Clinic Policies and Procedures Regarding Privacy & Security of Patient Information

Revised February 2008
Revised June 2005
Original Date April 2003
# Table of Contents

## I. Introduction .......................................................................................................................... 1

## II. Definitions .......................................................................................................................... 1

## III. Use and Disclosure of IIHI Pursuant to Consent---Treatment, Payment or Health Care Operations ..................................................................................................................... 4

## IV. Use and Disclosure of IIHI Pursuant to Written Individual Authorization ................................ 4

   A. Psychotherapy Notes
   B. Marketing
   C. Research
   D. HIV/AIDS
   E. Alcohol or Drug Abuse Treatment
   F. Treatment Facilities
   G. Other Disclosures
   H. Authorization Content and Format

## V. Use and Disclosure of IIHI without Written Consent or Authorization ......................... 7

   A. Health Oversight Activities
   B. Public Health Activities
   C. Abuse, Neglect or Domestic Violence Reporting
   D. Judicial and Administrative Proceedings
   E. Threats to Health and Safety
   F. Disclosures for Law Enforcement Purposes
   G. Disclosures for Workers’ Compensation

## VI. Use and Disclosure of IIHI Requiring an Opportunity for the Patient to Agree or to Object ................................................................................................................................. 8

   A. Individuals Involved in the Patient’s Care
   B. Disaster Relief Activities
   C. Victims of a Crime
VII.  Use and Disclosure for Educational Purposes ........................................9
   A. Use on Clinic Premises
   B. Removal from Clinic Premises
   C. Disposal
   D. Unaffiliated Students and Other Health Care Professionals: Unaffiliated Students
   E. External Rotations
   F. Accreditation Activities

VIII. Use and Disclosure of IIHI for Research .............................................. 12
   A. Individual Authorization
   B. De-identified Data
   C. Limited Data Sets
   D. Reviews Preparatory to Research
   E. Waiver of Individual Authorization
   F. Research on Decedents
   G. Study Recruitment
   H. Student Records

IX. General Rules Governing Use and Disclosure of IIHI ....................... 13
    A. Minimum Necessary Standard
    B. Incidental Disclosures
    C. Personal Representatives
    D. Verification
    E. Designated Record Sets (DRS)
    F. Disclosures to Other Components of the University
    G. Business Associates

X. Patient Right to Notice of Privacy Practices ..................................... 18
    A. Posting
    B. Electronic Delivery
    C. Acknowledgement
    D. NPP Consent
    E. Documentation
    F. Revisions to NPP

XI. Patient Right to Request Privacy Restriction ..................................... 19
    A. In Writing
    B. Designated Individual
    C. Denial of Request
    D. Required Documentation
    E. Terminating a Restriction
XII. Patient Right to Request Confidential Communications .................................................. 20
   A. Request in Writing
   B. Granting a Request
   C. Denying a Request
   D. Required Documentation

XIII. Patient Right to Inspect and Copy Records ................................................................. 20
   A. Requests in Writing
   B. Timely Action
   C. Granting a Request for Access in Whole or in Part
   D. Denying a Request for Access in Whole or in Part
   E. Documentation

XIV. Patient Right to Request Amendment of Records .......................................................... 23
   A. Requests in Writing
   B. Timely Action
   C. Denying a Request for Amendment
   D. Granting a Request for Amendment
   E. Accepting Forwarded Amendments
   F. Required Documentation

XV. Patient Right to an Accounting of Disclosures ............................................................... 25
   A. Exceptions
   B. Accounting Content
   C. Multiple Disclosures to Same Entity
   D. Timely Action
   E. Cost
   F. Documentation
   G. Suspension of Accounting
   H. Examples of Disclosures that must be accounted for

XVI. Security of Electronic Health Information ................................................................. 27
   A. General Security Management
   B. Information Access Management
   C. Facility Access Controls
   D. Privately Owned Equipment
   E. Workstation Use
   F. Password Management
   G. Security of Servers, Workstations, Mobile Systems
   H. Software Management
I. Activity Control and Review  
J. Person or Entity Authentication  
K. Transmission Security  
L. Data Integrity  
M. Remote Access  
N. Wireless Access Policy  
O. Device and Media Controls  
P. Contingency Plans  
Q. Security Emergency Access

XVII. Administrative Requirements ................................................................. 38

APPENDIX

- Sample Form Authorization for Use and Disclosure of Health Information
- Sample Request Form for Restriction(s) on Use and Disclosure of Health Information
- Sample Request Form for Confidential Communications
- Letter Denying Request to Inspect or Copy Health Information: Unreviewable Denial
- Letter Denying to Request to Inspect or Copy Health Information: Reviewable Denial
- Sample Request Form for Amendment of Health Information
- Sample Letter Approving Requested Amendment of Health Information
- Sample Letter of Notification to Third Parties Regarding Amendment of Health Information
- Sample Letter Denying Requested Amendment of Health Information
- Sample Disclosure Log
- Sample Request Form for Accounting of Disclosures of Health Information
- Information System Access Request (Example)
- Sample Confidentiality and Security Agreement
- Termination of Access Check List
- Portable Device Receipt & Acknowledgement
I. Introduction

This document is intended to provide University Clinics operating on the Lawrence Campus with general guidance and standards regarding the handling of health information. This document does not apply to the Kansas Athletic Corporation. 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 Privacy Officer for the Lawrence Campus at (785) 864-9528.

As a general matter, efforts have been made to provide information which 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”). In many cases, these state and Federal laws are consistent. There may be circumstances, however, where conflicts arise. Where student records 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 (FERPA, also known as the Buckley Amendment). Questions or concerns relating to the interaction of state or federal privacy laws may be addressed to the Privacy Officer, the General Counsel’s Office, or the Vice Provost for Student Success.

II. Definitions

For purposes of this document, 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 Treatment, Payment or Operations (other than TPO).

Business Associate. A person or entity, other than a member of the Clinic’s Workforce, who performs or assists in the performance of a function or activity involving the Use or Disclosure of IIHI, e.g., claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and re-pricing. Business Associates may also include persons who provide legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to the Clinic if they receive IIHI from the Clinic in the course of providing such services.

Clinic(s). All medical and mental health Clinics and other units providing direct healthcare services to Patients on the Lawrence Campus of the University of Kansas. This definition does not include the Kansas Athletic Corporation.

Consent. The mechanism for obtaining an individual’s permission, for the Use and Disclosure of IIHI pertaining to the individual, in the context of Treatment, Payment and Operations.
**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.

**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 containing medical, billing, enrollment, or Payment information Used by or for a Clinic to make decisions about Patients.

**Disclosure.** The release, transfer, provision of access to, or divulging in any other manner, IIHI to any party or individual outside the Clinic and its approved Business Associates, not including the Patients themselves or their properly documented Personal Representative(s).

**Hybrid Entity** - A single legal entity that is a Covered Entity, performs business activities that include both covered and noncovered functions, and designates its health care components as provided in the Privacy Rule. 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.

**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.

**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. The University refers to the IRB as the Human Subjects Committee Lawrence, or HSCL.

**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.
**Operations.** The operational and administrative tasks of a Clinic, including the training of students.

**Patient.** The past or current Patient of the Clinic who is the subject of the PHI.

**Payment.** The activities undertaken by a Clinic to obtain or provide reimbursement for the provision of health care.

**Personal Representative.** An individual who has authority, by law, to act in the place of the Patient.

**Protected Health Information ("PHI").** Individually Identifiable Health Information (IIHI) held or maintained by a HIPAA Covered Entity or Covered Component of the University, or a Business Associate acting for the Covered Entity or Covered Component of the University, that is transmitted or maintained in any form or medium, including electronic, paper and/or oral.

**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**. The following are **not** included: 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.

**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.

**Treatment.** The provision, coordination, or management of health care and related services by one or more health care providers.

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

**University.** The University of Kansas, Lawrence Campus.

**Use.** The sharing, employment, application, utilization, examination, or analysis of information within an entity that maintains such information.

**Workforce.** Employees, volunteers, trainees 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.
III. Use and Disclosure of IIHI Pursuant to Consent---Treatment, Payment or Health Care Operations

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. Clinics have discretion to design a Consent process that works best for their own Operations and Patients, provided the Consent process and Consent document is consistent with state and federal laws applicable to the Clinic. Depending upon the information contained in the “Consent” document used by the Clinic, it 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 IV below), or other requirements or conditions may exist for the Use or Disclosure of IIHI.

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

Written Authorizations, in the form outlined in section IV.E. below, are required prior to Disclosure of IIHI in the following circumstances. 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 DRS.

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. Use or Disclosure of IIHI for marketing purposes generally requires a prior written Authorization. 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. It also includes the sale of information so that the purchaser of the information may make a communication about its own product or service. 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.
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 VII).

D. **HIV/AIDS.** Use or Disclosure of IIHI pertaining to 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 include (but are not limited to) Disclosures of IIHI to an employer or life insurance company.

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

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

3. 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. A 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. An 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.

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. 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. An Authorization for Use or Disclosure of PHI 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 PHI 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 PHI for such Research or a 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. 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/researchrepositories.asp](http://privacyruleandresearch.nih.gov/researchrepositories.asp)

   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).

V. **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, including:

A. **Health Oversight Activities.** A Clinic may disclose IIHI to a health oversight agency for oversight activities 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.** 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. However, the disclosure of treatment records to an agency may be a disclosure subject to FERPA (the Family Educational Rights and Privacy Act of 1974, as amended) and should be cleared through the University Privacy 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, 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.

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 University 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 University General Counsel to assist with reviewing the paper work. The University 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 University 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.

VI. **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 IIHI 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.

VII. 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 one of the following requirements is met:
1. The information has been de-identified, by removal of all 18 of the following identifiers:

- Names;

- All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP Code, and their equivalent geographical codes, except for the initial three digits of a ZIP Code if, according to the current publicly available data from the Bureau of the Census:
  - The geographic unit formed by combining all ZIP Codes with the same three initial digits contains more than 20,000 people.
  - The initial three digits of a ZIP Code for all such geographic units containing 20,000 or fewer people are changed to 000;

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

- Telephone numbers;

- Facsimile numbers;

- Electronic mail addresses;

- Social Security numbers;

- Medical record numbers;

- Health plan beneficiary numbers;

- Account numbers;

- Certificate/license numbers;

- Vehicle identifiers and serial numbers, including license plate numbers;

- Device identifiers and serial numbers;

- Web universal resource locators (URLs);

- Internet protocol (IP) address numbers;

- Biometric identifiers, including fingerprints and voiceprints;

- Full-face photographic images and any comparable images; and

- Any other unique identifying number, characteristic, or code, unless otherwise permitted by the Privacy Rule for re-identification;
2. Written authorization of the Patient has been obtained in accordance with the policies and procedures of the Clinic. Full-face images/videos or presentations that involve live participation by the Patient may only be used after obtaining written Authorization of the Patient.

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 is never acceptable. Similarly, use of electronic records for educational purposes should never be retained on a harddrive, portable device (e.g. laptops, PDA’s, USB devices, etc.). Deletion of the file is not sufficient. For more information on “wiping” or “sanitizing” electronic devices, please consult the I.T. Help Desk for assistance.

D. Unaffiliated students and other health care professionals: Unaffiliated students and/or community health care professionals may participate in the training/education activities of the Clinic in accordance with University and unit department policies and procedures. An affiliation agreement or other appropriate agreement between the University and 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.

F. Accreditation Activities. Students/trainees should consult with the Privacy Office 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.
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 HSCL Coordinator or Privacy Office.

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 the study has been approved by the Human Subjects Committee Lawrence Campus (HSCL).

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. Alternative requirements for de-identification of data may apply in other contexts. Note well, however, that Research involving de-identified data may be considered human subjects Research, and subject to human subjects regulations and IRB (HSCL) approval.

C. Limited Data Sets. A Limited Data Set (“LDS”) is one in which the direct identifiers have been removed, but certain potential identifiers remain. 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. Research employing a Limited Data Set is subject to human subjects’ regulations. The project must be approved by the HSCL prior to initiation.

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 HSC Coordinator or the Privacy Office. Additional or alternative requirements may apply in other contexts. Approval by the HSCL may be required.
E. Waiver of Individual Authorization. A HIPAA Covered Component of the University may Disclose Protected Health Information 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 Protected Health Information 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 HSC Coordinator or the Privacy Office. Additional or alternative requirements may apply in other contexts.

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. Please consult the Privacy Office for more on the use and/or disclosure of Education Records of Students (e.g. treatment records) prior to the use/disclosure.

IX. General Rules Governing Use and Disclosure of IIHI

A. Minimum Necessary Standard

1. 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 (e.g., 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).
2. **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. **Determining what is Medically Necessary.** Clinic Workforce members may assume that a request for IIHI is for the minimum necessary information when:

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

   b. The information is requested by an entity (or component of an entity) that is covered by the Health Insurance Portability and Accountability Act (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 represents that the information requested is the minimum necessary for the stated purpose(s); 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 in Section VII above.

4. **Exceptions.** The Minimum Necessary Standard outlined in this Section VIII.A. does not apply to Uses or Disclosures that are required by law, made to the Patient or pursuant to an Authorization initiated by the Patient, made to or requested by a healthcare provider for Treatment purposes, or required for compliance with applicable laws.

**B. 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. Reasonable safeguards will vary from Clinic to Clinic. A Clinic should analyze its own needs and circumstances, such as the nature of the Patient information (IIHI) it holds, and assess the potential risks to patients’ privacy. A Clinic 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.

Examples of reasonable safeguards 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 names in public areas;
• posting signs to remind Workforce members to protect patient confidentiality;
• isolating and/or locking file cabinets or records rooms; or
• providing additional security, such as passwords, password protected
screensavers, and timed log-outs on computers maintaining personal
information.

C. 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. Minors as well as incapacitated and deceased 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, consistent with the scope
of the Personal Representative’s legal authority.

2. Minors. 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.

3. **Abuse and Neglect.** If it is believed that a Patient, including an unemancipated 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 treat that person as the Personal Representative, if doing so would not be in the best interests of the Patient.

4. **Deceased Patients.** IIHI created during the life of a Patient continues to be protected from Use and Disclosure after death of the Patient, unless otherwise permitted by law.

D. **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.
E. 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 and/or maintained 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 which should not be considered part of the 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 or surgical 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;

7. IIHI that may not be disclosed to the Patient without violating the Clinical Laboratory Improvements Act (CLIA) amendments of 1988. For example, CLIA may require a clinical laboratory to disclose certain test results or reports only to the physician who ordered a test.

F. Disclosures to Other Components of the University.

1. General Rule. Generally speaking, disclosures to other University Clinics, facilities or departments must be treated as disclosures to a legally separate entity. In other words, unless such Disclosure is expressly permitted by law, the transfer of IIHI between such areas should be allowed only to the same extent such a Disclosure is permitted to a separate entity.
2. **Support 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. Where such support services involve the disclosure of IIHI, the University department involved in providing the support service must identify those individuals who require access to the IIHI maintained by the Clinic. The University department must take appropriate steps to limit the sharing of IIHI beyond the individuals identified, and must ensure that such individuals receive education regarding the requirements of applicable state and Federal privacy laws. The University departments providing such support services to Clinics may not Use or Disclose IIHI that they create or receive from or on behalf of a Clinic in a way prohibited by these guidelines, or state or Federal law.

G. **Business Associates.** Clinics may disclose IIHI to a Business Associate that is not affiliated with the University, and may allow such a Business Associate to create or receive IIHI on its behalf, only if the Clinic (University) obtains prior satisfactory written assurances that the Business Associate will appropriately safeguard the information. Such contracts must be in the format approved for such purposes by the University, and in the case of HIPAA Covered Components of the University, must comply with the requirements of HIPAA. If a Clinic becomes aware of a material violation by the Business Associate and it 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 Coordinator for the Lawrence Campus.

X. **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. 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, or if the NPP is delivered electronically, special rules apply. The Lawrence Campus Privacy Coordinator should be contacted for more information.

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, 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. NPP’s must be reviewed by the Lawrence Campus Privacy Coordinator prior to implementation.

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.

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.

**XI. 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. See Appendix—Request Form for Restrictions on Use and Disclosure of Health Information.

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. See Appendix—Request Form for Restrictions on Use and Disclosure of Health Information. 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 or received after the Clinic has informed the Patient.

XII. **Patient Right to Request Confidential Communications**

Patients have the right to request to receive communications of IIHI by alternative means or 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, if the Patient does not specify an alternative method of contact.

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.

XIII. **Patient Right to Inspect and Copy Records**

A Patient has a general right to inspect and obtain a copy of IIHI about the Patient that is contained within the DRS maintained by the Clinic.

A. **Requests in Writing.** A Clinic should require requests for access to be in writing. See Appendix—Sample Request Form to Inspect of Copy Health Information.

B. **Timely Action.** 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.
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. 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.

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 PHI, or mailing the copy of the IIHI at the Patient's request.

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 PHI, if the fee is agreed to in advance by the Patient. State laws regarding maximum fees for copying healthcare records must be followed.

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


   a. 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. 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. 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. 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. 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. The Clinic does not maintain the information.


a. 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. 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. 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. 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. The Clinic must provide a timely, written denial to the Patient. See Appendix—Sample Response Letters to Request to Inspect and Copy Health Information. 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 Privacy Coordinator and to 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.

XIV. Patient Right to Request an Amendment of Records

Patients have the right 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. See Appendix--Sample Request for Amendment of Health Information.

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. See Appendix—Sample Response Letters to Request for Amendment of Health Information. 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 Lawrence Campus Privacy Coordinator (including title and telephone

KU THE UNIVERSITY OF KANSAS
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 and agreement to have the Clinic notify the relevant persons with whom the amendment needs to be shared, as required in subsection 3 immediately below. See Appendix—Sample Letter Approving Requested Amendment of Health Information.

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. See Appendix—Sample Letter of Notification to Third Parties of Amendment of Health Information.

**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.

XV. Patient Right to an Accounting of Disclosures

A Patient has a right to receive an accounting of Disclosures 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).

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

1. To carry out Treatment, Payment and health care Operations;
2. To Patients about themselves;
3. Pursuant to an individual authorization;
4. To persons involved in the patient’s care, such as a patient’s Personal Representative;
5. As part of Limited Data Set
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;
B. Accounting Content. For each Disclosure, the accounting must include the date of the Disclosure, the name (and address, if known) of the entity or person who received the IIHI, a brief description of the IIHI disclosed, and a brief statement of the purpose of the Disclosure that reasonably informs the Patient of the basis for the Disclosure. See Appendix--Sample IIHI Disclosure Log.

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

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 worker’s compensation and workplace surveillance (for work-related injuries).

XVI. Security of Electronic Health Information

A. General Security Management.

1. Office of IT Security. The University has created the Office of IT Security (ITSO) to coordinate the University’s IT security program and provide security-related support services to the University community. The University has appointed the Director of IT Security to oversee this Office. Assistance or information regarding the IT Security Office and University IT Security policies and procedures can be obtained by accessing the IT Security Office web site at www.security.ku.edu, or by calling (785) 864-9003.

2. Technical Liaisons and Field Security Officers. Security management at the University is decentralized and where appropriate, certain responsibilities for IT security have been delegated to “Technical Liaisons” and “Field Security Officers” working within the various Units and departments of the University. Each Clinic is required to register a Technical Liaison with the IT Security Office.
3. **Clinics.** Each Clinic is responsible for:

   a. 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. Maintaining the confidentiality, integrity and availability of the electronic IIHI;

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

   d. 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. Addressing environmental or operational changes affecting the security of such information.

4. **Periodic Risk Analysis and Evaluation.**

   a. The information contained in this document shall be reviewed, evaluated and updated on a periodic basis, but not less often than every two years, by the IT Security Officer, the Privacy Office, Lawrence Campus, and Coordinator of Information Technology Policy and Planning.

   b. Each Clinic, in coordination with its Technical Liaison, 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.

   c. Clinic information systems housing electronic IIHI shall undergo a periodic Risk and Vulnerability Assessment (RVA) by the IT Security Officer or his/her designee, 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. **See University of Kansas RVA Guidelines at www.policy.ku.edu.**
5. **Security Incident Reporting and Response.** The University has developed and implemented a coordinated 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*.

**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 and the required level of supervision of the position. Security responsibilities include general responsibilities for implementing or maintaining security, as well as any specific responsibilities for the protection of the confidentiality, integrity, or availability of electronic IIHI on University information systems. Security responsibilities and supervision requirements 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. See Appendix—Sample Confidentiality and Security Agreement.

2. **Authorization of Access to electronic IIHI.** Each Clinic must implement a process for authorizing and documenting the authorization of Workforce access to systems and networks containing electronic IIHI. See Appendix—Sample Authorization of Access Form. 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 electronic IIHI.
IIHI upon termination or change of jobs. Typically, this process should be performed on a weekly basis in non-urgent cases. The process must include a mechanism to document/confirm termination of access. **See Appendix—Sample Termination of Access Check List.** Access 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 key punch 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 computer 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 Coordinator of IT Policy and Planning 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. **See University of Kansas IT Security Policy.**

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, locks, 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. Generally, privately owned equipment may not be used to create, store, or transmit electronic IIHI that is the result of KU operations.

2. In order for privately owned equipment to be considered for connectivity and/or uses described herein, the owner must obtain prior approval of the Unit Director or the individual designated by the Unit Director for this purpose, and use of such equipment must meet any additional requirements imposed by the Unit and Information Services and/or ITSO.

E. **Workstation Use.** Clinic policies and procedures 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, e.g., diskettes or CD-ROMs, 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. Use of a surge-protecting power-strip that is not to be shared with devices that draw high amperage, e.g. vacuum cleaners, coffee makers, photocopiers, etc.; and
   e. 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 I.D.’s 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. Generic User I.D. and Passwords. A generic user identification and password may be utilized for a shared or common area workstation so long as the login provides no access to electronic IIHI. An additional unique user identification and password must be supplied to access applications and database systems containing electronic IIHI.

3. Password Security. Clinic policies and procedures regarding the structure, aging and safeguarding of passwords must comply with the University of Kansas Password Policy. See www.policy.ku.edu.

G. Security of Servers, Workstations, Mobile Systems. Each Clinic is responsible for implementing technical security safeguards for Clinic servers, workstations and mobile devices used to create, access, receive, store or transmit electronic IIHI, in compliance with applicable University policies (www.policy.ku.edu) and state and federal laws. These security safeguards include, but are not limited to:
1. **Server Security**

   a. The system administrator or root account must be password protected.

   b. A User Identification and Password authentication mechanism must be implemented to control user access to the system.

   c. A security patch and update procedure must be established and implemented to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected.

   d. All unused or unnecessary services must be disabled.

   e. The server must be located in the KU Computing Center, in the area designated by the IT Security Office for this purpose. Exceptions may be granted by the Vice Provost for Information Services if deemed appropriate on the basis of the Clinic’s Risk and Vulnerability Assessment activities.

   f. Logging must be enabled on the server. At a minimum, Logging successful and failed login attempts, successful and failed account management, successful and failed logon events, success and failed policy and system events.

   g. If folders or directories are used, access should be granted with the least amount of privileges necessary.

2. **Workstations**

   a. The system administrator or root account must be password protected.

   b. A user identification and password authentication mechanism must be implemented to control user access to the system. Mobile devices such as laptops must use a boot password to ensure that the system is only accessible to authorized users.

   c. A security patch and update procedure must be established and implemented to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected.

   d. A virus detection system must be implemented including a procedure to ensure that the virus detection software is maintained and up to date.

   e. All unused or unnecessary services must be disabled.

   f. Workstations located in unattended, common or otherwise insecure areas must also implement the following measures:
i. A password-protected screensaver or automatic logoff mechanism. The location of the workstation and sensitivity of the electronic IIHI must be considered when determining appropriate time out periods.

ii. The workstation screen or display must be situated in a manner that prohibits unauthorized viewing. Use of a screen guard or privacy screen is recommended.

iii. A theft deterrent device, such as a cable locking mechanism.

3. **Mobile Systems**

   a. The system administrator or root account must be password protected.

   b. A user identification and password authentication mechanism must be implemented to control user access to the system. Mobile devices and laptops must use a boot password so that access is limited to authorized users.

   c. A security patch and update procedure must be established and implemented to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected.

   d. A virus detection system must be implemented, including a procedure to ensure that the virus detection software is maintained and up-to-date.

   e. All unused or unnecessary services must be disabled.

   f. The mobile devices must not be used for long-term storage of electronic IIHI. The Clinic must develop and implement procedures to purge the electronic IIHI as soon as it is no longer needed on the device.

   g. The mobile device must be stored in a physically secure location when not in use.

   h. Mobile stations that are used in unattended, common or otherwise insecure areas must use:

      i. An inactivity timer or automatic logoff mechanism. The location of the device and the sensitivity of the electronic IIHI must be considered when determining appropriate time out periods.

      ii. A theft deterrent device such as a laptop locking cable, for use when the device is left unattended.

      iii. Clinics should consider requiring authorized users of mobile devices to sign a Mobile Device User Agreement such as the one found in the
Appendix to this document. See Appendix—Sample Mobile Device User Agreement.

4. Firewall Use. Networks containing electronic IIHI-based systems and applications must implement perimeter security and access control with a firewall. The IT Security Office will work with units to implement and configure the firewall appropriately.

H. Software Management. Installation of software, freeware or shareware must be approved and/or performed by the units Technical Liaison. University policies regarding licensing, intellectual property and copyright must be followed. See www.policy.ku.edu.

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 extent, frequency and nature of these reviews must be determined by the Clinic’s security environment. 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 Technical Liaison) 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. Workforce members seeking access to any network, system or application must not misrepresent themselves by using another authentication device.
3. Workforce members are not permitted to allow other persons or entities to use their unique authentication device.

4. A reasonable effort must be made to verify the identity of the person or entity prior to transmitting electronic 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) unless a determination has been made (and documented) by the Clinic that the current network configuration or an alternative confidentiality control effectively precludes unauthorized interception, mis-direction, re-direction or modification to electronic IIHI. Use of email to communicate PHI is strongly discouraged; email should not be used if other forms of communication are available, such as telephone call or overnight mail. Clinic policies and procedures 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. The University’s Office of Information Services has developed policies and procedures for remote access to University networks, systems and applications. See Virtual Private Network (VPN) Service on the University of Kansas Data Network at www.policy.ku.edu. In order to provide for the security of electronic IIHI assistance must be obtained from IT Security Office prior to implementing wireless access.

N. Wireless Access Policy. The University has developed policies and procedures for wireless access to University networks, systems and applications. See Wireless Local Area Network (LAN) Systems Policy at www政策.ku.edu. 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, floppy drives, CD ROMs) into and out of the Clinic, and the movement of these items within the Clinic. Such procedures must:
1. Provide for a determination as to whether a retrievable copy of electronic IIHI is required prior to movement, re-use, or disposal.

2. Address the final disposition of electronic IIHI and/or the hardware on which it is stored.

3. Address removal of electronic IIHI from electronic media before it is made available for re-use.

4. Provide for a record of the movements of hardware and electronic media and the person responsible therefore.

5. 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 calling the IT Security Office at 864-0491.

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 which data 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.

**XVII. Administrative Requirements**

A Clinic is responsible for:

A. Compliance with University policies and procedures and state and Federal laws which relate to confidentiality and privacy 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 administrative, technical and physical safeguards 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.

D. Ensuring that all members of the Clinic’s Workforce, including student employees and volunteers, receive education on University and Clinic policies and procedures and laws regarding privacy and security of Patient information/PHI. Such education must be provided (and documented) within a reasonable period of time after the individual joins the Clinic’s Workforce.

1. **Privacy and Security Awareness.** The University will make available to Clinics an on-line Privacy and Security Awareness Program. Clinic Workforce shall be required to complete the on-line Program prior to April, 2005 and all Workforce members hired after April, 2005 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 as needed) 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 [www.security.ku.edu](http://www.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. 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.
F. Communicating to Clinic Workforce members their duty to report breaches of privacy or confidentiality to their supervisor or to the Lawrence Campus HIPAA Privacy Officer.

G. Communicating to Patients and others their right to submit complaints, questions or concerns regarding the Use and Disclosure of PHI on the Lawrence Campus to the Clinic where the complaint, question or concern arose or to the Lawrence Campus Privacy Office at (785) 864-9528.

H. Investigating violations of applicable policies or laws regarding confidentiality and privacy of health information. 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 Lawrence Campus Privacy Coordinator.

I. Ensuring that appropriate sanctions for 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.

J. 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.

K. Documenting compliance with these guidelines. Documentation must be maintained for a minimum of six years.
APPENDIX

Sample Forms and Letters
AUTHORIZATION FOR USE OR DISCLOSURE OF HEALTH INFORMATION

PATIENT NAME: _______________________________________________________

PATIENT ADDRESS:____________________________________________________

DATE OF BIRTH:_____________ MEDICAL RECORD #: _____________

1. Type of Information to be disclosed:

2. Persons, facility, or class of persons authorized to use or disclose the information:

3. Persons, facility or class of persons authorized to receive the information:

4. Purpose of the use or disclosure:

5. Expiration Date (Not to exceed one year):

6. **Authorizing Signature:** I understand that once the uses or disclosures have been made as permitted by this form, the records/information may be subject to redisclosure and no longer protected by federal privacy regulations. I understand that I may refuse to sign this authorization and that my refusal to sign will not affect my ability to obtain treatment. I understand that I may revoke this authorization at any time in writing by delivering a written revocation to __________________________, but if I do, it will not have any effect on actions the Clinic took in reliance on this authorization prior to receiving the revocation. I authorize the use or disclosure of the records/information described above. I have read and understand this form.

_____________________________  _________________________________
Signature of Patient            Date

_____________________________  _________________________________
Signature of Parent/Legal Rep.  Date
(If Patient is under 18 years of age)

_____________________________
Address and Telephone of Legal Representative

_____________________________
Description of Legal Representative’s Relationship to Patient

2/01/2008 Version
REQUEST FORM FOR RESTRICTION(S) ON USE AND DISCLOSURE OF HEALTH INFORMATION

____________________________  __________________________
Patient Name                                                  Social Security #

I ____________________________________[print name], hereby request the following restriction(s) on the uses and disclosure of my health information. [Please describe the requested restrictions in as much detail as possible. Attach additional sheets as necessary.]

____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________

________________________________________________
Note: All previously signed restriction requests are void and the current document represents all restriction requests that may, if granted, be in effect. If the Clinic agrees to a restriction request or a portion thereof, such restriction shall not apply in emergency treatment situations.

☐ I will accept and submit to treatment without the approval of this restriction.
☐ I will not accept or submit to treatment without the final approval of this restriction.

__________________________           __________________
Signature                                                               Date

Please do not write below this line.

☐ The terms of this request are acceptable.
☐ The terms of this request are not acceptable.
☐ The terms of this request are acceptable, with the following amendment:

____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________

______________________________________________________
_________________________________________           _____________________
Signature                                                               Date

_________________________________________           _____________________
Print Name                                                              Title
REQUEST FORM FOR CONFIDENTIAL COMMUNICATIONS

You have a right to request that communications concerning your personal health information be made through confidential channels. We will do our best to accommodate all reasonable requests.

I, ________________________________(print name), SS#________________________ request the use of certain confidential channels for the communication of information related to my personal health, treatment or payment for treatment:

Alternate Phone Number:___________________________________________________
Alternate Address:
Street ________________________________________  City _____________________
State______ Zip Code _____________   E-mail address __________________________
Description of special communication methods to be used (not listed above):
______________________________________________________________________________
__________________________________________________________________

I understand that e-mails from my health care provider will travel over an unsecured network and that the privacy of my health information communicated through this channel cannot be guaranteed.

______________________________________________   ________________________
Signature of Patient or Patient’s Personal Representative                         Date

This decision can be made only by an authorized Clinic employee.

□ Accepted, the request can be reasonably accommodated by Clinic.
□ Denied, the request can not be reasonably accommodated by Clinic

Decision made by ________________________________

Employee Name (Print)                        Title

______________________________________   _________________________
Employee Signature                                      Date

Recorded in Patient’s Designated Record Set?   □ Yes □ No
Letter Denying a Request to Inspect or Copy Health Information: UNREVIEWABLE DENIAL

Dear (Patient):

At [insert Clinic name] each patient is provided the right to request to inspect and/or obtain a paper copy of his or her health information. Each request is reviewed and is subject to the limitations outlined in state and Federal law. Based upon this review, your request has been denied (either in full or in part) due to the following (circle one):

a. You are involved in research that includes treatment. You agreed to the denial of access when you consented to participate. The right of access will be reinstated upon completion of the research.
b. The records you requested include psychotherapy notes.
c. The records you requested include information compiled for use in civil, criminal or administrative actions.
d. The records you requested include information that is subject to a prohibition on access by a federal law entitled the Clinical Laboratory Improvements Amendments (CLIA).
e. The information that is contained in the records is subject to a federal law entitled the Privacy Act, 5 U.S.C. Section 522a, and the denial meets the requirements of that law.
f. The facility is acting under the direction of a correctional institution.
g. The facility does not maintain the information. Please contact _________________ facility to access this information.

Per Federal Law this denial is not subject to further review or appeal.

Please contact me with any questions or concerns regarding this matter. You may submit a complaint regarding this matter to the Privacy Coordinator, Lawrence Campus, by calling (785) 864-9528, or you may contact the Secretary of the U.S. Department of Health and Human Services.

[signature]
[name and title]

cc: (Attending Practitioner)
Dear (Patient):

At [insert name of Clinic] each patient is provided the right to request to inspect and/or obtain a paper copy of his or her health information. Each request is reviewed subject to state and Federal laws. Based on this review, your request has been denied (either in full or in part) for the following reason: [insert a description of the basis for the denial. HIPAA permits a denial of access, with an opportunity to have the decision reviewed, for the following reasons: (a) A licensed health care professional has determined, in the exercise of professional judgment, that the requested access is reasonably likely to endanger the life or physical safety of the individual or another person; (b) The health information makes reference to another person and a licensed health care professional has determined, in the exercise of professional judgment, that the requested access is reasonably likely to cause substantial harm to such other person; (c) The request for access is made by the individual's personal representative, and a licensed health care professional has determined, the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.]

You may request a review of this denial by submitting a written request for review to me at the address below.

Please contact me with any questions or concerns regarding this matter. You may submit a complaint regarding this matter to the University’s Privacy Coordinator, Lawrence Campus, by calling (785) 864-9528, or you may contact the Secretary of the U.S. Department of Health and Human Services.

[Signature]
[Name, Title and address]

cc: (Attending Provider)
REQUEST FORM FOR AMENDMENT OF HEALTH INFORMATION

You have the right to request that health information that pertains to you be amended if you believe that it is incorrect or incomplete. We will review your request and either grant your request or explain the reason why it will not be granted. If your request is not granted you have the right to submit a statement of disagreement that will accompany the information in question in future Disclosures.

I, ________________________________, (print name), SS# _____________, request that the following health information pertaining to me be amended (describe the information that you believe is incorrect or incomplete):

Date medical services were provided: ____________________

Location where medical services were provided:_________________________________

Entry that you are requesting to be amended:____________________________________
______________________________________________________________________________
__________________________________________________________________

I believe that the information that you currently have on file is incomplete or incorrect for the following reasons:______________________________________________________
______________________________________________________________________________
__________________________________________________________________

Additionally, I request that the following people be notified of the correction:__________
______________________________________________________________________________
______________________________________________________________________________
__________________________________________________________________

By identifying the above individuals and/or entities you are giving permission for this Clinic to notify the above individuals and/or entities of the amendment, if accepted. Such notification may include providing them with a copy of this completed form.

_____________________________________ ________________________
Signature of Patient or Patient’s Personal Representative                                    Date

Please do not write below this line

This Amendment is:

___Accepted
___Denied; information is accurate and complete as is
___Denied; information is not part of the designated record set
___Denied; information is not available for inspection

_____________________________________ ________________________
Employee Name and Title                                    Date
Letter Approving Requested Amendment of Health Information

Date: ______________

________________________________
________________________________
________________________________
________________________________

RE: Approval of Requested Amendment of Health Information

☐ Your request to amend your personal health information has been approved.

☐ We are in the process of notifying the individuals and/or organizations that you identified in your “Request for Amendment” form.

☐ We have identified the following additional persons and/or organizations that need to be notified of the amendment. If you would like for us to notify the persons and/or organizations listed below, please sign, date and return a copy of this letter to the address below. We will not notify the following persons or organizations until this signed form is returned.

____________________________________________________________________________
____________________________________________________________________________
____________________________________________________________________________
______________________________________________________

[Insert Clinic address]

[insert Name and Title]

I give my permission for [insert Clinic name] to notify the person(s) and/or organizations above.

________________________________________                 ___________________
Signature of Patient or Personal Representative                                    Date
Letter of Notification Third Parties Regarding Amendment of Health Information

Date: ______________

________________________________
________________________________
________________________________
________________________________

RE: Amendment of Patient Health Information

We have agreed to a request from the following Patient to amend his/her health information.

Patient’s Name: __________________________________________________________

Last                                     First                              Middle

Patient’s Date of Birth ___________________

Patient’s Social Security Number ____________________

☐ The amendment we have made to the Patient’s health information is reflected on the copy of the enclosed request form.

☐ The actual amendment is as follows:

______________________________________________________________________________
______________________________________________________________________________
______________________________________________________________________________
______________________________________________________

We are notifying you of this information so that you may amend your records appropriately.

[Name/Signature]

______________________________________________________________________________

Title
Letter Denying Requested Amendment of Health Information

Date: ______________

________________________________
________________________________
________________________________
________________________________

RE: Denial of Request to Amend Health Information

Your request to amend your health information has been received and reviewed. We have consulted with our staff and have determined that we cannot accept your requested amendment. Your request has been denied for the following reason(s):

☐ We have determined that the information is accurate and complete as is.

________________________________

☐ The information did not originate here.

________________________________

☐ The information is not part of the designated record set (medical and billing records).

________________________________

You may submit a written statement disagreeing with this denial. If you wish to submit a statement of disagreement please send your written statement to the following address: [insert address].

If you do not submit a written statement, you may also ask that the Clinic include a copy of your amendment request form and this denial letter with any future releases of your medical records. If you would like us to do so, please notify us of your desire, in writing, at the above address.

Please contact me with any questions or concerns regarding this matter. You may submit a complaint regarding this matter to the University’s Privacy Coordinator, Lawrence Campus, by calling (785) 864-9528, or you may contact the Secretary of the U.S. Department of Health and Human Services.

_________________________________                       __________________________
Signature                                                                          Title
**Disclosure Log**

This log is a tool to document all Disclosures of IIHI that a Patient may not be aware of. These fields may be incorporated into a computerized tracking system. You do not need to account for the following types of Disclosures:

- To carry out Treatment, Payment and health care Operations;
- To Patients of about themselves;
- Pursuant to an individual Authorization;
- To persons involved in the patient’s care, such as a patient’s Personal Representative;
- As part of Limited Data Set
- For the Clinic's directory (if applicable) or to persons involved in the Patient's care;
- For national security or intelligence purposes;
- To correctional institutions or law enforcement about an inmate
- That occurred prior to the April 14, 2003.

**Patient Name:** _______________________________________

**Medical Record No.** __________________________________

<table>
<thead>
<tr>
<th>Date Disclosed</th>
<th>Disclosed to (Name and Address)</th>
<th>IIHI disclosed (Title of document and date or other identifying information)</th>
<th>Purpose of Disclosure</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Request Form for Accounting of Disclosures of Health Information

You have a right to request an accounting of non-routine Disclosures of your personal health information. You may receive one accounting of such Disclosures free of charge every 12 months. There will be a cost based fee charged for any accounting requested more frequently than 12 months. The accounting will include Disclosures made up to six years prior to the date of the request (or a shorter period if requested). However, it will not include Disclosures made before April 14, 2003.

I, ________________________________(print name), SS#________________________ request an accounting of Disclosures of my personal health information by ___________ during the following time period __________________________.

I understand that this accounting will not reflect disclosures:

- To carry out treatment, payment and health care operations of the Clinic;
- To Patients of health information about themselves;
- Pursuant to an individual authorization;
- To persons involved in the patient’s care, such as a patient’s Personal Representative;
- As part of Limited Data Set;
- For the Clinic's directory (if applicable) or to persons involved in the Patient's care;
- For national security or intelligence purposes;
- To correctional institutions or law enforcement about an inmate; or
- That occurred prior to the April 14, 2003.

__________________________
Signature of Patient

__________________________
Signature of Personal Representative of Patient

__________________________
Description of Personal Representative’s Authority to Act for Patient

__________________________
Date
Information System Access Request (Example)

Request for:  [ ] Add  [ ] Change  [ ] Delete

Clinic/Unit/Dept. Name: __________________________________________________

User Name: ____________________________________________________________________

(Last)     (First)     (MI)

User Job Title: _______________________________ User Extension: __________________

Which category best describes the requesting User:   [ ] Unit/Clinic staff    [ ] Faculty
[ ] Student       [ ] Volunteer    [ ] Other: _______________________________________

Requesting access to Standard Configuration Group Profile:

<table>
<thead>
<tr>
<th>Requesting access to the following System</th>
<th>Signature of Authorized System “Owner”/”Data Steward”</th>
<th>Title of System “Owner”/”Data Steward”</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ ] Patient Billing/Accounting System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[ ] Electronic Medical Record System</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

If requesting access to the Internet, please justify the business need for this service:
_____________________________________________________________________________________
___________________________________________________________________________________

I understand that University/Unit information systems may be used only to carry out authorized job responsibilities. I agree to comply with the policies of the University of Kansas and my unit with regard to the proper use of computing resources and requirements for accessing, using and disclosing confidential data.

User Signature: ___________________________ Title: __________________ Date: ____________

Supervisor Signature:_______________________ Title: __________________ Date: ____________

To be completed by Technical Liaison/IT Staff:

<table>
<thead>
<tr>
<th>Status</th>
<th>Completed by</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Training completed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Set up in production</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User notified</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supervisor notified</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Additional Comments Regarding Set Up:_____________________________________________
______________________________________________________________________________

Return Form to: _________________________________

2/01/2008 Version - 53 -
Sample Confidentiality and Security Agreement

Name _________________________________      Unit___________________________
Supervisor_____________________________

1. I recognize that I will have access to confidential data that is governed by University policy and state, and federal law. Examples of confidential data include but are not limited to information pertaining to individual’s physical or mental health and treatment, individual’s financial information and other personally identifiable data, such as Social Security Numbers.

2. I recognize that data accessed by me is for conducting official University business and may only be used for the purposes outlined in University and unit policies and procedures. I will not store, use, or access data except as permitted by the official policies and procedures of the University and my unit.

3. I recognize that disclosure of data is governed by the policies and procedures of the University and my unit, as well as by state and federal law. I will not release data in any circumstances other than those defined by the policies and procedures of the University or my unit; or as otherwise permitted or required by law and only after proper identification and verification of identity and authority is ensured.

4. I will not share sign-on passwords or log-on information with anyone except as requested by my supervisor or unit head, by an information services professional in order to resolve a technology problem, or by a University official or law enforcement official in an emergency situation (as permitted or required by applicable law) and only after proper identification and verification of identity and authority is ensured.

5. I agree to report loss of a password, or any actual or attempted unauthorized access, use or disclosure of confidential data to my supervisor or unit head and to other University personnel or officials as required by the policies or procedures of the University or my unit.

6. I understand that violation of these policies and procedures may result in disciplinary action, including but not limited to, privilege revocation and/or suspension or termination.

7. I understand that my obligations under this Agreement will continue after termination of my relationship with the University. Upon termination, I will immediately return any documents or media containing confidential data to the University.

8. I have read and understand this document.

_________________________________  ____________
Signature                                                                     Date

_________________________________  ____________
Supervisor Signature                                                   Date
TERMINATION OF ACCESS CHECK LIST

This checklist is intended as a guide for terminating employee access to University facilities and information resources. If you believe that an individual’s access privileges should be suspended on an immediate basis to maintain the security, confidentiality and/or integrity of University Data or IT systems, the Coordinator of IT Policy and Planning must be notified immediately at 864-4999.

Employee Name/Title: ____________________________ Date: ____________

Department/Manager: ____________________________________________

1. University Property
   __ Returned desktop computers/laptops and accessories
   __ Returned Mobile phones and pagers
   __ Returned other equipment/devices
   __ Returned all computer disks, tapes, other electronic storage media
   __ Returned other records, files

2. Keys/Access Cards/Badge
   __ Returned all keys to facility/office/lab
   __ Returned all keys to desk/filing cabinets/storage units
   __ Returned all access cards
   __ Combination/cipher locks changed
   __ Returned ID Badge

3. University Information Systems
   __ Provided location of all electronic information
   __ Unit Technical Liaison notified of change and the systems/applications accessed by exiting employee so that access can be terminated.* (List systems/applications below)

   1. ____________________________________________________
   2. ____________________________________________________
   3. ____________________________________________________
   4. ____________________________________________________
   5. ____________________________________________________

Authorized Signature ______________________________________ Date ____________

-------------------------------------------------------------------------------------------------------------------

Confirmation of Access Termination:

The above individual’s access to the systems/applications listed in section 3 has been terminated.

__________________________________________   __________________________
Technical Liaison or other Responsible Party       Date
Portable Device Receipt & Acknowledgement

I, ____________________________________ hereby accept receipt of the following equipment from the University of Kansas:

<table>
<thead>
<tr>
<th>Device Name &amp; Description</th>
<th>Model #</th>
<th>Serial #</th>
<th>Asset Tag #</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

I hereby acknowledge that these devices are provided solely for my use in conducting business related to my work for the University of Kansas. I agree to abide by the following protocol for use of such devices:

- The device is to remain in my sole possession unless otherwise approved by my immediate supervisor.
- Any device with a display is to be protected from casual viewing.
- The password protection features will remain enabled, will be used as established and used as I was instructed. I will not share by password with anyone.
- When the device is taken outside the Unit, it will be secured from loss, theft, unauthorized access, or temperature extremes.
- If the device is lost or stolen, I will immediately report the loss/theft to my supervisor/Unit Director and other University personnel as required by University policy.
- I will not download any software except as permitted by Unit and University policies and procedures.
- I will not connect additional peripherals (external drives, modems, etc.) except in accordance with Unit and University policies and procedures.
- I will not attempt to alter the serial number or the asset tag number.
- I understand that violation of Unit or University policies and procedures regarding the use of portable devices and computer resources may result in disciplinary action, including but not limited to, privilege revocation and/or suspension or termination.

_____________________________________________________   ________________
Signature of Recipient       Date

________________________ ______________________________________
Dept.    Unit