ISU HIPAA Compliance Manual

ISU HIPAA Compliance Manual

Table of Contents

Introduction

In 1996, the United States Congress enacted the Health Insurance Portability and Accountability Act (HIPAA). HIPAA was designed to accomplish a number of objectives, one of which is to protect the privacy of individually identifiable health information. Protection standards exist for protected health information (PHI) in all forms, including electronic formats (ePHI).

The standards set forth by HIPAA apply to "covered entities," including health care providers and the agencies they work within. ISU Clinics are covered entities and thus required to comply with the regulations specified by HIPAA. This manual details the policies and procedures established for ISU Clinics to ensure HIPAA compliance.

Policies and Procedures

Administrative Safeguards. Administrative safeguards refer to the policies and procedures used by the ISU Clinics to comply with HIPAA standards.

Privacy Officer

The ISU Privacy Officer is the designated University person responsible for knowing HIPAA regulations, training the Clinic staff, student clinicians, and supervisors ("Clinic Personnel") in HIPAA compliance, and assuring that HIPAA-related policies and procedures are instituted and followed. To that end, the Privacy Officer will:

- Update HIPAA policies and procedures.
- Oversee the implementation of the policies and procedures contained in this Manual.
- Ensure that all Clinic personnel are trained regarding HIPAA and the policies and procedures of the Clinic.
- Review activity that takes place in the Clinic to detect security risks.
- Investigate and respond to security incidents and take appropriate action in the event of a breech in security, and eliminate or mitigate any damaging effects.
- Institute appropriate corrective measures to help ensure that similar violations do not occur in the future. Corrective measures may include personnel re-education, policy revision, building modification, and/or equipment alterations.
- Engage in a yearly assessment of the Clinic's adherence to the policies detailed in the manual. As part of the annual assessment, teams consisting of faculty and student clinicians are asked to search the Clinic for any potential security problems and to recommend additional security measures.
- Ensure that appropriate physical safeguards are in place to control physical access to protected information, including building access, mailbox access, clinic access, physical records, recordings, and document retention.
- Ensure technical safeguards are in place to control access to computer systems, workstations, and other means of communications containing PHI transmitted electronically from being intercepted by anyone other than the intended recipient.

HIPAA Training Program

All Clinic personnel are required to participate in a formal HIPAA training program. The training program can be instituted and conducted by the Clinic and with assistance provided by the Privacy Officer as needed, and all existing personnel are required to complete the training and conduct an annual review. All incoming clinical students and any new clinical faculty should receive the training within 60 days of their arrival to ISU.

The training may involve watching a HIPAA Training for Covered Entities tutorial, and then taking the HIPAA Training Quiz. Successful completion of the training and quiz is required in order to work in the Clinic. The Clinic Director/Security Officer reviews with each quiz-taker

any content associated with a failed item on the quiz. Anyone receiving a grade less than 85% on the quiz must repeat the training.

Additionally, this Manual may be given to all Clinic personnel. It is also available online and in hard-copy in the Clinic library.

Documentation of Training

Training of Clinic personnel is to be recorded in a HIPAA Training Log.

HIPAA Privacy Notice

All clients who receive services in a Clinic should be offered a HIPAA Privacy Notice. (see Appendix A). They sign another document indicating that they received the Notification. Additionally, the HIPAA Privacy Notice should be visible and available in the Clinic waiting room.

Release of Information

Client PHI is typically released to another party only when the release is requested, in writing, by the client or client's legal guardian. The "Authorization for Use or Release of Health Information" form is completed when a request is made (see Appendix B).

PHI may at times be release without client authorization, but only in accordance with strict policies (see HIPAA Notification for *Uses and Disclosures with Neither Consent nor Authorization* in Appendix A*).*

Ensuring that Disclosures are the Minimum Necessary

When a request is received to disclose PHI, the request should be reviewed by a case supervisor and the Clinic Director. Only the minimum necessary amount of information will be disclosed. The principle guiding the release of PHI is to limit disclosure of information that is not reasonably necessary to accomplish the purpose for which the request is made.

Accounting for Disclosures

The Clinic staff complete an Accounting for Disclosures form whenever a release of information is requested by a client (see Appendix C). In keeping with HIPAA Privacy Rules, the form specifies who has received access to the client's PHI and ePHI. Yearly requests for accounting of disclosures will be provided free of charge, and given within 60 days of a request for the information.

Requests for File Review and Copy

Clients who have records in the Clinic may request to inspect and obtain a copy of their PHI in the "designated record set," defined as the medical and billing records maintained by the Clinic

and used to make decisions about the client. The request must be made in writing, and will be fulfilled within 30 days of receipt.

Requests to Amend a Record

Clients have the right to amend their record if they believe the record is incomplete or not accurate. The amendment will become part of their ongoing file. Requests for record amendments must be made in writing. Clients may not expunge any prior information or part of the Record.

Policies and Procedures to Access Protected Health Information

Access to PHI is limited to Clinic personnel and business associates (see below), and further restricted by virtue of what information is needed by personnel to complete a job function and/or clinical training.

Security Assessment

The Privacy Officer will engage in a yearly assessment of the Clinic's adherence to the policies detailed in this manual. As part of the annual assessment, teams consisting of faculty and student clinicians are asked to search the Clinic for any potential security problems and to recommend additional security measures.

Reporting of Security Violations

Clinic personnel are required to report any violations of HIPAA standards to the Privacy Officer.

Responding to Violations and Preventing Further Violations

When security incidents or deficiencies are reported or discovered, the Privacy Officer investigates the situation. He/she then institutes appropriate corrective measures to help ensure that similar violations do not occur in the future. Corrective measures may include personnel re-education, policy revision, building modification, and/or equipment alterations.

Responding to a Breach of Protected Health Information

A breach is defined as the acquisition, access, use or disclosure of PHI in violation of the HIPAA Privacy Rule. Examples of a breach include stolen or improperly accessed PHI; PHI inadvertently sent to the wrong provider; the unauthorized viewing of PHI, and the like. A use or disclosure of PHI that violates the Privacy Rule is presumed to be a breach unless the Privacy Officer conducts a risk assessment and determines that there is a low probability that PHI has been compromised. In the event that the risk assessment indicates that there has been a breach, breach notification procedures will be followed.

Breach Notification Procedures

The HIPAA Breach Notification Rule requires covered entities to notify affected individuals of unsecured PHI. Most notifications must be provided without unreasonable delay and no later than 60 days following the discovery of a breach. The Privacy Officer shall be responsible for providing affected individuals with the appropriate notice.

Research Activities

Client information may not be used for research purposes unless the client has agreed to allow his/her PHI to be used in this manner.

Clinic Visitors

In general, having visitors in the Clinic is discouraged. However, visiting is permitted on a brief and limited basis if the visitor is escorted by Clinic personnel who take care to ensure that PHI is not visible.

Building Access

Access to the Clinic should be limited to Clinic personnel who are given keys coded for full or limited access depending on job duties and need for access. Keys are dispersed by the Clinic Director who maintains a record of key distribution. Keys are returned to the Clinic Director upon termination from

Appendices

A: Notice of Privacy Practices

B: Consent for Release or Exchange of Information

C: Accounting for Disclosures Form

D: Security Incident Report

E: HIPAA Consent to Participate in Research

Appendix A

INDIANA STATE UNIVERSITY NOTICE OF PRIVACY PRACTICES

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW THIS NOTICE CAREFULLY.

Effective July 5, 2018

I. Purpose of this Notice

Indiana State University (ISU) is committed to protecting the privacy of individual health information in compliance with the Health Insurance Portability and Accountability Act (HIPAA) of 1996. This Notice of Privacy Practices ("Notice") describes the privacy practices of ISU related to treatment, payment or other health care operations including but not limited to clinical affiliated services such as massage, speech, occupational, and physical therapy, student counseling, psychology, athletic training, sports rehab, nursing, and other clinical affiliated services. Federal law requires ISU to make sure that any medical information that it collects, creates or holds on behalf of its health care providers that identifies you remains private. This Notice describes how ISU may use or disclose your medical information, your rights concerning your medical information, and how you may contact ISU regarding privacy policies. This Notice applies to any use or disclosure of your medical information occurring on or after the effective date written at the top of this page, even if ISU created or received the information before the effective date.

II. How ISU May Use or Disclose Your Medical Information

ISU understands that medical information about you and your health is personal. ISU restricts access to your personal information to only those persons with a need to know. ISU maintains physical, electronic, and procedural safeguards that meet state and federal regulations to guard your personal information. ISU may use or disclose your medical information only as described in this section.

a. **Treatment.** Your medical information may be disclosed to a health care provider for your medical treatment.

b. **Payment.** ISU may disclose your medical information so that ISU can bill for the services you received and collect payment. For example: ISU may share information with your insurance company to obtain prior approval for treatment when applicable, or to bill and receive payment for treatment you received. ISU may also share your information with other affiliated or contracted entities who performed a service during your visit to our facility (example, other physicians, technicians, labs, etc).

c. **Health Care Operations**. ISU may use and disclose your medical information as necessary for internal operations. Examples of such uses and disclosures include, but are

not limited to: appointment reminders; to inform you about treatment alternatives or other health related services that may interest you; to review our services, evaluate our performance, and decide what additional services to offer; for research purposes under certain circumstances, to doctors, nurses, and other personnel for review and learning purposes.

d. Required by Law. ISU will use or disclose your medical information if a federal, state, or local law requires it to do so.

e. Disclosure to you. ISU may disclose your medical information to you or to a third party to whom you request us in writing to disclose your medical information.

f. Disclosures to Individuals involved with Your Health Care. ISU may use or disclose your medical information in order to tell someone responsible for your care about your location or condition. ISU may disclose your medical information to your relative, friend, or other person you identify, if the information relates to that person's involvement with your health care or payment for your health care.

g. Serious Threat to Health or Safety. ISU may use or disclose your medical information if necessary because of a serious threat to someone's health or safety.

h. Incidental Uses and Disclosure. Uses and disclosures that occur incidentally with a use or disclosure described in this section are acceptable if they occur notwithstanding ISU's reasonable safeguards to limit such incidental uses and disclosures.

i. Written Authorization. ISU may use or disclose your medical information under circumstances that are not described above only if you provide permission by "written authorization." If you provide ISU permission to use or disclose your medical information, you may still revoke that permission, in writing, at any time. If you revoke your permission, ISU will no longer use or disclose medical information about you for the reasons covered by your written authorization. However, ISU cannot take back any disclosure already made under that authorization.

III. Restrictions

a. ISU will not use your medical information for fundraising or marketing purposes.

b. ISU will never use your genetic medical information for underwriting purposes.

c. ISU does not sell your medial information.

IV. Your Rights Concerning Your Medical Information

a. Right to Request Restrictions. You have the right to request a restriction or limitation of the medical information ISU uses or discloses about you for treatment, payment or other health care operations. You also have the right to request a limit on the medical

information ISU discloses about you to someone who is involved in your care or the payment for your care, such as a family member or friend. You must make your request in writing to the ISU Privacy Officer at HIPAAPrivacyOfficer@indstate.edu. Your request must state (1) the information you want to limit, (2) to whom you want the limit to apply, (3) the special circumstances that support your request for a restriction on medical disclosures, and (4) if your request would impact payment, how payment will be handled. ISU will consider your request, but is not required to agree to it. If we do agree, ISU will comply with the request unless the information is needed to provide you emergency treatment.

b. **Right to Confidential Communications.** You have the right to request that ISU communicate your medical information to you by a certain method (for example, by email) or at a certain location (for example, only at work). You must make your make your request in writing to the ISU Privacy Officer at the email address listed above or at the time of registration.

c. **Right to Inspect and Copy.** You have the right, in most cases, to inspect and copy and/or request copies of your records. This includes medical and billing records, but does not include physician notes. If you request a copy of the records, ISU may charge a reasonable fee for the costs of copying, mailing, or other supplies associated with your request. You must make your request in writing to the ISU Privacy Officer at the email address listed above.

d. **Right to Amend.** If you feel that the medical information in your records is incorrect or incomplete, you may ask us to amend that information. You have a right to request an amendment for as long as the information is kept. You must make your request in writing to the ISU Privacy Officer at the email address listed above, and you must give a reason that supports your request. However, we may deny your request if it is deemed that our information is accurate and complete.

e. **Right to Accounting of Disclosures.** You have the right to request a list of disclosures of your medical information that have been made by ISU. You must make your request in writing to the ISU Privacy Officer at the email address listed above. Your request must state the time period during which the disclosures were made, which may not include dates more than six years prior to the request. ISU may charge you a fee for the list of disclosures if you request more than one list within 12 months. ISU does not have to list the following disclosures: disclosures for treatment; disclosures for payment; disclosures for health care operations; disclosures of a limited data set for health care operations; disclosures to you; disclosures to individuals involved with your health care; disclosures to federal officials; disclosures made with your written authorization; disclosures that occur incidentally with other permissible uses and disclosures; and in certain circumstances, disclosures to law enforcement officials or health oversight agencies.

f. **Right to Make a Complaint.** If you believe your privacy rights have been violated, you may file a written complaint to ISU's Privacy Officer or with the federal government's

Department of Health and Human Services. ISU will not penalize you or retaliate against you in any way if you file a complaint.

g. **Right to a Paper Copy of This Notice.** You have a right to request a paper copy of this Notice, even if you have received this Notice electronically. You may make your request to the ISU Privacy Officer at the email address listed above.

V. For More Information or to Report a Problem

If you have questions or would like additional information about our privacy practices or this Notice, you may contact our Privacy Officer during normal business hours at:

To file a written complaint with the federal government, please use the following contact information:

Office for Civil Rights
U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Room 509F, HHH Building
Washington, D.C. 20201

Toll-Free Phone: 1-(877) 696-6775

Website: http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html

Email: OCRComplaint@hhs.gov

VI. Changes to this Notice

ISU reserves the right to change the terms of this Notice at any time. ISU also reserves the right to make the revised notice effective for medical information ISU already has about you. Within 60 days of a material revision of this Notice, ISU will post a copy of this revised notice on its Human Resources or applicable Clinic websites.

Appendix B

Indiana State University

CONSENT FOR RELEASE OR EXCHANGE OF INFORMATION

By completing and signing this form you authorize us to release protected information from your clinical record to the facility/person you designate, and/or authorize the release of your health records from other facilities to the ISU _____ Clinic.

_____	_____
Name of Client	Organization / Person to Receive Information
_____	_____
Street Address	Street Address
_____	_____
City/State/Zip Code	City/State/Zip Code

_____
Date of Birth

I authorize and consent to the release of the following information.

_____ Intake Report	_____ Evaluation Report
_____ Summary of Treatment Report	_____ Treatment Plan
_____ Other, as specified below	_____ Verbal communication

_____

The information is being released for the purpose of:

_____ Coordination of care
_____ Attorney request
_____ Other, as specified here_____

This consent may be revoked by me in writing at any time, and will expire in 60 days *or* as specified below

_____

I understand that information to be released may include information regarding drug or alcohol abuse, psychological or psychiatric impairments, confidential communications, HIV and/or AIDS, physical conditions or other information which may be privileged or confidential under State and/or Federal law. I also understand that the information disclosed may be subject to redisclosure by the recipient of the information and may no longer be protected by the HIPAA Privacy Rule.

_____ (Client initials)

_____
Signature of Patient Date

_____
Signature of Parent/Guardian (if patient is a minor) Date

Please return requested information to:

_____
(Name of ISU Clinic Clinician)

[INSERT NAME OF CLINIC AND ADDRESS]

Appendix C

Indiana State University Clinic
Accounting for Disclosures
Form

_____There were no applicable disclosures made of your protected health information for the period your specified.

_____Disclosures of your protected health information were made by this office to:

Date of Disclosure	Name of Whom Information was Disclosed	Address	Description of Information Disclosed	Purpose of Information Disclosed

We are temporarily unable to process the accounting for disclosures you have requested due to:

_____A suspension required by law.

_____Other, specify: _____

However, your request will be provided by _____
(Month/Day/ Year)

If you have any questions concerning this accounting for disclosures, please contact:

_____ at : _____
(Signature of Medical Professional or Staff Member) (Telephone number)

_____ _____
Printed Name Date

Appendix D

ISU Clinic
Security Incident Report

Date: _____

Description of Security Incident:

_____
_____
_____
_____
_____
_____
_____

Measures Taken to Resolve the Problem or Mitigate Effects:

_____
_____
_____
_____
_____
_____
_____

Steps Taken to Prevent Recurrence:

_____
_____
_____
_____
_____
_____
_____

_____
Privacy Officer

_____
Signature of Privacy Officer

E: HIPAA Consent to Participate in Research

Indiana State University
Clinic HIPAA Consent to Participate in Research

1. **Purpose.** As a research participant, I authorize (faculty name) and the researcher's staff to use and disclose my (and my child's) individual health information for the purpose of conducting the research project entitled (enter title of the study).

2. **Individual Health Information to be Used or Disclosed.** Individual health information from my (my child's) evaluation that may be used or disclosed to conduct this research includes: (list all components of the evaluation).

3. **Parties Who May Disclose My Child's and My Individual Health Information.** The researcher and the researcher's staff may obtain my (my child's) from:

4. **Parties Who May Receive or Use My Individual Health Information.** The individual health information disclosed by parties listed in item 3 and information disclosed by me during the course of the research may be received and used by (list all researchers and assistants).

5. **Right to Refuse to Sign this Authorization.** I do not have to sign this Authorization. If I decide not to sign the Authorization, I may not be allowed to participate in this study or receive any research related treatment that is provided through the study. However, my decision not to sign this authorization will not affect any other treatment, payment, or enrollment in health plans or eligibility for benefits.

6. **Right to Revoke.** I can change my mind and withdraw this authorization at any time by sending a written notice to (researcher's name) to inform the researcher of my decision. If I withdraw this authorization, the researcher may only use and disclose the protected health information already collected for this research study. No further health information about me (or my child) will be collected by or disclosed to the researcher for this study.

7. **Potential for Re-disclosure.** My individual health information (and that of my child) disclosed under this authorization may be subject to re-disclosure outside the research study and no longer protected. For example, researchers in other studies could use my and my child's individual health information collected for this study without contacting me if they get approval from an Institutional Review Board (IRB) and agree to keep the information confidential.

   Also, there are other laws that may require my (or my child's) individual health information to be disclosed for public purposes. Examples include potential disclosures if required for mandated reporting of abuse or neglect, judicial proceedings, health

oversight activities and public health measures.

This authorization does not have an expiration date.

I am the research participant or personal representative authorized to act on behalf of the participant.

I have read this information, and I will receive a copy of this authorization form after it is signed.

Signature of research participant or research participant's personal representative	Date
Printed name of research participant or research participant's personal representative	Date

Description of personal representative authority to act behalf of the research participant: