HIPAA Sanctions Guidance

HIPAA Guidance - 01

About This Guidance

Effective: 08/01/2013
Last Updated: 04/02/2025

Responsible University Office:
Office of the Chief Privacy Officer

Responsible University Administrator:
Chief Privacy Officer
mawerlin@iu.edu

Guidance Contact:
HIPAA Privacy Officer HIPAA
Security Officer
hipaa@iu.edu

Scope

This guidance applies to the workforce members in the designated Indiana University (IU) HIPAA Covered Healthcare Components and Critical Health Data Areas, anyone rendering services as a Business Associate, and anyone who creates, receives, maintains, or transmits Protected Health Information (PHI) in any capacity at IU, including, but not limited to, faculty, staff, students, trainees, volunteers, visiting scholars, and third-party agents. For the purposes of this policy, all of the above will be referred to as workforce members.

This guidance addresses the sanctions that may be applied when protected health information (PHI) is used and disclosure in a manner that contradicts university policy, HIPAA or Indiana State Law.

Guidance Statement

A. Parties Responsible for Imposing Sanctions. Supervisor, Managers, Directors, Human Resource personnel in IU Critical Health Data Areas

B. Persons Who May Be Subject to Sanctions. Members of the workforce of IU Critical Health Data Areas, including employees, volunteers, trainees, and other persons whose conduct, in the performance of their work, is under the direct control of the IU Critical Health Data Area, whether or not they are paid by IU, may be subject to corrective action under this Guidance. Independent contractors are considered IU's business associates, not members of IU's workforce, and are not subject to discipline under this Guidance.

C. Violations That Will Prompt Consideration of Sanctions. Persons may be subject to sanctions, up to and including discharge and/or restitution, for violations of either;

1. The Privacy or Security Standards; or
2. These Policies and Procedures relating to the confidentiality of health care information.

Managers or supervisors may also be subject to corrective action, up to and including discharge or restitution, if their lack of diligence or lack of supervision contributes to a subordinate's privacy or security violation.

D. Exceptions. A person shall not be subject to corrective action as a result of performing one or more of the following:

1. Filing a complaint with the Secretary for a suspected violation of the Privacy Standards;
2. Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing in connection with the Administrative Simplification provisions of HIPAA;
3. Opposing any act or practice made unlawful by the Privacy Standards, provided that:
   a. the person has a good faith belief that the practice opposed is unlawful; and
   b. the manner of the opposition is reasonable and does not involve a disclosure of PHI in violation of the Privacy Standards
4. Disclosing PHI if:
   a. the person believes in good faith either that IU has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by IU potentially endanger one or more patients, workers, or the public; and
   b. the disclosure is either to a health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of IU, to an attorney retained by or on behalf of the person for the purpose of determining the person's legal options with regard to the relevant conduct, or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct; or
5. Disclosing PHI to a law enforcement officer if:
   a. the person is the victim of a criminal act that occurred on or off the premises,
   b. the PHI relates to the suspected perpetrator of the criminal act, and
   c. no PHI other than the following is disclosed: current location, name, address, date of birth, place of birth, social security number, ABO blood type, RH factor, type of injury (if applicable), date and time of treatment (if applicable), date and time of death (if applicable), and a description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars, and tattoos.

E. Imposition of Sanctions. Any corrective action imposed should be appropriate to the nature of the violation that prompted the corrective action. Determination of the proper level of corrective action requires that the facts and circumstances surrounding the violation be considered. After considering the relevant facts and circumstances of a privacy or security violation, IU shall impose corrective action that it deems appropriate, in its sole discretion, to the nature of the violation that prompted the corrective action. Corrective action may include, but is not limited to, written warning, suspension, and/or termination.

F. Enforcement of Sanctions. IU shall ensure that the imposed corrective action is adequately communicated to the violator and enforced. In the event that the corrective action triggers any rights of appeal (for instance, under a management/union agreement), all such rights of appeal shall be available to the violator. However, in the event that the party hearing the appeal is not a party authorized in paragraph 1 of this Guidance to impose corrective action, the identity of the individual whose privacy rights were violated shall be removed to the extent feasible.

G. Documentation of Sanctions. IU shall document the corrective action, including:

- the privacy violation;
- the parties that determined the action;
- the facts and circumstances considered in determining the action (without regard to whether such considerations were relied upon in determining the corrective action);
- the corrective action imposed (including lack of corrective action); • the appeals process used, if any, and the results thereof; and
- the actions taken in order to enforce the corrective action.

IU shall maintain the documentation described in the above paragraph for a period of at least 6 years from the date it was created.

IU may use or disclose its documentation containing the identity of the individual whose privacy rights were violated only under the following circumstances:

- if required by law or by court order;
- in accordance with the individual's authorization;
- in determining corrective actions for subsequent violations; or
- to investigate or determine compliance with this Guidance and/or the Privacy Standards (whether such investigation originates internally or by request of the individual or the Secretary).

Under any other circumstances, such documentation must be de-identified (as to the individual whose privacy rights were violated) prior to any use or disclosure. For example, documentation of corrective actions, if de-identified, may be stored in the violator's personnel file. In addition, where feasible, the violator's identity should be removed prior to any use or disclosure, for example if the documentation is to be used by those responsible for privacy training.

H. Categories of Violations

Category 1 – Unintentional breach of privacy or security which may be caused by carelessness, lack of knowledge, or lack of judgment. Examples include, but are not limited to:

- Registration errors causing billing to be sent to the wrong person
- Mistakenly sending e-mails or faxes containing PHI to the wrong recipient
- Discussing PHI in public areas
- Leaving a computer accessible and unattended with unsecured PHI
- Loss of an unencrypted electronic device containing unsecured PHI
- Improperly disposing of PHI in violation to policy
- Failure to report his/her password has potentially been compromised

Category 2a – Deliberate unauthorized access to PHI without PHI disclosure, such as accessing confidential information of any patient out of curiosity and failure to follow policy without legitimate reason, such as password sharing. Examples include but are not limited to:

- Intentional, unauthorized access to your own, friends, relatives, co-workers, public personalities, or other individual’s PHI (including searching for an address or phone number)
- Fails to properly verify the identity of individuals requesting PHI which results in inappropriate disclosure, access or use of PHI
- Logs into the network resources (including EMRs) and allows another individual to access PHI
- Connects devices to the network and/or uploads software without having received authority
- Second occurrence of any Category 1 violation (it does not have to be the same offense)

Category 2b – Deliberate unauthorized disclosure of PHI or deliberate tampering with data without malice or personal gain. Such as accessing information out of curiosity and then re-disclosure to the news media or unauthorized modification of an electronic document to expedite a process. Examples include but are not limited to:

- Intentional, unauthorized access to friends, relatives, co-workers, public personalities, or other individuals PHI and then sharing with news media or on social media
- Intentionally assisting another individual to gain unauthorized access to PHI. This includes, but is not limited to, giving another individual your unique username and password to access electronic PHI
- Changing or tampering with documents for the sole purpose of passing a system edit
- Second occurrence of any Category 2a violation (it does not have to be the same offense)

Category 3 – Deliberate unauthorized disclosure of PHI for malice or personal gain. Selling information to tabloids or stealing individually identifiable health information to open credit card accounts. Examples include but are not limited to:

- Unauthorized intentional disclosure and/or delivery of PHI to anyone for financial gain
- Intentionally assisting another individual to gain unauthorized access to PHI for financial gain
- Unauthorized intentional disclosure and/or delivery of PHI to anyone to cause financial and/or reputational harm or embarrassment to the individual

I. Examples of Possible Sanctions

Category 1: Violations may result in documented performance counseling, corrective action plan and/or a written warning by the first line supervisor in accordance with IU's Corrective Action Policy.

Category 2a: Violations may result in first line supervisor and next immediate manager work with the Department of Human Resources to initiate a written warning, corrective action plan and possible suspension or termination in accordance with IU's Corrective Action Policy.

Category 2b: Violations may result in most senior staff member directly responsible for operations works with the Department of Human Resources to initiate a formal corrective action up to and including dismissal in accordance with IU's Corrective Action Policy.

Category 3: Violations may result in most senior staff member responsible for overall operations works with the Department of Human Resources to initiate immediate suspension pending dismissal in accordance with IU's Corrective Action Policy. Notify IU General Counsel's Office for guidance related to notification of Law Enforcement and/or the Indiana Attorney General's Office.

Reason for the Guidance

Indiana University (IU) will apply appropriate sanctions against members of its workforce who fail to comply with IU's Policies and Procedures concerning the protection of PHI, according to the United States Department of Health and Human Services (DHHS) HIPAA and HITECH privacy and security regulations, in conjunction with existing state laws, federal laws, and Indiana University Policy covering human subjects, security and privacy.

Definitions

See Glossary of HIPAA Related Terms for complete list of terms.

History

07/11/2013 – Draft reviewed by Council
07/22/2013 – Draft reviewed by HR
08/08/2013 – Final approved by HIPAA Privacy and Security Council
01/12/2016 – Updated definition section
08/01/2016 – Added link to Glossary
12/13/2021 – Updated contacts
04/02/2025 – Updated the term "HIPAA Affected Areas" to "Critical Health Data Areas"

Related Information

HIPAA-P01 Uses & Disclosures of Protected Health Information Policy
HIPAA-P02 Minimum Necessary Policy