OFFICE OF
THE VICE
CHANCELLOR
FOR
RESEARCH
UIC

Office for the Protection of Research Subjects (OPRS)
Institutional Review Board
FWA# 00000083

201 AOB (MC 672)
1737 West Polk Street
Chicago, IL 60612-7227
Phone: 312 996-1711
Fax: 312 413-2929
http://research.uic.edu/human-subjects-irbs/

POLICY: Research Data Security

Version:1.1; Date: 06/25/2015
Approved by: Human Protections Administrator, Director of OPRS, and Executive IRB Chair
AAHRPP REF #: 616
AAHRPP Elements: II.3.E.

BACKGROUND:

The protection of personal and confidential information of research participants is one of the University's highest priorities. The University of Illinois at Chicago (UIC) conducts research in compliance with all applicable state and federal laws and regulations and UIC policies. Federal regulations require that research studies involving human subjects include adequate provisions to protect the privacy interests of participants and to maintain the confidentiality of data. In its review of research, the UIC Institutional Review Board (IRB) considers whether adequate provisions exist for the security of research data, whether in paper or electronic form, throughout the research, including data analysis and retention. Investigators are responsible for ensuring that adequate controls, as described in the research protocol, are in place and followed to protect identifiable and confidential information and that only the minimum protected health information (PHI) necessary for purposes of the research is collected. It is also the responsibility of the Principal Investigator to abide by any additional data security provisions that may be required by the IRB or under the terms of a sponsored project agreement (such those in the Federal Information Security Management Act or the Food and Drug Administration's Electronic Records regulations).

While privacy and confidentiality issues are covered by several related UIC Human Subjects Protection Program (HSPP) policies, recent federal legislation [i.e., American Recovery and Reinvestment Act of 2009 (ARRA) / Health Information Technology for Economic and Clinical Health Act (HITECH Act)/Final Omnibus Rule] and new University policies require the Office for the Protection of Research Subjects (OPRS) and the IRBs to reassess data security requirement specific for human subject research.

The HITECH Act has established new notification requirements regarding the unauthorized disclosure, use, acquisition or access of unsecured PHI that poses a significant risk of financial, reputational or other harm to an individual. Notice of the breach generally must be given to the individuals involved by mail or e-mail if the individual affected has agreed to receive notices electronically. If, however, the breach involves the PHI of ten or more individuals for whom there is insufficient or out of date contact information, then notice of the breach must be posted on the web or in "major print or broadcast media where the individuals likely live." The notice also must be posted in local print and broadcast media if the breach involves more than 500 individuals, and the HHS Secretary must also be immediately notified in this case. The notice must be given as soon as reasonably possible, and in no event later than 60 calendar days after the breach is discovered, or should have been discovered. The breach notification requirements are not applicable to encrypted or de-identified data.

In September 2009, the *Interim University Information Security Policy* was approved by the University Technology Management Team and established security principles. This policy prohibits the storage or transmission of University information unless adequate controls have been established to protect the information in the event of theft or other loss.

On July 1, 2014, the UIC Information Technology Security Program policies were enacted, which includes requirements for safeguarding all UIC data including data collected for research purposes. The IT Security Program and its policies have been approved by the UIC Informatics Technology Governance Council (ITGC) – Infrasec Committee, the UIC Deans Council, the UIC Chancellor and Vice Chancellor Committee, and the UIC Faculty Senate.

The UIC HSPP policy *Research Data Security* is intended to guide compliance with new regulations and policies, and, by making use of technological advances in data security, enhance privacy and confidentiality safeguards.

POLICY:

I. UIC researchers must ensure that research data are protected, at a minimum, in a manner consistent with human subject protection regulations (45 CFR 46, 21 CFR 50 and 56), the HIPAA Privacy and Security Rules (45 CFR 160 and 164), 2009 HITECH Act, 2013 Breach Notification (Omnibus) Rule, other federal and state laws (e.g., FERPA), and University and UIC policies (e.g., UI Social Security Number Policy, UIC IT Security Program).

II. The research protocol and corresponding protocol application must include a data security and management plan. A data security/management plan should address the following:
- How data will be collected and recorded
- The type of identifiers linked to the research data
- How the data will be stored and secured, including paper and electronic formats
- When identifiers will be removed (data de-identified)
- Disposition or storage of data after study completion
- Any future use of the research data.

III. This policy focuses on the data security requirements and the minimal standards for the collection, storage, use, transmission, and destruction of UIC PHI associated with research data to meet new federal mandates and institutional policies, including University Information Security policies. However, these data security standards will be similarly applied by the UIC IRBs to research involving other types of sensitive and highly sensitive information.

IV. This policy outlines the reporting requirements when a security breach involving sensitive information occurs and the additional reporting requirements when the research involves the use of PHI.

V. Research data consisting solely of de-identified health information do not meet the definition of PHI and therefore is not subject to the 2009 HITECH Act breach notification requirements.

VI. Encryption of PHI or destruction of the media containing the PHI following the procedures stipulated in the statutes are the only methods recognized by the HITECH Act as rendering data into a form where it is unusable, unreadable, or indecipherable to unauthorized individuals and obviating the need for breach notification. Data is considered “secured” after encryption or destruction.

VII. For research involving the JBVAMC, refer to the VA data privacy and security requirements and corresponding HSPP policies requirements.

DEFINITIONS:

I. DATA ENCRYPTION: Encryption is the conversion of data into a form, through use of an algorithm, which renders electronic data, unusable, unreadable, or indecipherable by unauthorized persons. Decryption is the process of converting encrypted data back into its original form, so the data can be usable and understood.

II. PROTECTED HEALTH INFORMATION (PHI): Individually identifiable health information transmitted or maintained in any form or medium, including oral, written or electronic. Individually identifiable health information relates to an individual’s health status or condition, furnishing health services to an individual, or paying or administering health care benefits to an individual. Information is considered PHI where there is reasonable basis to believe the information can be used to identify an individual.

III. ePHI: Electronically protected health information.

IV. PERSONAL INFORMATION (PI): As defined by the IL Personal Information Protection Act (PIPA – 815 ILCS 530/5), an individual’s first name or first initial and last name in combination with any one or more of the following data elements when either the name or the data elements are not encrypted or redacted: (1) social security number; (2) driver’s license number or State identification card number; or (3) account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual’s financial account. “Personal information" does not include publicly available information that is lawfully made available to the general public from federal, State, or local government records.

V. PERSONALLY IDENTIFIABLE INFORMATION (PII): Any information about an individual that could, potentially identify that person, such as a name, street address, credit card number, email address, telephone number or social security number. A subset of PII is PHI.

VI. DE-IDENTIFIED HEALTH INFORMATION: Health information that does not identify an individual, and there is no reasonable basis to believe that the information can be used to identify an individual, is considered de-identified. In accordance with the HIPAA Privacy Rule, health information can be de-identified by two means:

A. *Statistical Method*. An independent, qualified statistician:
   1. Determines that the risk of re-identification of the data, alone or in combination with other data, is very small; and
   2. Documents the methods and results by which the health information is de-identified, and the expert makes his/her determination of risk.

B. *Removal of All Identifiers (Safe Harbor Method)*. The removal of all 18 HIPAA elements from the health information that could be used to identify the individual or the individual's relatives, employers, or household members.

The de-identified health information may include a code (re-identification code) that will permit the information to be re-identified, if necessary, provided that; the key to such a code is not accessible to the researcher requesting the use or disclosure of the de-identified health information; that the code was not derived from or related to information about the individual or cannot be used to identify individuals; and the covered entity does not use or disclose the code for any other purpose, and does not disclose the mechanism for re-identification

VII. SECURITY BREACH: A situation in which unencrypted PHI or sensitive information is reasonably believed to have been acquired by an unauthorized person, including an employee's and/or student's access of PHI that is not in accordance with the job responsibilities, and that poses a significant risk of financial, reputational, or other harm to the individual whose records were accessed. A suspected security breach means that this information may have been lost or stolen, accessed in an unauthorized fashion or infected by a virus or worm, but it is not yet known whether the information has been compromised to meet the level of a security breach (see section IV.C. for further information).

The HIPAA Breach Notification Rule defines a "breach" as the acquisition, access, use or disclosure in a manner not permitted under the Privacy Rule that compromises the security or privacy of the protected health information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual.

Exceptions to the definition of breach are described at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html

In the case of a Breach of PI of an Illinois resident, the University will notify the resident that there has been a breach in the most expedient time possible and without unreasonable delay, consistent with any measure necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system. (Note: If the PI of residents from other States has been compromised, those States' breach notification laws should be evaluated.)

VIII. SENSITIVE/HIGHLY SENSITIVE INFORAMTION: As defined by the September 2009 Interim *University Information Security Policy*, sensitive information is defined as information that if disclosed or modified without authorization would have severe or serious adverse effect on the operations, assets, or reputation of the University, or the University's obligations concerning information privacy. Information in this category includes, but is not limited to:

- Assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure, such as credit card information
- Covered by federal and state legislation, such as HIPAA, FERPA, or the Data Protection Act
- Payroll, personnel and financial information

In the research setting, sensitive information also includes, but is not limited to individually identifiable information involving:

- AIDS, sexually transmitted diseases, or alcohol or substance abuse or treatment.
- Illegal conduct or arrest record
- Student education records
- Sexual attitudes, preferences, or practices
- Psychological or mental health information
- Disclosure of information outside of research that could reasonably cause discrimination or stigmatization, or result in damage to subjects' financial well-being, employability, or reputation

IX. UNSECURED PHI: Protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology specifically involving the encryption of data that are at rest (i.e. residing in databases) and/or data in motion (i.e. wireless transmission).

PROCEDURE:

I. Collection, Storage, Use, and Transmission of Research Data with PHI and Other Sensitive Information

A. In addition to federal human subject protections regulations, electronic research data containing PHI must both be used and stored in a HIPAA compliant fashion. The HIPAA Omnibus Rule (Final Breach Notification Rule) identifies IT security technologies and methodologies that if used render PHI unusable, unreadable or indecipherable to unauthorized individuals (see References).

B. The research protocol and protocol application, including applicable appendixes, must describe the security measures in place for maintaining the privacy of the subjects and confidentiality of the data.

C. Only the minimum necessary PHI and other sensitive information should be collected to achieve the purposes of the research. The protocol and protocol application should describe exactly what identifiable data elements will be collected and include the submission of a data collection form/spreadsheet as part of the protocol submission packet.

D. The UIC IRB expects investigators to have in place one or more of the following standards when their research data contains PHI. The IRB will determine the level of security for each protocol based on the presence of identifiers, sensitivity of the data and risks of a breach.

1. Electronic PHI (ePHI), PII, and sensitive data hosted on any device, whether in an open area and/or is potentially exposed to theft or loss (i.e., laptops, portable hard drives, flash drives, USB memory sticks, smart phones, mp3 players, or similar portable storage devices not specifically listed) or hosted on a desktop computer, must be encrypted. The HITECH Act reporting requirements are applicable to unsecured PHI and not encrypted PHI.
   a) Encryption software applications should preferably be supported by the UIC Academic Computer and Communications Center (ACCC), and allow central management, have a central key repository with a password recovery mechanism and contain auditing functions. Symantec Encryption Desktop (formerly known as PGP Desktop) is the encryption solution supported by ACCC and is available to UIC faculty, staff, and students on University computers at no cost - http://accc.uic.edu/service/encryption

      The use of PHI within the e UI Health System must be compliant with their policy IM 4.13 (Portable Electronic Device Safeguards). Any PII or confidential data contained on portable electronic devices must be encrypted. Portable electronic devices are not to contain PHI. For encryption software applications other than those supported by ACCC or UI Health System, the investigator must provide the IRB with documentation confirming the software's compliance with the HITECH Act standards.

b) Because electronic portable devices are particularly susceptible to loss or theft, the storage of identifiable subject data, even encrypted files, should be limited and data transferred to a secure system as soon as possible. When not in use, electronic portable devices must be securely stored.

2. ePHI hosted on servers secured and housed in a HIPAA compliant environment. Currently an example of such a server at UIC meeting these criteria is the UI Health System server. For example, PHI collected from Cerner for a chart abstraction could be securely stored on the UI Health System H drive or the REDCap installation maintained at the Institute for Health Research and Policy (IHRP). Notification is required if a breach occurs, e.g., the server is hacked and unsecured PHI is removed.

3. Record and retain only de-identified data. The IRB will require documentation that investigators will not have access to identifiers or code linked to identifiers and will not attempt to identify the subjects. No notification required if breach occurs.

4. When possible, limit PHI to a limited data set, where identifiable elements are limited to city, state, ZIP Code, elements of date, and other numbers, characteristics, or codes not considered to be direct identifiers. Any breaches must be reported to the IRB and privacy officer. In addition, the Breach Notification (Omnibus Final) Rule may require notification if the covered entity determines the breach poses a significant risk of financial, reputational or other harm.

5. When encryption, de-identification or a limited dataset are not able to be implemented, research data should be coded and identifiers removed by the PI or a research team member as soon as feasible, with a master list containing the identifiers secured and kept in separate file cabinets (paper records) or on a separate physical device (electronic data). The web-based research electronic data capture application, REDCap, can be used to securely collect and manage such high risk data- http://www.ccts.uic.edu/content/redcap-research-electronic-data-capture.

E. Access to identifiers should be limited to authorized research personnel and be physically secured throughout the conduct of the research.

1. Any paper records should be stored in a locked cabinet or other fixture in a secure location with access limited to research personnel. All personnel must be listed on the protocol application or *Appendix P*, and have met UIC's human subject protections and HIPAA research training requirements.
2. The consent forms/authorizations should be kept separately and securely from the data files.

F. Identifiers should be removed/destroyed as soon as they are no longer needed. The protocol should specify plans for retention or destruction of identifiers/de-identification. Once research data are de-identified, they are no longer PHI and, therefore, no longer subject to the HIPAA Breach notification requirements.

G. PHI and other sensitive research information should only be transmitted over secure networks, regardless of location, or as encrypted data files over public networks. PHI should not be transmitted via e-mail unless encrypted. If the research involves electronic transmission of PHI and other sensitive information, the types of transmission and methods to secure the data during transmission must be described in the research protocol and IRB application. When email is used, whenever possible, the UIC hosted or UI hospital email system should be used. For example, the use of Gmail accounts for recruitment purposes may inadvertently create additional risk to the University through those accounts.

H. Any investigator who uses external survey software, other than Qualtrics or REDCap, must provide evidence of a business agreement between the University and the external survey software provider if PII, including PHI, will be collected. Qualtrics is a sophisticated, easy to use web-based service for creating, publishing, and analyzing survey data for which the University has a business associate agreement with and thus allowing the collection of high risk data using this application – http://accc.uic.edu/tag/qualtrics

I. Telefaxing of PHI for research purposes is generally NOT permitted. If PHI is transmitted via fax it must be done so in accord with UI Hospital Policy IM 4.08 (Fax Transmittal of Protected Health Information (PHI)).

J. PHI and other identifiable information, including contact information, cannot be distributed outside UIC without the specific authorization of research subjects and approval by the IRB. The distribution of PII, including PHI external to UIC requires a data use agreement, a business associate agreement or patient/subject consent/authorization.

K. Upon completion of the research study and submission of the *Final Research Report*, the investigator must describe the final disposition of all research data. If identifiers must be retained in the data files because of specific needs of this research study or anticipated future research use, the investigator must provide a justification, which may require the establishment of a data repository protocol. The IRB will expect that data be destroyed or the investigator must specify a long-term plan for maintaining the security of the data, including the identity of the individual/entity that is designated as the custodian of the data.

L. Investigators leaving the employ of UIC who desire to remove the data generated from their research are required to obtain a *Data Transfer/Use*

Agreement, *Material Transfer Agreement*, or equivalent in accordance with University requirements. Additional requirements may apply regarding the removal of PHI (refer to OVCR ORS website or contact ORS).

Upon the departure of an investigator, custody of data remaining at UIC must be established and communicated to the IRB. Faculty sponsors must ensure that PHI or other identifiable information is not removed in an unauthorized fashion by their students, fellows, or residents.

M. The principal investigator and research team members are responsible for working with their IT administrator to ensure computers are updated with *appropriate* basic security measures such as strong passwords, anti-virus, anti-spyware, firewall and encryption software, as well as the latest software and operating system patches.

II. Destruction and Disposal of PHI

A. Documents that contain PHI must be shredded before disposal or disposed of through a university approved document destruction service. Documents or materials that contain identifiers and that cannot be shredded should have the identifiers obscured or obliterated before disposal. Documents or materials with subject identifiers should never be put in the general trash.

B. If a unit is using a university approved document destruction service, it must have a Business Associate Agreement for this service. Units must work with the Office of Business and Financial Services (OBFS) to enter into such a service agreement. The unit should also keep records of the documents that were provided for destruction and obtain from the service a certificate or other evidence of destruction.

C. Electronic media, including copiers and scanners must be cleared, purged, or destroyed such that PHI cannot be retrieved and in accordance with NIST Special Publication 800-88, *Guidelines for Media Sanitization -* University policies, and state laws*.*

III. Breaches of Data Security

A. To fulfill the HIPAA HITECH breach reporting requirements and in accordance with *UI Health System HIPAA Breach Notification* policy (Policy No. IM 4.23), any breach or suspected breach involving UI Health System PHI in the custody of the principal investigator, co-investigator(s), research staff, students, or business associate should be immediately reported to the HIPAA Privacy Officer: (312) 355-5650 privacyoffice@uic.edu.

B. Breaches or suspected breaches of data security, including PHI and other sensitive information, are considered by UIC policy to meet the definition of a potential unanticipated problem and must be reported to the IRB using the

Prompt Reporting to the IRB form within 5 working days of becoming aware of the event. The IRB will review the report and contact the UI Health System HIPAA Privacy Officer if the breach involves UIC PHI or other applicable University officials (i.e. University Registrar for breach involving FERPA data). Examples of possible data breaches include, but are not limited to, the following:

- Lost or misplaced files, folders, etc.
- Lost or stolen computer, laptop or other electronic storage device with unencrypted PHI
- Access of PHI without a *business* need to know – (i.e., workforce access of PHI of friend or celebrity)
- Faxes sent to the wrong fax machine
- Improper disposal of paper containing PHI – (i.e., not shredded)
- Information delivered to the wrong participant using the postal service, courier, or other delivery method
- Loss/violation of the integrity of decryption key or process
- Compromised computer/device – (i.e., infection by a worm or virus)

C. Investigators are strongly encouraged to immediately report breaches and suspected breaches of data security to the College/Department/Unit IT administrator and follow applicable IT incident reporting policies. Any physical property loss must also be reported to the University police. Information regarding reporting and responding to IT security incidents may be found in the UIC IT Security Program policies (RC.P.5.0 Reporting and Responding to IT Security Incidents Procedure).

IV. Implementation

A. New protocols - All new research protocols involving PHI submitted for IRB review after March 01, 2011 must address the information security requirements through the submission of *Initial Review Application: Health and Biological Sciences* (Vs. 4.4 or later) or *Initial Review Application: Social and Behavioral Sciences* (Vs. 4.1 or later).

B. Existing protocols – Any active, IRB-approved research protocol involving PHI must address the HIPAA HITECH Act information security requirements at the time of continuing review through the submission of an amendment of *Appendix M – Research Data Security Plan*. In addition, investigators may also submit Appendix M as an amendment prior to the time of continuing review.

REFERENCES:

45 CFR Parts 160 and 164 – HIPAA Privacy and Security Rules

HIPAA Breach Notification Rule – 45 CFR 164.400-414 –
http://www.hhs.gov/ocr/privacy/hipaa /administrative/breachnotificationrule/index.html

Illinois Personal Information Protection Act 815 ILCS 530/5
http://statutes.laws.com/illinois/chapter815/2702

UI Health System Policy No. IM 4.23, "HIPAA Breach Notification"

OVCR Office of Research Services (ORS) Guidance "Material Transfer Agreement" -
http://research.uic.edu/sponsored_programs/award/mta

Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) - http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

UI Social Security Number Policy - http://www.ssn.uillinois.edu/ssn_home/

UIC Information Technology Security Program (7/1/2014) –
http://security.publish.uic.edu/policies/

REVISION LOG:

Version (#, date)	Replaces (#, date)	Summary of changes
1.1, 06/25/2015	1.0, 02/02/2012	Updated items based on HITECH Final Rule; incorporation of IL PIPA; inclusion of UIC IT Security Program policy, updates of website links.