research are exempt (because all authorization-based disclosures are exempt). The accounting requirement can be met by providing individuals with a list of all protocols for which their PHI may have been disclosed pursuant to a waiver, as well as the researcher's name and contact information. (Where 50 or fewer records are involved, the accounting must meet the normal specificity requirements listed below.)
2. A research subject should be provided at least the following information where not otherwise excluded or waived including:

a. the date of the disclosure (if multiple disclosures, the start and stop dates and the frequency);

b. the name of the entity or person who received the protected health information and, if known, the address of such entity or person;

c. a brief description of the protected health information disclosed; and

d. a brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure.

3. Similar to Clinics, the researcher usually has 60 days to meet requests for an accounting of Disclosures, with a 30-day extension available if the requestor is provided with a written explanation for the delay. The researcher should also document such accounting.

PART IV: SECURITY

I. Security of Electronic Health Information

Each Clinic and supporting units is responsible for the security and privacy of the individually identifiable health information that it creates, receives, maintains, and/or transmits, in any form or format as this information is Category I data "Confidential". The policies are in the KU policy library under Information Access and Technology, Privacy and Security. This includes the following specific requirements to manage the risk involved in the use or disclosure of the data. While the HIPAA Security Rule only applies to ePHI (electronic PHI), the HIPAA Privacy Rule requires the safeguarding of any type of PHI; further, the University requires the safeguarding of any identifiable data under the Data Classification & Handling Policy and Procedures, as well as other standards and guidelines for digital data.

A. General Security Management.

1. IT Security Office. The University has created the IT Security Office (ITSO) to coordinate the University's IT security program and provide security-related support services to the University community. The University has appointed the Information Security Officer to oversee this Office, and to serve as HIPAA Information Security Officer. Assistance or information regarding the IT Security Office and University IT Security policies and procedures can be obtained by calling (785) 864-9003.

2. Departmental Technical Staff. Security management at the University is a mixture of centralized and decentralized functions. Certain responsibilities for IT security have been delegated to Departmental Technical Staff working within the various Units and departments of the University. Clinics without Department Technical Staff or TSC support must register their Technical Liaison staff with the IT Security Office.

3. Clinics. Each Clinic is responsible for:

    a. *Inventory*. Maintaining an inventory of the electronic IIHI accessed, created, received, stored and transmitted by the Unit and the hardware and electronic media containing the electronic IIHI. The inventory should detail the location of and the person responsible for the hardware and electronic media and must be updated when the location or person changes.

    b. *Information*. Maintaining the confidentiality, integrity and availability of the electronic IIHI;

c. *Threats*. Protecting against any reasonably anticipated threats or hazards to the security or integrity of such information;

d. *Use and Disclosure*. Protecting against any reasonably anticipated uses or disclosures of such information that are not permitted or required by law;

e. *Compliance* with these requirements, University policies and procedures, and laws addressing the privacy and security of such information; and

f. *Changes or updates* may be required annually or more often to reasonably and appropriately address environmental or operational changes affecting the security of such information.

4. Periodic Risk Analysis and Evaluation.

   a. *Periodic Review and Revision*. Each Clinic, in coordination with its Departmental Technical Staff, must provide for periodic review and revision of Clinic security policies and procedures to address technological, environmental or operational changes. This review should be conducted at least annually.

   b. *Risk and Vulnerability Assessment.* Clinic information systems housing electronic IIHI shall undergo a periodic Risk and Vulnerability Assessment (RVA) by the IT Security Office in accordance with the University of Kansas Information Technology Security Policy. This review shall include assessment of the potential risks and vulnerabilities to confidentiality, integrity, and availability of electronic IIHI held by the Unit, as well as identification of measures sufficient to reduce such risks and vulnerabilities to a reasonable and appropriate level.

5. Security Incident Reporting and Response. The University has developed and implemented a coordinated security incident reporting and response process. Information regarding how to identify and report security incidents or abuses is set forth in the University of Kansas Information Technology Security Policy.

   a. *Required Reporting.* All members of the KU community are obligated to report a known or suspected information Security incident by immediately reporting any concerns to IT Customer Service Center at (785) 864-8080.

   b. *Timely Action.* All reporting should occur in line with procedures within 48 hours of the discovery of such incident.

B. Information Access Management.

1. Workforce Clearance.

    a. *Verification Checks.* Clinic procedures must provide for completion of background and verification checks required by University policy and applicable law prior to authorization of access to electronic IIHI. Examples of verification checks include validation of references and verification of academic and professional credentials.

    b. *Position Descriptions.* When defining a Clinic position that will have access to electronic IIHI, the Clinic must identify and define the security responsibilities of the position. Security responsibilities must be reflected in the applicable position description.

    c. *Temporary or Contract Workforce.* In cases where a workforce member with access to electronic IIHI is provided via an agency, the contract with the agency must clearly state the agency's responsibilities for reviewing the candidate's background.

    d. *Workforce Confidentiality/Security Agreements.* Workforce members who access Clinic or University Information Systems containing electronic IIHI must sign a confidentiality/security agreement in a form approved by the University for this purpose**.**

2. Authorization of Access to electronic IIHI. Each Clinic must implement a process for authorizing and documenting the authorization of Workforce access to information systems containing electronic IIHI. The authorization process must provide for the minimum necessary access required for each Workforce member's role and responsibilities. The permitted authorizations for Workforce members' access must be reviewed annually by an appropriate member of Clinic management and modified where appropriate.

3. Termination of Access. Each Clinic must establish a process to terminate on a timely basis a Workforce member's or Business Associate's access to IIHI upon termination or change of jobs. The process must include a mechanism to document/confirm termination of access. Access to Information Systems containing IIHI may not extend beyond the date of termination or change of job unless there is a legal basis for doing so, e.g., the former Workforce member will be acting as a "Business Associate" of the

Clinic. Clinic procedures relating to termination of access must provide for:

a. *Deactivation of relevant user accounts* and removal from relevant access control lists.

b. *Changing of codes* for keypunch systems/cipher-lock mechanisms, equipment access passwords (routers and switches), administrator passwords, and other common access control information, where appropriate.

c. *Changing the combinations* of combination lock mechanisms.

d. *Retrieving physical access control items*, e.g., keys, ID badges, smart cards and tokens.

e. *Retrieving University or Clinic-issued equipment*, e.g. pagers, cellular phones, portable or mobile computers or devices, diskettes and other electronic storage media.

f. *Other steps necessary* to ensure that locked files can be opened by an authorized supervisor/director or notification of the System Access Office at 864-0439 if email and/or application proxies are needed.

g. *Immediate notification of the IT Account Management group* is required if Clinic management believes that an individual's access privileges should be suspended to maintain the security and/or integrity of ePHI or related IT systems.

C. Facility Access Controls. Each Clinic is responsible for safeguarding the facilities, systems and equipment used to store electronic IIHI from unauthorized physical access, tampering or theft. Clinic policies and procedures must provide for the following:

1. Access Control and Validation. Procedures to control and validate an individual's access to facilities housing electronic IIHI based on the individual's role or function. Examples include but are not limited to the following:

   a. Requiring Workforce to wear University/Clinic identification badges when on site.

   b. Use of physical access control mechanisms, e.g., keys, code locks, smart cards.

   c. Procedures to validate and document visitor access to facilities or restricted areas housing electronic IIHI, e.g., implementation of a sign-in process.

d. Procedures to provide visitors with escorts to and from their destination.

2. Maintenance Records. Procedures to manage and document repairs and modifications to the physical security components of the facility, for example, lock, windows, doors and other physical access control hardware.

3. Contingency Operations. Procedures to allow physical access to the facility during emergencies to support restoration of data under the Clinic's Disaster Recovery/Contingency Plan. **See Section P. Contingency Plans.**

D. Privately Owned Equipment.

1. Privately owned equipment must not be used to create, store, receive, or transmit electronic IIHI that is the result of KU operations. All requirements of Mobile Devices provided by KU to a Clinic member, workforce, or user who may create, use, receive, disclose, or maintain IIHI on privately owned equipment shall apply.

2. All Clinic Data shall be considered KU Data for purposes of Information Management, no matter where the data is stored.

E. Workstation Use. Clinics must provide Workforce members who have access to electronic IIHI with the following information:

1. The proper functions to be performed on the specific workstation or class of workstations;

2. The manner in which such functions are to be performed on the specific workstation or class of workstations, for example:

   a. The required methods for securing the application when leaving the workstation unattended, e.g. logging out or "locking" the workstation;

   b. The manner in which storage media used with the workstation are to be securely stored;

   c. Prohibitions regarding the practice of writing down user IDs and passwords where others can find and or use them; and

   d. The process, where applicable, for making backups on a regular basis to protect against business interruption, and

   e. Requirements for turning off the workstation at the end of the work shift.

3. Requirements regarding the physical attributes of the surroundings of a specific workstation or class of workstation, for example:

    a. Prohibitions on leaving the workstations unattended for prolonged periods of time while active;

    b. Prohibitions on moving workstations to other areas within the Clinic without appropriate approval of Clinic management;

    c. Securely locking the room in which the workstation is located;

    d. Measures to be taken to minimize casual viewing by passersby, e.g., turning of monitor, polarized screen filter, etc.

F. Password Management.

1. Unique User IDs and Passwords. Clinic Workforce members who access networks, systems, or applications used to create, access, receive, store or transmit electronic IIHI must be supplied with a unique user identification and password to gain access to the electronic IIHI. Workforce members must supply a password in conjunction with their unique user identification to gain access to any application or database system used to create, transmit, receive or store electronic IIHI.

2. Password Security. Clinic policies and procedures regarding the structure, aging and safeguarding of passwords must comply minimally with the University of Kansas Password Policy. More stringent standards may be adopted by clinics.

G. Whole or Full Disk Encryption as provided by the University is required for any workstation that stores any IIHI on a local drive. Please contact the IT Security Officer for more information and coordination of this service.

H. Software Management. Installation of software on University devices must be approved and/or performed by authorized University staff. University policies regarding licensing, intellectual property and copyright must be followed.

I. Activity Control and Review. Each Clinic must develop and implement a plan for monitoring Clinic IT system activity where deemed reasonable and appropriate based on the Clinic's Risk and Vulnerability Assessment activities The procedures for system activity control and review must:

1. Identify the systems and applications for which system activity will monitored;

2. Identify the hardware, software and/or procedural mechanisms that will be used to record and examine activity, such as utilization of logs, access/activity reports or other mechanisms;

3. Identify the information to be logged for each system;

4. Provide for review by an appropriate individual (such as the Departmental Technical Staff) on a regular basis, at intervals commensurate with the associated risk of the information system and the sensitivity of the electronic IIHI;

5. Provide for reporting of security incidents such as activity exceptions and unauthorized access attempts to the IT Security Office in accordance with the University's IT Security Policy.

J. Person or Entity Authentication. Each Clinic must establish and implement procedures to verify that the person or entity seeking access to electronic IIHI is the person or entity claimed.

1. Workforce members seeking access to any network, system or application that contains electronic IIHI must satisfy a user authentication mechanism approved by the IT Security Office.

2. A reasonable effort must be made to verify the identity of the person or entity prior to transmitting electronic IIHI. Each Clinic must establish a protocol for verifying the identity of the person or entity requesting IIHI.

K. Transmission Security. Use of encryption is required in cases where electronic IIHI is transmitted over electronic networks (including use of email to communicate electronic IIHI). Use of email to communicate IIHI is **strongly** discouraged internally and externally; email should not be used if other forms of communication are available, (e.g. telephone call, overnight mail, etc.). Clinic policies, procedures, and on-going training must communicate to Clinic Workforce the applicable requirements for, and limitations on, the transmission of electronic IIHI.

L. Data Integrity. Each Clinic must develop and implement a plan to prevent or detect unauthorized alteration or deletion of electronic IIHI or critical system and network files where deemed reasonable and appropriate based on the Clinic's Risk and Vulnerability Assessment activities, for example:

1. Running automated integrity checks against files or files types containing electronic IIHI or determined to be critical;

2. Assigning staff responsibility for reviewing the results of integrity checking and handling discrepancies; and

3. Restoring any electronic IIHI that may become corrupted.

M. Remote Access. KU IT has developed policies and procedures for remote access to University networks, systems and applications.

N. Wireless Access Policy. The University has developed policies and procedures for wireless access to University networks, systems and applications. In order to provide for the security of electronic IIHI, assistance must be obtained from IT Security Office prior to implementing wireless access.

O. Device and Media Controls. Clinic policies and procedures must address the receipt and removal of hardware and electronic media (e.g., hard drives, removable disks/drives, floppy drives, CD ROMs, DVDs, USB/flash drives, SD cards, etc.) into and out of the Clinic, and the movement of these items within the Clinic. Such procedures must minimally:

1. Address the final disposition of electronic IIHI and/or the hardware on which it is stored.
2. Address removal of electronic IIHI from electronic media before it is made available for re-use.
3. Provide for a record of the movements of hardware and electronic media and the person responsible therefore.
4. The IT Security Office has developed standards for the removal/destruction of confidential data before reuse or disposal. Information regarding acceptable methods of data removal/destruction may be obtained by reviewing Electronic Data Disposal Policy and Procedures or by contacting the IT Security Office at 785-864-9003.

P. Contingency Plans. Each Clinic must develop a Contingency Plan for implementation in the event of an emergency, disaster or other occurrence (i.e. fire, vandalism, system failure and natural disaster), for systems that contain electronic IIHI. The Contingency Plan must address the following:

1. Applications and Data Criticality. Each Clinic must prioritize its computer and other electronic systems in order of importance to the ongoing operation of the Clinic, so that the Clinic may focus resources on those systems and processes most critical to the Clinic, should staff resources or ability be diminished due to a disaster or other negative event.
2. Data Backup. Based upon the Clinic's Risk and Vulnerability Assessment activities and its assessment of the relative "criticality" of specific applications and data, each Clinic must document the data that will be backed up and how, including schedules and procedures. Backup media must be stored in a secure location.

The need to store backup media at a secure off-site location should be considered. Information Services offers an appropriate back-up site for a fee. If an alternative storage facility or backup service is used, a Business Associate Agreement, in the form approved by the University, must be in place.

3. Disaster Recovery. Clinic procedures must provide for timely restoration and recovery of electronic IIHI and the systems needed to make that electronic IIHI available in the event of an emergency or disaster, such as fire, vandalism, terrorism, systems failure or natural disaster affecting systems containing electronic IIHI. The disaster recovery procedures must provide for restoration of data from backups in the event of data loss, logging of system outages, failures, and data loss to critical systems, and notification of appropriate individuals to implement the disaster recovery procedures.

4. Emergency Mode Operations. Clinic procedures must address continuation of critical business processes for protection of security of electronic IIHI while operating in emergency mode.

5. Documentation and Testing. The Contingency Plan must be easily available to necessary personnel at all times and appropriate Workforce members must be trained on how to implement the Contingency Plan and related procedures. The Contingency Plan must be tested on a periodic basis to ensure that electronic IIHI and the systems needed to make electronic IIHI available can be restored and recovered and that critical business processes can continue in a satisfactory manner while operating in emergency mode.

Q. Security Emergency Access. This policy shall not be construed to prohibit access to electronic IIHI by a health care professional responding to an emergency in cases where denial of access would inhibit or negatively affect the patient's care. Requests for access in the event of a health or safety emergency should be directed to the Director of the Clinic involved.

PART V. ORGANIZATIONAL REQUIREMENTS

I. Additional Administrative Requirements

In addition to the items in this manual, the University as the organizational entity must ensure that other policies and procedures are in place for the Covered Components and Supporting Units, in order to comply with HIPAA.

A Clinic is responsible for:

A. Compliance with University policies and procedures and state and Federal laws that relate to confidentiality, privacy, and security of Patient information. A Clinic may not require an individual to waive his or her rights under applicable privacy laws as a condition of treatment or service.

B. Revisions to Clinic-specific policies and procedures pertaining to privacy of health information, as necessary to comply with changes in the law and or practice. Material changes must be documented, implemented and communicated to the affected Workforce within a reasonable period of time after the material change becomes effective.

C. Provision of appropriate safeguards, (administrative, technical and physical) to protect IIHI maintained by the Clinic from any intentional or unintentional Use or Disclosure that is in violation of applicable policies or law. These safeguards include, but are not limited to the following:

1. Appointment of an individual to be responsible for on-site coordination of activities relating to compliance with these guidelines and state and federal privacy laws, and for responding to complaints regarding the handling of IIHI at the Clinic.

2. Identification of those persons or classes of persons in its Workforce who need access to IIHI to carry out their duties and for each such person or class of persons, the category or categories of IIHI to which access is needed and any conditions appropriate to such access. A Clinic Workforce member may access IIHI only if it is necessary to carry out his or her duties and he or she has been authorized to access IIHI by the department supervisor.

3. Risk Analysis. Subject to the requirements of the Security Section, Clinics must comply with regular risk analyses, including the Risk and Vulnerability Assessments, of the IT Security Office and documentation requests or updates from Privacy Office or Institutional Compliance office. As identified previously, this should occur on at least an annual basis.

D. Training. Ensuring that all members of the Clinic's Workforce, including faculty, staff, student-employees, students, residents, fellows, trainees, and volunteers, receive education and awareness on University and Clinic policies and procedures, including laws regarding privacy and

security of Patient information/PHI or IIHI. Such education and awareness must be provided, documented, and retained (in the personnel files of the Clinic workforce member within a reasonable period of time after the individual joins the Clinic's Workforce, but not later than 30 days after onboarding to the unit.

1. Privacy and Security Awareness. The University will make available to Clinics an on-line Privacy and Security Awareness Program. Clinic Workforce must complete the program within a reasonable time after joining the Workforce.

2. Unit-Specific Training. Each Clinic is responsible for providing its Workforce with education and training on "unit-specific" policies and procedures relating to the security of ePHI. Such training must be documented and updated to take into account material changes in the Clinic's IT security environment or procedures. Documentation may include a roster of attendance by Workforce members and the curriculum for the training.

3. Security Updates and Reminders. Each Clinic (in coordination with the Clinic's Technical Liaison/Partner) must provide its Workforce with periodic updates on changes to University/Unit security policies or procedures, and where appropriate, warnings regarding identified threats, breaches, vulnerabilities or other security incidents. Assistance with such activities is available from the IT Security, which has created a web site at security.ku.edu to provide Units with security alerts, information about security tools, and other helpful security resources.

4. Temporary/Contract Workers and Business Associates. Clinics authorizing access to ePHI to temporary/contract workers or Business Associates are responsible for documenting that appropriate training regarding University/Unit policies and procedures relating to the privacy and security of Clinic data have been provided to the individuals accessing such data on behalf of the Clinic.

E. Breach Reporting. Regular and continuing communicating to, and training of, Clinic Workforce members regarding their **duty to report breaches** of privacy or confidentiality to their supervisor or to the KUL Privacy Officer. The Clinic should first report a suspected incident or breach to the IT Customer Service Center at 785-864-8080 and then to notify the Privacy Office.

F. Complaints and Communicating to Patients and others their right to submit complaints, questions or concerns regarding the Use and

Disclosure of IIHI on the Lawrence Campus to the Clinic where the complaint, question or concern arose or to the KUL HIPAA Privacy Officer.

G. Investigating potential violations of applicable policies or laws regarding confidentiality and privacy of health information. Reporting of suspected breaches or violations should be made to the unit supervisor and local Privacy Officer prior to the investigation phase. Such Investigations must be conducted consistent with University's existing policies and procedures regarding such investigations, including the due process guidelines of the University. Inquiries concerning investigation procedures should be referred to the University General Counsel's Office or the KUL HIPAA Privacy Officer.

H. Risk Assessment. Following the report and investigation of a breach, the KUL Information Security office and/or KUL HIPAA Privacy Officer should make a Risk Assessment in conjunction with and cooperation of the Clinic/unit.

I. Mitigating, to the extent practicable, any harmful effect that is known to the Clinic of a Use or Disclosure of IIHI that is in violation of applicable policies and procedures or the requirements of Federal or state law. The following factors should be evaluated to determine (whether or) how to mitigate any harm:

1. Whether any damage occurred or was sustained;
2. The nature of the damage that occurred, if any;
3. The amount of damage, if any;
4. The PHI or IIHI that was used or disclosed;
5. The reasons for the use or disclosure; and
6. Whether the harm can be mitigated.

Note: Encryption in transit and storage of ePHI ***may*** provide a Safe Harbor to additional reporting or actions. Check with the IT Security Office for options available.

J. Notification. Under HIPAA as well as some state laws, a Clinic may be required to notify individuals whose unsecured protected health information (uPHI) or PII has been, or is reasonably believed to have been, accessed, acquired, or disclosed as a result of a privacy or "security incident", sometimes called a "breach." [22]

1. Clinics must work with the KU Privacy and IT Security Office to address review and determination of Notification.
2. Reporting or notification of HHS must comply with the requirements of the Breach notification rule

a. Clinics should compile a calendar year list of any breaches of PHI that failed to require notification at the close of each calendar year.

b. Clinics should submit those lists to the Privacy Office for joint review and discussion if they require HHS filing.

3. Any notification of breach **requires** the input of the KUL HIPAA Privacy Officer as well as others convened on the Incident Response Team.

K. Sanctions reasonable and appropriate to ensuring the privacy of health information violations are imposed. Violations of these guidelines, other University policies and procedures, or laws regarding confidentiality and privacy of health information may result in disciplinary action and other corrective measures. Determinations regarding disciplinary action and corrective measures must be made in accordance with the University's existing policies and procedures regarding such matters, and should be documented in employee personnel files.[23] Sanctioning (or enforcement of policy) is required for breaches.

1. Each Clinic should adopt a Sanction Model that includes policy and procedure and that is in line with University policy. Such model may be reviewed and approved by Office of Legal Counsel and/or the Privacy Officer.

2. The policy should be communicated to all workforce members and in workforce training updates and exercises. The policy should address appropriateness of sanctions, include investigation of disclosures made by the workforce members that may be whistleblowers (see next item below) and account for Good Faith errors.

3. Although enforcement of policy and procedures is required by Clinics, Sanctions may be modified based on mitigating factors in conjunction with harm assessment. Examples of factors that may affect a sanction include:

a. Violator's knowledge of privacy and security practices (e.g., inadequate training, training barriers, or limited English proficiency);

b. Culture of surrounding environment (e.g., investigation determines inappropriate practices in business unit);

c. Violation occurred as a result of attempting to help a patient;

d. Victim(s) suffered no harm (financial, reputational, or other personal harm);

e. Violator voluntarily admitted the violation in a timely manner and cooperated with the investigation;

f. Violator showed remorse; and/or

g. Action was taken under pressure from an individual in a position of authority

L. No retaliation. Communicating to patients and Clinic Workforce that intimidation, retaliation or discrimination against a Patient or any other individual for exercising his or her rights under applicable privacy laws, including but not limited to filing a complaint regarding a privacy practice, is strictly prohibited. See also the KU Whistleblower policy in the KU Policy Library.

M. Documenting compliance with these guidelines. Documentation must be maintained for a minimum of six (6) years. Materials regarding an individual workforce member should be retained in his/her personnel files.

.

GLOSSARY

For purposes of the Clinic HIPAA Manual, the following terms are defined as follows:

Authorization. The mechanism for obtaining an individual's permission for the Use and Disclosure of IIHI pertaining to the individual, in contexts **other than T**reatment**, P**ayment or **O**perations (other than TPO).

Breach (as it relates to PHI) — The unauthorized acquisition, access, use, or disclosure of protected health information, which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. (Defined in the American Recovery and Reinvestment Act of 2009)

Breach (as it relates to PII) — The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic. (Defined in OMB M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information)

Business Associate. Person or entity that creates, receives, maintains, or transmits PHI in fulfilling certain functions or activities for a HIPAA-covered entity other than in the capacity of a workforce member. See 45 CFR 160.103

BA may include a person or entity, **other than a member of the Clinic's Workforce**, who

1. performs or assists in the performance of a function or activity involving the Use or Disclosure of PHI, e.g., claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and re-pricing; or
2. provide legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to the Clinic if they receive PHI from the Clinic in the course of providing such services.

   A Covered Entity may be a Business Associate of another Covered Entity. Business Associate includes a person or subcontractor that creates, receives, stores, or transmits PHI on behalf of the Business Associate, See 45 CFR 160.103

   Business associate excludes a health care provider with respect to disclosures by the covered entity to a health care provider concerning the treatment of the individual/patient. See 45 CFR 160.103

Clinic(s). Medical and mental health Clinics and other units providing direct healthcare services to Patients on the Lawrence Campus of the University of Kansas.

Common Control. Exists if an entity has the power, directly or indirectly, significantly to influence or direct the actions or policies of another entity. See 45 CFR 164.103.

Consent. The mechanism for obtaining an individual's permission for the Use and Disclosure of IIHI pertaining to the individual, **in the context of T**reatment, **P**ayment and **O**perations.

Covered Entity. A health plan, a health care clearinghouse, or a health care provider who transmits health information in electronic form in connection with a transaction for which HHS has adopted a standard.

Covered Functions. Those functions of a covered entity the performance of which makes the entity a health care provider, health plan, or health care clearinghouse under the HIPAA Administrative Simplification Rules. See 45 CFR 164.103

Data Use Agreement. An agreement into which the covered entity enters with the intended recipient of a limited data set that establishes the ways in which the information in the limited data set may be used and how it will be protected.

Designated Record Set (DRS). Any record (item, collection or grouping of information, including PHI and maintained, collected, used, or disseminated by or for a covered entity/Clinic) containing medical, billing, enrollment, or Payment information Used by or for a Clinic to make decisions about Patients. See 45 CFR 164.501.

Disclosure. The release, transfer, provision of access to, or divulging in any other manner, of information (here meaning IIHI) to any party or individual outside the Clinic (including other non-covered components of the University) and its approved Business Associates, not including the Patients themselves or their properly documented Personal Representative(s). See 45 CFR 160.103

"Disclosure" under FERPA means to permit access to or the release, transfer, or other communication of personally identifiable information contained in education records by any means, including oral, written, or electronic means, to any party except the party identified as the party that provided or created the record. *(Authority: 20 U.S.C. 1232g(b)(1) and (b)(2); 34 CFR 99.3 Definitions*

Education records (under FERPA) are records pertaining to an identifiable student that are maintained by a University, Clinic, or agent of the University

Electronic media means

1. Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives)

and any removable/transportable digital memory medium magnetic tape or disk, optical disk, or digital memory card;

2. Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Note, paper, fax transmissions, or voice (over Internet protocol) may be included if originally existing in electronic format. See 45 CFR 160.164.

Genetic Information regarding an individual, information about the individual's genetic tests, the genetic tests of an individual's family member(s), the manifestation of a disease/disorder in individuals' family member(s), or any request for/receipt of genetic services, including participation in a clinical research project with genetic services by the individual or family member(s). This shall include a fetus or embryo of an individual, but exclude information about sex or age of an individual. See 45 CFR 160.103.

Genetic Services means a genetic test, genetic counseling (obtaining, interpreting, or assessing the genetic information) or genetic education. See 45 CFR 160.103.

Genetic Test means an analysis of human DNA, RNA, chromosomes, proteins, metabolites, or analysis detecting any genotypes, mutation, or chromosomal change, excluding analysis of proteins/metabolites directly related to a manifested disease, disorder, or pathological condition. See 45 CFR 160.103.

Health care component means component or combination of components of a Hybrid Entity designated by the hybrid entity. See 45 CFR 164.103

Health Care Provider means a provider of medical or health services and any other person or organization that furnishes, bills, or is paid for health care in the normal course of business. See 45 CFR 160.103.

Health Information means any information, including genetic information, whether oral or recorded in any form or medium, that:

1. Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

2. 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.

See 45 CFR 160.103.

Hybrid Entity - A single legal entity that 1) is a Covered Entity, 2) performs business activities that include both covered and non-covered functions, and 3) designates its health care components as provided in the Privacy Rule. See 45

CFR 164.103. *If a Covered Entity is a Hybrid Entity, the Privacy Rule generally applies only to its designated health care components. However, non-health care components of a Hybrid Entity may be Business Associates of one or more of its health care components, depending on the nature of their relationship.*

Incident — The act of violating an explicit or implied security policy. Of course, this definition relies on the existence of a security policy that, while generally understood, varies among organizations. These include but are not limited to:

- attempts (either failed or successful) to gain unauthorized access to a system or its data
- unwanted disruption or denial of service
- the unauthorized use of a system for the processing or storage of data; and changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent. (US CERT)

Identifying information (Red Flags) means any name or number that may be used alone or in conjunction with any other information, to identify a specific person, including:

- name
- address
- telephone number
- social security number
- date of birth
- government issued driver's license or identification number
- alien registration number
- government passport number
- employer or taxpayer identification number
- unique electronic identification number
- computer's Internet Protocol address or routing code

Individual means the person who is the subject of PHI or the PII.

Individually Identifiable Health Information (IIHI). Information that is a subset of health information, including demographic information collected from an individual, that is (1) created or received by a health care provider, health plan, employer, or health care clearinghouse, and (2) 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 Payment for the provision of health care to an

individual; and that (a) identifies the individual, or (b) with respect to which there is a reasonable basis to believe that information can be used to identify the individual. 45 CFR 160.103.

Information — Any communication or representation of knowledge such as facts, data, or opinions in any medium or form; including textual, numerical, graphic, cartographic, narrative, or audiovisual forms. (Defined in OMB Circular A-130, Transmittal Memorandum #4, Management of Federal Information Resources, 6(a))

Information System — A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (Defined in NIST SP 800-53, Recommended Security Controls for Federal Information Systems, appendix B)

Information Technology Resources - includes but is not limited to: personal computers and related peripheral equipment and software, network and web servers, telephones, facsimile machines, photocopiers, Internet connectivity and access to internet services, e-mail and, for the purposes of this policy, office supplies. It includes data stored in or transported by such resources for HHS purposes.

Institutional Review Board (IRB) - An IRB performs the review of Research protocols involving human subjects and may act as the Privacy Board for the privacy review.

Marketing. Making a communication about a product or service that encourages recipients of the communication to purchase or use the product/service.

45 CFR 164.501 Some exclusions apply, see definition.

Minor. An individual under the age of 18 who has not been legally emancipated by a court, who is not legally or previously married, serving in the armed forces, an inmate in a correctional facility, or who is at least 16 years old, and living away from home and managing his/her own finances. (See Kansas Statutes Annotated). May also be referred to as an “Un-emancipated Minor”.

Operations. The operational and administrative tasks of a Clinic, including the training of students. Typically, this includes all administrative, financial, legal, and quality improvement activities necessary to run the Clinic and support the core functions of Treatment and Payment.

Patient. The past or current Patient/client of the Clinic, who is the subject of the IIHI.

Payment. The activities undertaken by a Clinic to obtain or provide reimbursement for the provision of health care to the individual/patient. 45 CFR 164.501. For example, eligibility determinations or coverage, utilization review activities (precertification, preauthorization, retrospective review), reviewing

health care services for medical necessity, coverage, justification of charges, billing & collection activities, etc.

Personally Identifiable Information (PII) — Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. (Defined in OMB M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information)

Personal Representative. An individual who has authority, by law, to act in the place of the Patient. Typically, this person "stands in the shoes of the individual" and has the ability to act for the individual and exercise the individual's rights and is determined by state law (or other applicable law, e.g., tribal law, power of attorney for healthcare matters, etc.). This person may be someone such as a parent or legal guardian of a minor, a conservator, etc. Please check with Office of the General Counsel or Privacy Office for more information depending on the situation. (KSA Chapter 59 Probate Code; Chapter 38 Uniform Transfers to Minors Act; Chapter 58, Art 6 Power of Attorney

Privacy — The appropriate use of personal information. (Defined in the International Association of Privacy Professionals site glossary)

Privacy Incident — an incident that involves personally identifiable information or protected health information. (US CERT)

Privacy Liaison/Coordinator. The Person designated by each health care component and charged with carrying out the HIPAA compliance responsibilities for their respective health care component.

Privacy Officer. The Person and associated office designated by the University to carry out and coordinate activities related to privacy of health information as required by HIPAA.

Protected Health Information (PHI) — "Individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. "Individually identifiable health information" is information, including demographic data, that relates to:

- the individual's past, present or future physical or mental health or condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

Electronic Protected Health Information (ePHI) means any PHI that is created, stored, transmitted or received in any electronic media. The HIPAA Security Rule covers the following and any future technologies used for accessing, transmitting, or receiving PHI electronically:

- Storage Media/Data at Rest:
- Personal computers with hard drives (internal or externally connected) used at work, home or traveling
- Portable or mobile hard drives, including storage drives, iPods, tablets, smart phones, etc.
- Magnetic tape
- Removable storage devices, such as USB memory sticks, SD cards, CDs, DVDs, or any other technological storage device
- Transmission of Data (wired or wireless) including modem, DSL, cable, fiber, laser, or other connections
- Email and file transfer, including shared cloud storage applications or technology

Unsecured Protected Health Information (uPHI) means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in guidance (as updated annually). See 45 CFR 164.402.

Protected health information (PHI) is typically rendered unusable, unreadable, or indecipherable to unauthorized individuals such that it is not uPHI, if one or more of the following applies:

1. ePHI is encrypted as specified by HIPAA 45 CFR 164.304 and NIST standards, such that decryption tools are stored on device or in location separate from the data they are used to encrypt/decrypt for Data at Rest/in Storage (see NIST SP 800-111) and for Data in Motion/Transit (see NIST SP 800-52, 800-77, 800-113 and FIPS 140-2)
2. media on which the PHI is stored/recorded has been destroyed in one of the following ways:
    - Paper, film, hardcopy media shredded or destroyed such that PHI cannot be read/reconstructed (redaction is not appropriate);
    - Electronic media is cleared, purged or destroyed consistent with NIST SP 800-88 and PHI cannot be retrieved.

Psychotherapy Notes. Notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the

contents of conversation during a private counseling session or a group, joint, or family counseling session and that are **separated from the rest of the Patient's medical record**. See 45 CFR 164.501 Further, these notes are not intended to be shared with other professionals and they are only accessible by the recording therapist. See APA Guidelines for Record Keeping Excluded from Psychotherapy notes are: Medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date. See 45 CFR 164.501.

Red Flag. A pattern, practice or specific activity that indicates the possible existence of identity theft.

Required by law. Mandate contained in law that compels an entity to make a use or disclosure of PHI and that is enforceable in court of law. See 45 CFR 164.103. For example, court orders, court-ordered warrants, subpoenas or summons by a court, grand jury, inspector or administrator body authorized to require the demand, etc. 45 CFR 160.103

Research. A systematic investigation, including Research development, testing and evaluation, designed to develop or contribute to generalizable knowledge. This includes the development of research repositories and databases for research. See 45 CFR 164.501.

Safeguards refer to the security standards that are required for a Covered Entity/Clinic or Business Associate that must act in accordance with 45 CFR 164. 306 to maintain the Confidentiality, Integrity and Availability of the data or information of the Covered Entity or Business Associate pertaining to the identifiable patient and known as Administrative, Physical or Technical Safeguards as defined by HIPAA. 45 CFR 164 Subpart C, Security Standards for the Protection of ePHI.

> *Administrative safeguards* are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information
>
> *Physical safeguards* are physical measures, policies, and procedures to protect a covered entity's or business associate's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.
>
> *Technical safeguards* mean the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.
>
> See 45 CFR 164.304

Security Liaison/Contact:

Person designated by each health care component to serve as their component's primary liaisons for security related communications and incident response.

Security incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. See 45 CFR 164.304.

Security Officer means the Person and associated office designated by the University to develop and implement policies and procedures and to carry out and coordinate activities related to privacy and security of health information as required by HIPAA.

Subcontractor means a person or entity to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate. 45 CFR 160.103

Transaction means the transmission of information between two parties to carry out financial or administrative activities related to health care. Transaction (or “standard transaction”) includes the following types of information transmissions:

1. Health care claims or equivalent encounter information.
2. Health care payment and remittance advice.
3. Coordination of benefits.
4. Health care claim status.
5. Enrollment and disenrollment in a health plan.
6. Eligibility for a health plan.
7. Health plan premium payments.
8. Referral certification and authorization.
9. First report of injury.
10. Health claims attachments.
11. Health care electronic funds transfers (EFT) and remittance advice.
12. Other transactions that the Secretary may prescribe by regulation. See 45 CFR 160.103.

Treatment means the provision, coordination, or management of health care and related services by one or more health care providers. See 45 CFR 164.501. This includes 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 referral of a patient for health care from one health care provider to another. See 45 CFR 164.501.

"**Treatment records**" under *FERPA*, are:

records on a student who is eighteen years of age or older, or is attending an institution of postsecondary education, which are made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his/her professional or paraprofessional capacity, or assisting in that capacity, and which are made, maintained, or used ***only in*** connection with the provision of treatment to the student, and are not available to anyone other than persons providing such treatment, except that such records can be personally reviewed by a physician or other appropriate professional of the student's choice. See 20 *U.S.C.* § 1232g(a)(4)(B)(iv); 34 *CFR* § 99.3, (Disclosure of treatment records converts the records in to "Education records" and are subject to FERPA.)

TPO. The acronym under HIPAA for Treatment, Payment or healthcare Operations.

University. The University of Kansas, Lawrence Campus (including units not residing in Lawrence, but under the control and direction of this campus e.g. Edwards Campus, Parsons, etc.).

Use. The sharing, employment, application, utilization, examination, or analysis of information within an entity that maintains such information. See 45 CFR 160.103.

Violation. Failure to comply with an administrative simplification or Clinic provision. See 45 CFR 160.103.

Volunteer. The Individual who performs uncompensated services for the University under the direction and control of a University supervisor.

Workforce. Employees, volunteers, trainees, students, and other persons (including potentially independent contractors if not under a Business Associate agreement) that are under the direct control of a Clinic, whether or not they are paid by the Clinic. See 45 CFR 160.103.

The HIPAA Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g. (Defined in the HIPAA Privacy Rule)

SOURCES

[1] Health Information Portability and Accountability Act of 1996 (HIPAA), Privacy, Security and Breach Notification Rules, HHS.gov at the Health Information Privacy webpage.

[2] See the Health Information Privacy webpage.

[3] See Joint Guidance on the Application of the Family Educational Rights and Privacy Act (FERPA) And the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to Student Health Records, by the U.S. Department of Health and Human Services and U.S. Department of Education, November 2008, found at the Joint Guidance on the Application of FERPA and HIPAA to Student Health Records webpage.
or see Does FERPA or HIPAA apply to records on students at health clinics run by postsecondary institutions? 11/25/2008

[4] Student Record under FERPA is defined to be "education records" that are 1) maintained by the institution (or its agent) and 2) refers to an identifiable eligible student. See 34 CFR §99.3

[5] 34 CFR 99.30 and 99.31.

[7] 45 CFR 164.105

[8] 45 CFR 164.105; also see Joint Guidance on FERPA & HIPAA, p. 10

[9] See also HIPAA Regulations**:** 45 CFR §164.530(i) Administrative requirements: Policies and procedures; §164.504(a-d) Uses and disclosures: organizational requirements

[10] , as permitted by and in compliance with § 164.506;

[11] of §§ 164.502(b), 164.514(d), and 164.530(c) with respect to such otherwise permitted or required use or disclosure;

[12] Except for uses and disclosures prohibited under § 164.502(a)(5)(i), and in compliance with 164.508

[13] (§ 164.510)

[14] In compliance with, § 164.512, § 164.514(e), (f), or (g).

[15] 164.524 and 164.528

[16] KU Identity Theft Prevention Program, in the KU Policy Library

[17] 45 CFR 164.502 & 508

[18] Examples of BA's include at least the following: Claims processing or administration, Data analysis, processing, or administration, Utilization review, Quality assurance, Billing, Benefit management, Practice management, Re-pricing services, HIO, E-prescribing Gateway, Other person provides data transmission services to CE involving PHI & requires routine access to PHI, PHR vendor providing services on behalf of CE, Subcontractor that Creates, Receives, Maintains or Transmits PHI on behalf of BA

[19] See paragraph (2)(iv) of the definition of "protected health information" at § 160.103.

[20] See also 45 CFR 164.528.

[21] 45 CF 46.101(b)(4).

[22] See 45 CFR 164.408

[23] The Department of HHS receives complaints and investigates through its Office of Civil Rights (OCR) and can impose Civil & Criminal Penalties (4 tiers) for findings of violations under the HITECH amendments to HIPAA.