



Landon Blakey  
ID 10510445

# University of Virginia-HIPAA Module

University of Virginia - IRB-HSR RESEARCHER BASIC COURSE

**University of Virginia** is solely responsible for the accuracy and appropriateness of the material, the compliance with applicable legal requirements such as copyright, and the maintenance of this custom module. This module is included in your course at the request of this organization. Questions or concerns regarding this material should be directed to **University of Virginia**.



## CITI Program, University of Virginia's HIPAA module




### --HIPAA Introduction

In 1996, Congress enacted the Health Insurance Portability and Accountability Act

(HIPAA). The primary purpose is continuity of health insurance coverage if you change

(HIPAA). The primary purpose is continuity of health insurance coverage if you change jobs, but it also provides for standards for health information transactions and privacy and security of patient data. HIPAA provides patients the right to know who will use their protected health information for research purposes. Protected health information, or **PHI**, is **any** medical information (for example, x-rays, specimens, databases, registries)

that can be identified as belonging to a particular individual. **It is NOT just the medical record!**



## --IRB for Health Sciences Research at UVA (IRB-HSR) vs. Privacy Board

HIPAA regulations allow the Institutional Review Board (IRB-HSR at UVA) or a separate body known as a privacy board to oversee the HIPAA regulations at an institution. UVA has decided to add HIPAA oversight to the responsibilities of the IRB-HSR instead of creating a separate committee which would also have to approve research. Therefore, the IRB-HSR has added additional questions to the protocol template to provide the IRB-HSR with the information needed to comply with HIPAA.



## --HIPAA and IRB-HSR Consent Forms

A patient's identifiable protected health information (PHI) can be used for research **ONLY** if the subject has signed a HIPAA authorization or a waiver is granted by the IRB-HSR. The IRB-HSR consent form templates include all HIPAA requirements so that the IRB-HSR consent form acts not only as the consent for the research protocol, but also covers the HIPAA authorization. HIPAA requires that HIPAA authorizations be kept for 6 years therefore the consent form must now be kept for 6 years from the closure date of the protocol. (If your protocol is part of a FDA application, they may need to be kept longer- please check with the sponsor.)



## --Identifiable Criteria under HIPAA

The IRB-HSR will determine if the protocol requires HIPAA oversight. If the data collected for the protocol includes any of the following identifiers, then the data is "IDENTIFIABLE" per HIPAA regulations and the protocol would be regulated by HIPAA in addition to current federal regulations governing research. All items refer to those items affiliated with the subjects of this protocol or the subject's relative, household member or employer.

1. Name
2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of the zip code if, according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same 3 initial digits contains more than 20,000 people and (2) The initial 3 digits of a zip code for all such geographic units containing 20,000 is changed to 000.
3. 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.
4. Telephone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social Security number
8. Medical Record number
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers

12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, code that is derived from or related to information about the individual (e.g. initials, last 4 digits of Social Security #, mother's maiden name, first 3 letters of last name)
19. Any information that could be used alone or in combination with other information to identify an individual (e.g. rare disease, researcher has access to a code)

## --Release of Identifiable Data

Identifiable data may be used and released for research in several ways. The simplest way is with authorization from the patient via a IRB-HSR approved consent form. The second method is via a HIPAA waiver of consent from the IRB-HSR. A HIPAA waiver may be granted by the IRB-HSR as long as the protocol meets the HIPAA waiver requirements listed below.

- A. The use or disclosure of protected health information involves no more than minimal risk to the privacy of individuals, based in, at least, the presence of the following elements:
  1. An adequate plan to protect the identifiers from improper use and disclosure;
  2. An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and
  3. Adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law.

for authorized oversight of the research study, or for other research for which the use or disclosure of protected health information would be permitted by this subpart.

- B. The research could not practicably be conducted without the waiver or alteration, and
- C. The research could not practicably be conducted without access to and use of the protected health information

## --Tracking Requirements under a HIPAA Waiver of Consent


If the IRB-HSR has granted a waiver of consent under HIPAA for identifiable protected health information to be released without authorization or consent from a patient, the principal investigator is responsible for TRACKING the release of this information. A patient has the right to request a report that includes a listing of where their identifiable protected health information has been released without their authorization/consent. This report must include disclosures for up to 6 years (beginning April 14, 2003). If your protocol is granted a waiver of consent under HIPAA, the IRB-HSR will notify the PI of this at the time of IRB-HSR Approval. The PI must then follow the tracking instructions found on the IRB-HSR WEB-site.

## Limited Data Sets

HIPAA provides for a middle option between "IDENTIFIABLE" and "UNIDENTIFIABLE" This is called a Limited Data Set. The difference between "UNIDENTIFIABLE" and a "LIMITED DATA SET" is that full dates, additional geographic information (except the subject's street address) and codes derived from subject information may be used in a Limited Data Set. The data from a protocol can be considered part of a Limited Data Set if none of the following identifiers are recorded. All items refer to those items affiliated with the subjects of this protocol or the subjects relative, household member or employer.

1. Name
2. Postal address information, other than town or city, state, and zip code
3. Telephone numbers
4. Fax numbers
5. Electronic mail addresses
6. Social Security number
7. Medical Record number
8. Health plan beneficiary numbers
9. Account numbers
10. Certificate/license numbers
11. Vehicle identifiers and serial numbers, including license plate numbers
12. Device identifiers and serial numbers
13. Web Universal Resource Locators (URLs)
14. Internet Protocol (IP) address numbers
15. Biometric identifiers, including finger and voice prints
16. Full face photographic images and any comparable images

Under HIPAA regulations IDENTIFIABLE protected health information may not be released unless the patient has signed a HIPAA authorization (IRB-HSR consent form or UVA stand-alone HIPAA authorization) or the IRB-HSR has determined it meets the criteria of a limited data set or has been granted a waiver. The benefit to the investigator of limiting data to a Limited Data Set is that consent and/or tracking is not required, however a Data Use Agreement will be required. If your protocol meets the criteria of a Limited Data Set, the IRB-HSR or the Grants and Contracts office will provide you with instructions regarding the Data Use Agreement at the time of approval.



## Summary of Requirements to Comply with UVa Health System, Medical Center and University Policies and Guidance

***PHI is health information combined with a HIPAA identifier.***

- LIMIT- Limit the HIPAA identifiers to the minimal amount needed- e.g. use initials instead of name, use a code instead of initials, limit amount/type of health information collected
- SECURE- Secure PHI- encrypt any electronic file containing PHI, password protect computer and use VPNs/firewalls, lock it up, limit number of people who have access
- PROTECT- Protect PHI when using it.
  - Do not leave a file open on your desk.
  - Have discussions in private.
  - Do not lose it.
  - Do not share with those not on the study team or those who do not have a need to know.
  - Do not share with sponsor unless subject has already signed a consent form or IRB has approved waiver of consent.
  - Avoid emailing PHI outside of the "UVa HIPAA covered entity" unless the file is encrypted.
    - The "UVa HIPAA covered entity" includes the hospital, health system, School of Medicine, School of Nursing and the VP for Research Office.
- STOP, THINK and BE CAREFUL-
  - If this was your sensitive health information how would you want it protected?
  - There are significant monetary fines for loss or misuse of PHI
  - Your job may also be on the line

*For additional information see links under Information Sources below.*

**Information Sources**

UVa has policies covering the protection of PHI. These policies include the:

- UVa [Institutional Data Protection Standards](#)
- UVa policy on [Electronic Storage of Highly Sensitive Data](#), and
- UVa [Information Security Incident Reporting procedure](#),
  - The Information Security Incident Reporting procedure must be followed if sensitive research data is exposed. Sensitive research data would include any medical information that reveals an individual's medical condition and/ or history of medical services use.
- Medical Center Policy # 0021 "Confidentiality of Patient Information" Section D8

## --Databases/Specimen Banks

HIPAA regulations require IRB-HSR approval for the establishment of research databases/specimen banks. An additional IRB-HSR approval is required to use data/specimen from a research database/specimen bank. Many physicians develop databases to track their patients clinically. IRB-HSR approval is not required to establish or use the information from these databases for clinical or quality assurance purposes. Certain databases are also established for "mixed use" (e.g. both clinical and potential future research). IRB-HSR approval is required to establish these databases or to add additional data to a database established prior to April 14, 2003 if the primary purpose of the database is for research. An additional IRB-HSR approval is also required to use the data from any database for research.

## --Data Breach

In 2009, Title XIII of the American Recovery and Reinvestment Act (ARRA) entitled Health



Information Technology for Economic and Clinical Health Act (the "HITECH ACT" implemented significant changes with respect to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Subtitle D of the HITECH Act

1. extended the reach of HIPAA, the Privacy Rule and the Security Rule
2. imposed breach notification requirements on HIPAA covered entities and their business associates,
3. limited certain uses and disclosures of PHI,
4. increased individuals rights with respect to PHI and significantly,
5. increased enforcement of, and penalties for, violations of privacy and security of PHI.

A data breach is defined in the HITECH Act (43 USC 17932) as an unauthorized acquisition, access, or use of protected health information (PHI) that compromises the security or privacy of such information.

The HITECH Act requires the University to notify patients, including human subjects, whose "unsecured PHI" has been, or is reasonably believed to have been accessed, acquired, or disclosed as a result of a breach, if the breach poses a risk of significant harm as defined by the HITECH regulations.

The HITECH Act applies to breaches of both electronic data and data in paper form.

Unsecured electronic PHI is any PHI not secured by encryption processes that meet the National Institute of Standards and Technology (NIST) standards adopted by HHS, which enforces the HITECH Act. UVA offers encryption solutions to employees that meet these standards: see <https://security.virginia.edu/data-protection.>

## Timeline and Procedures for Reporting a Data Breach

**Important:**

- *A data breach of PHI must be reported as soon as possible and no later than 24 hours from the time the incident is identified.* If the data breach involves lost or stolen

electronic devices and media it must be reported to the UVa Police Department IMMEDIATELY.

- A data breach of even partially de-identified data that meets the criteria of a Limited Data Set should be reported.
- **There are potential criminal and civil penalties for the researcher and the institution for noncompliance with HITECH obligations.**

**Examples of a Data Breach That Must Be Reported:**

- Stolen or lost computer or other electronic device which contains identifiable patient/subject health information. A report must be made even if the data was encrypted.
- Identifiable patient/subject health information in paper or electronic form left unattended in a non-secure area for others to read. (e.g. lab results left in a restroom or cafeteria)
- Identifiable patient/subject health information faxed to incorrect number outside the study team.
- You become suspicious that your computer, which contains identifiable patient/subject health information may have been "hacked into".
  - The following situations may lead you to suspect your computer may have been "hacked into"
- Your computer or other electronic device becomes sluggish or noticeably slower doing routine work.
- You see a number of advertising pop-ups, or pop-up offers to fix or scan your

computer, or pop-up warnings that your computer is in trouble, etc.

- You suspect something is wrong with your computer but you're not quite sure what.
- You notice unusual activity, things you have never seen before, when you are using your computer.

### **Report to:**

1. the Corporate Compliance and Privacy Office, at 924-9741. The Corporate Compliance and Privacy Office will investigate to determine whether a notification of breach must be given to affected patients, the media and the Secretary of HHS, under the HITECH Act, and make any required notifications. See the Medical Center Policy # 0021 "Confidentiality of Patient Information" Section D8
2. ITC if the breach involves electronic data. Use the UVA [Information Security Incident Reporting procedure:](http://www.itc.virginia.edu/security/reporting.html)  
<http://www.itc.virginia.edu/security/reporting.html>
3. UVa Police Department if the data breach involves lost or stolen electronic devices and media. The data breach must be reported immediately

## Data Breach and Unanticipated Problem

**A data breach may also meet the criteria for an Unanticipated Problem if the Data Breach meets all 3 of the following criteria:**

- · Unexpected in terms of nature, severity or frequency given the research procedures that are described in the protocol –related documents AND the characteristics of the subject population being studied.

- · Related or possibly related to participation in the research. This means that there is a reasonable possibility that the incident, experience or outcome may have been caused by the procedures involved in the research study
- · The event, experience, issue, instance, problem or outcome suggests that the research places the subject or others at greater risk of harm than was previously known or recognized.

If the Data Breach meets the criteria of an Unanticipated Problem, the researcher must follow the IRB-HSR requirements for reporting and Unanticipated Problem **IN ADDITION TO** the UVa requirements for reporting a Data Breach.

**LINK: [PROCEDURES FOR REPORTING UNANTICIPATED PROBLEMS TO IRB-HSR](#)**

## **--Business Associates**

Business associates are:

- External individuals or entities that perform a service on your behalf and that create or have access to identifiable health information.
- Outside legal, actuarial, accounting, consulting, management, administrative, accreditation, data aggregation, and financial services that create or have access to such information.

Entities considered to be business associates include:

- Web-hosting/ data storage companies
- Third party billing company/consultant
- Third party hired to screen potential subjects

Entities not considered business associates include:

- Outside researchers
- Sponsors

A business associate is required to sign a HIPAA compliant Business Associate Agreement before any work may begin. Agreements with vendor business associates must be coordinated through University Procurement or Medical Center Materiel Management. Also, Business Associate Agreements may be obtained from the UVA General Counsel's office.

## --HIPAA Privacy Notice

HIPAA requires that all patients receive a Notice of Privacy Practices on their first contact with UVA after April 14, 2003. The Notice of Privacy Practices explains UVA's privacy practices regarding a patient's medical records. An acknowledgement of receipt of the UVA Notice must be obtained from all research subjects. If the subject is already a UVA patient, they may have already signed this form. You may check the A2K3 system to determine if they have signed it. If the person has not yet signed this form, the principal investigator is responsible for giving the subject the Notice and obtaining the subject's signature on the receipt acknowledgement form. If the person has a medical record #, the medical record # should be written on the Notice and the form should be faxed to Health Information Services at 924-1290. If you do not have access to A2K3, you will need to distribute the Notice of Privacy Practices and obtain the acknowledgement from all of your subjects. If the subject has a medical record number, the form should be sent to Health Information Services as previously described. If your subjects do not have medical record numbers, then the form should be kept with the consent form in your regulatory files. These must be kept for 6 years from the closure date of the protocol. PLEASE NOTE: The Notice of Privacy Practices is different from the IRB-HSR Consent Form and/or the stand-alone HIPAA authorization.





## --Recruitment of Research Subjects

HIPAA does not allow the disclosure of protected health information without a patient authorization (signed IRB-HSR consent form) or a waiver. Data may also be released as a Limited Data Set. If you will be disclosing\* protected health information from potential subjects who have not yet signed a consent form, it must be done under a waiver or as a Limited Data Set. Additional questions have been added to the IRB-HSR protocol template to provide the IRB-HSR the information needed to determine if the screening logs are de-identified or if they can be released under a waiver or a Limited Data Set. If the IRB-HSR determines the data can be released as a Limited Data Set, the sponsor will need to sign a Data Use Agreement. The Data Use Agreement will be incorporated into all future contracts with commercial sponsors. If the IRB-HSR determines the data is identifiable and grants a waiver, the principal investigator is responsible for tracking these releases. The principal investigator will be notified at the time of approval if tracking is required. The principal investigator will then need to follow the tracking instructions on the IRB-HSR WEB-site.

\*disclose- allowing a research sponsor's monitor to look at screening logs or sending screening



## --Consequences of Subject Revoking HIPAA Authorization for Release of Information

The IRB-HSR consent form template has the following statement under the Privacy of Records section.

"If you decide to withdraw your permission and end this agreement to release the information collected about you, please notify insert PI name in writing to insert address of PI. If you cancel your permission the investigator and his/her staff may continue to use or disclose your personal health information

obtained prior to your withdrawing your permission as necessary to maintain the accuracy of the study data. If you withdraw your permission and end this agreement you may no longer participate in this study."

HIPAA requires that the withdrawal of permission to release information be in writing. This does not apply to withdrawal from the protocol. Therefore, a written notice is NOT required from subjects in order to withdraw from the study, only to stop the release of information. The regulation allows for data gathered to the point of withdrawal of permission to continue to be used and disclosed as necessary to maintain the integrity of the research study. It would permit the continued use and disclosure of PHI to account for a subject's withdrawal from the research study, as necessary to incorporate the information as part of a FDA application, to conduct investigations of scientific misconduct, or to report adverse events.

## **INVESTIGATOR RESPONSIBILITIES**

If you are an investigator on a study you have the following responsibilities:

- Know the protocol and follow it. Before you begin work on the study, obtain a copy of the protocol and read it. If you have any questions contact the Principal Investigator or the IRB.
- Use only consent forms which have a current approval stamp on them.
- No health information with any HIPAA identifiers may be removed from the health system without the data being encrypted. For more information please see the UVa Policies listed under "Resources: in this presentation.
- Be aware of all requirements listed below in the Investigators Agreement.

## **THE INVESTIGATOR CONFIRMS:**

1. I am not currently debarred by the US FDA from involvement in clinical research studies.
2. I am not involved in any regulatory or misconduct litigation or investigation by the FDA.
3. That if this study involves any funding or resources from an outside source, or if the study team will be sharing data outside of UVA prior to publication that the Principal Investigator will contact the Dean's office regarding the need for a contract and letter of indemnification. If it is determined that either a contract or letter of indemnification is needed, subjects cannot be enrolled until these documents are complete.
4. The proposed research project will be conducted by the Principal Investigator or under his/her close supervision. It will be conducted in accordance with the protocol submitted to and approved by the IRB including any modifications, amendments or addendums submitted and approved by the IRB
5. That no personnel will be allowed to work on this protocol until they have completed the IRB-HSR On-line training and the IRB-HSR has been notified.
6. That all personnel working on this protocol will follow all IRB-HSR Policies and Procedures as stated on the IRB-HSR Website and on the School of Medicine Clinical Trials Office Website:
7. The Principal Investigator will ensure that all those delegated tasks relating to this study, whether explicitly or implicitly, are capable through expertise, training, experience and or credentialing to undertake those tasks.
8. The Principal Investigator confirms that the implications of the study have been discussed with all Departments that might be affected by it and have obtained their agreement for the study to take place.
9. That no subjects will be recruited or entered under the protocol until the Investigator has received the signed IRB-HSR Approval form stating the protocol is open to enrollment
10. That any materials used to recruit subjects will be approved by the IRB-HSR prior to use.



PROTOCOL

11. That all subjects will sign a copy of the most current consent form that has a non-expired IRB-HSR approval stamp.
12. That any modifications of the protocol or consent form will not be initiated without prior written approval from the IRB-HSR, except when necessary to eliminate immediate hazards to the subjects.
13. Any significant findings that become known in the course of the research that might affect the willingness of subjects to enroll or to continue to take part, will be promptly reported to the IRB.
14. The study team members will report immediately to the IRB any unanticipated problems involving risk to subjects or to others including adverse reactions to biologics, drugs or medical devices.
15. That any serious deviation from the protocol will be reported promptly to the Board in writing.
16. That any data breach will be reported to the IRB, the UVa Corporate Compliance and Privacy Office, and to UVa Police if applicable.
17. That the continuation status report for this protocol will be completed and returned within the time limit stated on the form.
18. That the IRB-HSR office will be notified within 30 days of a change in the Principal Investigator or of the closure of this study.
19. That a new PI will be assigned if the current PI will not be at UVA for an extended period of time.
20. Signed consent forms and other research records will be retained in a confidential manner. Records will be kept at least 6 years after completion of the study. These are considered institutional records and may not be transferred to another institution. A **copy** of the documents may be taken with the Principal investigator when transferring to another institution.

**This module has a quiz.**

[Return to Gradebook](#)

[Take the Quiz](#)

#### SUPPORT

888.529.5929

8:30 a.m. – 7:30 p.m. ET

Monday – Friday

[Contact Us](#)

#### LEGAL

[Accessibility](#)

[Copyright](#)

[Privacy and Cookie Policy](#)

[Statement of Security Practices](#)

[Terms of Service](#)

