Indiana Department of Health

Policies and **Procedures**

Title: HIPAA Consolidated Policies and Procedures	**Policy #**: IDOH-COS-OLA-HIPAA-01
Scope: ☒ All Staff ☐ Limited Staff: Scope of application if limited staff	**Approvals**: Lindsay Weaver, MD, FACEP March 12, 2026
Effective dates: 01-Jan-26 to 31-Dec-28	

Purpose

To establish a unified, consistent, and comprehensive approach to complying with (1) the Health Insurance Portability and Accountability Act (HIPAA); and (2) establishing policies and procedures with respect to Protected Health Information that address each applicable standard in the Privacy Rule.

Definitions

The definitions below apply to all of the policies and procedures contained herein.

Agency: The Indiana Department of Health (IDOH).

Agency Leadership: State Health Commissioner, Deputy State Health Commissioner, and his/her direct reports, Chief of Staff and his/her direct reports, and Assistant Health Commissioners.

Agency Management: Staff so designated by Agency Leadership as Directors, Managers, and Supervisors.

Business Associate: A person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information.

Covered Entity: Means a health plan, a health care clearinghouse, or a health care provider who transmits health information in electronic form in connection with a transaction for which the U.S. Dept. of Health and Human Services has adopted a standard. 45 C.F.R. § 160.103.

Designated Record Set: A group of records maintained by or for a covered entity that is:

1) the medical and billing records about individuals maintained by or for a covered health care provider;
2) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
3) used in whole or in part by or for the covered entity to make decisions about individuals.

HIPAA: The federal Health Insurance Portability and Accountability Act of 1996.

HIPAA Covered Component: A component or combination of components designated by IDOH, a Hybrid Entity. The designated Covered Components are listed under the "Procedures & Responsibilities" section. Each is an IDOH program engaging in activity subject to the HIPAA Privacy Rule and may be referred to as an IDOH Covered Component.

HIPAA Privacy Rule: Standards for Privacy of Individually Identifiable Health Information 45 CFR Part 160 and Subparts A and E of Part 164.

HIPAA Consolidated Policies and Procedures: Also known as the HIPAA policies, these Policies and Procedures are incorporated herein and listed hereunder as required under 45 C.F.R. § 164.530(i).

Hybrid Entity: Means a single legal entity that is a covered entity, performs business activities that include both covered and non-covered functions, and designates its health care components as provided in the Privacy Rule. 45 C.F.R. § 164.103.

Individually Identifiable Health Information: Health information which includes demographic information that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual and that identifies the individual or there is a reasonable basis to believe the information can be used to identify the individual.

Memorandum of Understanding (MOU): A signed document that details the intended use and disposition of data provided by an IDOH program.

Privacy Officer: A person designated by a covered entity who is responsible for the development and implementation of the policies and procedures of the entity. 45 C.F.R. § 164.530(a)(1).

Protected Health Information (PHI): Individually identifiable health information transmitted or maintained in any form or medium (electronic media (ePHI), print, or oral recordings). 45 C.F.R. § 160.103.

Security Officer: A security official who is assigned by the covered entity to be responsible for the development and implementation of the policies and procedures required by the HIPAA Security Standards for the Protection of Electronic Protected Health Information, 45 C.F.R. Part 164, Subpart C, for the covered entity. 45 C.F.R. § 164.308(a)(2)

Workforce: People, including employees, volunteers, trainees, Agency Leadership, Agency Management, and any other person whose conduct, in the performance of work for the IDOH or an IDOH Covered Component, is under the direct control of the IDOH or the IDOH Covered Component, whether or not they are paid for that work.

Policy Statement

The IDOH workforce shares the responsibility for complying with all HIPAA regulations governing our duties and responsibilities, including safeguarding PHI. By manifesting the Agency's mission to promote, protect, and improve the health and safety of all Hoosiers while adhering to its statutory directives, IDOH engages in certain activities that require it to access, receive, maintain, transmit, or use PHI and which trigger compliance with the provisions applicable to Covered Entities under HIPAA.

It is the policy of IDOH that the entire workforce adheres to this Policy and the HIPAA Policies incorporated below. The processes outlined herein guide the workforce and IDOH's designated Covered Components and apply to PHI created, acquired, or maintained by IDOH's designated Covered Components after April 14, 2003. IDOH has designated both a Privacy Officer and a Security Officer to create, implement, and train IDOH's workforce on these HIPAA Policies and Procedures and to review and update the Policies as necessary.

Procedures and Responsibilities

These specific HIPAA Policies, incorporated herein, have been created in compliance with 45 C.F.R. § 164.530(i) and set forth the framework for IDOH's compliance with HIPAA and 45 C.F.R. § 164, Subpart D and E.

IDOH is a Hybrid Entity as defined in 45 C.F.R. § 164.103 and includes both covered and non-covered components. IDOH's designated Covered Components include:

- Breast and Cervical Cancer Program
- Children's Special Health Care Needs
- Hemophilia Medical Services Program
- HIV Medical Services Program
- HIV Pre-Exposure Prophylaxis (PrEP) Medication Assistance Program (MAP)
- IDOH Labs
- Lead & Healthy Homes Program
- Mobile Response Operations
- Public Health Genetics (Genomic Newborn Screening (GNBS) and Early Hearing Detection and Intervention (EHDI))
- WiseWoman Program

A Covered Entity must implement policies and procedures with respect to PHI that address each applicable standard in the HIPAA Privacy Rule. Per 45 C.F.R. § 164.530(i), whenever there is a change in law that necessitates a change to the Covered Entity's policies or procedures, the Covered Entity must promptly document and implement the revised policy or procedure.

The IDOH HIPAA Policies are subject to change and will be revised in accordance with statutory and regulatory requirements. The IDOH HIPAA Policies are organized by the following topics.

Legal Authorities and References

- Laws
  - The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191

    - The Health Information Technology for Economic and Clinical Health (HITECH) Act, Public Law 111-5
- Regulations
    - HIPAA Privacy Rule, 45 C.F.R. Part 160 and Subparts A and E of Part 164
    - HIPAA Security Rule, 45 C.F.R. Part 160 and Subparts A and C of Part 164
    - HIPAA Administrative Simplification, 45 C.F.R. Parts 160, 162, and 164
- PHAB Standards
- Related Policies
    - IDOH Policy Management
    - IDOH Incident Response Policy

A. PHI Policies

The PHI Policy covers the following topics:

- Access Request for PHI Policy
- Accounting of Disclosures of PHI Policy
- Authorized Uses and Disclosures of PHI Policy
- Minimum Necessary Policy
- Permitted Uses and Disclosures of PHI Policy
- Personal Representatives and Rights of Minors Policy
- PHI Safeguards Policy
- Privacy of PHI Policy
- Removal of PHI from IN State premises Policy
- Required Uses and Disclosures of PHI Policy
- Request for Amendment of PHI Policy

Access Request for PHI Policy

Purpose

To ensure individual requests for access to PHI are reviewed and answered in a consistent and efficient manner.

Policy Statement

IDOH will allow an individual to inspect and to obtain a copy of his or her PHI for as long as we, or our business associates, maintain that PHI in designated record sets. IDOH will act on all access requests within 30 days unless the agency extends the time limit by an additional 30 days by notifying the individual in writing. IDOH may withhold from an individual only that PHI as specified in 45 CFR § 164.524.

Procedures and Responsibilities

Individuals will submit their requests for access to PHI in writing to the Privacy Officer. Any member of the IDOH workforce who receives a request for access to PHI from an individual should forward the request to the Privacy Officer. The Privacy Officer will determine the validity of the request and coordinate the efforts to be made by HIPAA-covered programs to fulfill the request. There are forms for submitting these requests, one form is for the Genomics Newborn Screening Program for newborn screening results, and the other form is for the other HIPAA-covered programs.

Failure to comply with requirements of this policy may subject an employee to discipline, per the HIPAA Sanctions Policy.

Legal Authorities and References

- Laws
  - IC 5-14-3 – Access to Public Records
- Regulations
  - 31 IAC 5-12 – Disciplinary Actions and Separations
  - 45 CFR 164.501 - Definitions
  - 45 CFR 164.524 – Access of Individuals to Protected Health Information
- PHAB Standards
- Related Policies
  - HIPAA Sanctions Policy, included herein

Forms

Health Information Access Request form
Genomics and Newborn Screening Access Request form

Accounting of disclosures of PHI Policy

Purpose

To ensure appropriate responses are provided to requests for accounting of disclosures of PHI.

Policy Statement

An individual may request an accounting of the disclosures of his or her PHI made by IDOH covered components or their business associates. IDOH covered components are required to account for their disclosures of PHI for up to a maximum of six years prior to the date of the request.

IDOH covered components are not required to account for disclosures that are exempt from accounting as specified below:

- Disclosures made for treatment, payment, or health care operations.
- Disclosures made to the individual or the individual's personal representative.
- Disclosures made for notification of or to persons involved in an individual's health care or payment for health care, for disaster relief, or for facility directories.
- Disclosures pursuant to an authorization.
- Disclosures made in a limited data set.

- Disclosures made for national security or intelligence purposes.
- Disclosures made to correctional institutions or law enforcement officials regarding inmates or individuals in lawful custody.
- Disclosures made incident to, or as a byproduct of, otherwise permitted or required uses or disclosures.

Accounting for disclosures to health oversight agencies and law enforcement officials may be temporarily suspended on their written representation that an accounting would likely impede their activities.

The IDOH will provide one free disclosure accounting per participant each twelve (12) months. The IDOH may charge the participant for each additional disclosure accounting during the same 12-month period.

For each accounting of disclosures, the IDOH will retain the following documentation six years from the date of creation or the date when it was last in effect, whichever is later:

- The information required to be included in an accounting under 45 CFR § 164.528(b).
- The written accounting that is provided to the individual.
- The titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.

Procedures and Responsibilities

Disclosure Tracking: IDOH covered components will track, and require their business associates to track, disclosures of PHI subject to accounting obligations. IDOH covered components will make the tracking information available as needed for the IDOH to fulfill its obligations to respond to requests for disclosure accountings. IDOH covered components will retain the required documentation according to the documentation requirements described above in this policy.

Disclosure Accounting Request Process: Individuals will submit requests for accounting of disclosures of PHI to the Privacy Officer, in writing. All requests must include information sufficient to identify the requestor's records and the IDOH covered component(s) involved, as well as the time period for the accounting of disclosures. If the request is complete and deemed valid, the Privacy Officer will submit a direction to account for disclosures, in writing, to the appropriate Program Privacy Coordinator for preparation of the requested accounting of

disclosures. The Privacy Officer and Program Privacy Coordinator will coordinate all requests for accounting of disclosures that involve business associates.

Timeframe: The IDOH will provide a written response to the requester no later than 60 days after receipt of a complete request. If the requested accounting cannot be completed or denied within the 60-day time period, one 30-day extension period can be used to complete the request. This extension is only permissible based upon the IDOH's provision to the requester of the reason for the delay and the date when the request will be completed.

Multiple Disclosures to Same Person/Entity: If during the period covered by the accounting, the IDOH covered component has made multiple disclosures of PHI to the same person or entity for a single purpose under the Privacy Rule provisions for Office for Civil Rights (OCR) investigations or reviews (45 CFR § 164.502(a)(2)(ii)), or for permitted uses and disclosures (45 CFR § 164.512), the accounting may, with respect to such multiple disclosures, provide:

- The full range of information required for the first disclosure during the accounting period;
- The frequency, periodicity, or number of disclosures made during the accounting period; and
- The date of the last such disclosure during the accounting period.

Research Disclosure Accounting: If during the period covered by the accounting, the IDOH covered component has made disclosures of PHI for a particular research purpose in accordance with the Privacy Rule's provisions on permitted uses and disclosures approved by an Institutional Review Board or a Privacy Board (45 CFR § 512 (i)), for 50 or more individuals, the accounting may, with respect to such disclosures for which the PHI about the individual may have been included, provide:

- Name of the protocol or other research activity,
- A plain language description of the research protocol or other research activity,
- A brief description of the type of PHI that was disclosed,
- The date or time period during which such disclosures occurred or may have occurred,
- The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed, and
- A statement that the PHI of the individual may or may not have been disclosed for a particular protocol or other research activity.

If the IDOH covered component provides an accounting for research disclosures, in line with the previous paragraph, and if it is reasonably likely that the PHI of the individual was disclosed for such research protocol or activity, the IDOH covered component shall, at the request of the individual, assist in contacting the entity that sponsored the research and the researcher.

Failure to comply with requirements of this policy may subject the employee to discipline, per the HIPAA Sanctions Policy.

Legal Authorities and References

- Laws
- Regulations
    - 31 IAC 5-12 – Disciplinary Actions and Separations
    - 45 CFR 164.502 – Uses and Disclosures of PHI: General rules
    - 45 CFR 164.512 – Uses and Disclosures for which an authorization or opportunity to agree or object is not required
    - 45 CFR 165.528 – Accounting of disclosures of protected health information
- PHAB Standards
- Related Policies
    - HIPAA Access Request Policy
    - HIPAA Sanctions Policy

Authorized Uses and Disclosures of PHI Policy

Purpose

To ensure a consistent and efficient manner of accepting, responding to, and documenting participants' authorization to release PHI.

Policy Statement

IDOH covered components must obtain the individual's written authorization for any use or disclosure of PHI, other than disclosures for:

- Treatment,
- Payment,
- Health care operations, or
- Uses or disclosures otherwise permitted or required by the Privacy Rule. (See Required Uses and Disclosures of PHI Policy and Permitted Uses and Disclosures of PHI Policy.)

Psychotherapy Notes: IDOH covered components must obtain an individual's authorization to use or disclose psychotherapy notes, with specific exceptions.

Marketing: IDOH covered components must obtain written authorization before using or disclosing an individual's PHI for any marketing communication, with specific exceptions. Marketing generally means "to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service."

An IDOH covered component may not condition treatment, payment, enrollment, or benefits eligibility on an individual granting an authorization, unless:

- the authorization is requested by the health plan prior to the individual's enrollment, and the authorization is not for a use or disclosure of psychotherapy notes;
- the authorization is requested for the use or disclosure of PHI for the provision of research-related treatment; and
- the authorization is requested by a health care provider solely for the purpose of creating PHI for disclosure to a third-party.

All authorizations must be in plain language and contain specific information regarding the information to be disclosed or used, the person(s) disclosing and receiving the information, an expiration date, the right to revoke in writing, and other terms.

IDOH covered components may not rely on an authorization known to be revoked or known to have expired. An individual may revoke authorization at any time by submitting a revocation statement in writing. Revocation of an authorization does not affect actions we may have undertaken in reliance on the authorization before we learned of its revocation. In addition, a revocation statement must include sufficient information to identify the requestor, state the IDOH covered component(s) to which it applies, and include an effective date.

Procedures and Responsibilities

If the covered component is unclear whether or not a particular use or disclosure of PHI requires an authorization, the Program Privacy Coordinator for that covered component should forward the question to the Privacy Officer or designee for guidance and a determination regarding the issue.

When a signed authorization is required for a use or disclosure of PHI, an IDOH covered component must obtain approval for its authorization form from the Privacy Officer, if the component does not already have a HIPAA-compliant authorization form. This form is to be forwarded to the individual or the individual's personal representative for completion. The

Program Privacy Coordinator must ensure collection and retention of the original version of each completed authorization form. If the authorization has been completed incorrectly or is incomplete or invalid, it must be returned to the individual or personal representative for completion or correction and resubmission.

IDOH covered components will retain, on paper or electronically, each signed authorization and each authorization revocation received until six years after the later of its creation or last effective date.

Failure to comply with requirements of this policy may subject the employee to discipline, per the HIPAA Sanctions Policy.

Legal Authorities and References

- Laws
- Regulations
  - 31 IAC 5-12 – Disciplinary Actions & Separations
  - 45 CFR 164.501 – Definitions
  - 45 CFR 164.508 – Uses and Disclosures for which authorization is required
- PHAB Standards
- Related Policies
  - Permitted Uses and Disclosures of PHI Policy
  - Required Uses and Disclosures of PHI Policy
  - HIPAA Sanctions Policy

Forms

N/A

Minimum Necessary PHI Policy

Purpose

To establish guidelines relating to the minimum necessary requirements for the use and disclosure of, and requests for, PHI.

Policy Statement

The IDOH must make reasonable efforts to use, to disclose, and to provide upon request of another covered entity, only the minimum necessary PHI to accomplish the intended purpose.

There is no minimum necessary limitation for:

- disclosure to or a request by a health care provider for treatment
- use with and disclosure to an individual (or the individual's personal representative) with respect to his or her own PHI
- use and disclosure pursuant to an authorization by an individual (or the individual's personal representative) with respect to his or her own PHI
- disclosures made to Health and Human Services (HHS) for compliance and enforcement activities
- use and disclosure required by law, including the Privacy Rule.

Minimum Necessary and Workforce Use of PHI

IDOH covered programs must make reasonable efforts to limit access to and use of PHI by workforce members to the minimum necessary to perform their duties.

Each IDOH covered program must use its professional judgment to identify all of the following:

- The covered entity staff who need access to PHI to carry out their job duties
- The category, or categories, of PHI access necessary for the job duties
- Any conditions appropriate to such access

IDOH covered programs must make reasonable efforts to limit the access of PHI to the identified covered program staff. The access limitations apply to electronic, paper, or oral communication of PHI.

Minimum Necessary and PHI Disclosures

Routine Disclosures: For any disclosures made on a routine and recurring basis, IDOH covered programs must implement policies and procedures that limit the PHI disclosed to the amount reasonably necessary to achieve the purpose of the disclosure.

Non-routine Disclosures: For non-routine disclosures, IDOH covered programs must develop criteria designed to limit the PHI disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought, and review requests for disclosure on an individual basis in accordance with such criteria.

Reliance on Minimum Necessary Claims for Disclosures: An IDOH covered program may rely, if reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when:

- Making disclosures to public officials as permitted under the Privacy Rule;

- Responding to requests by another covered entity;
- Responding to requests by a professional who is a member of the IDOH workforce or is a business associate of the covered program for providing professional services to the program, if the professional represents that the information requested is the minimum necessary for the stated purpose; or
- Provided with documentation or representations that comply with the applicable requirements under the Privacy Rule that have been provided by a person requesting the information for research purposes.

Minimum Necessary and PHI Requests

Requests by IDOH Covered Programs: IDOH covered programs must limit any request for PHI from other covered entities to that which is reasonably necessary to accomplish the purpose for which the request is made.

Routine requests: IDOH covered programs must implement procedures, for requests made on a routine and recurring basis, that limit the PHI requested to the amount reasonably necessary to accomplish the purpose for which the request is made.

Non-routine requests: IDOH covered programs must develop criteria designed to limit the request for PHI to the information reasonably necessary to accomplish the purpose for which the request is made, and review requests for disclosure on an individual basis in accordance with such criteria.

Procedures and Responsibilities

Workforce members in IDOH covered components should contact their Program Privacy Coordinator or appropriate supervisor with any questions about their specific Minimum Necessary obligations. If the issue cannot be resolved by officials within the program, the Program Privacy Coordinator should contact the Privacy Officer for guidance.

Failure to comply with requirements of this policy may subject the employee to discipline, per the HIPAA Sanctions Policy.

Legal Authorities and References

- Laws
- Regulations
    - 31 IAC 5-12 – Disciplinary Actions & Separations
    - 45 CFR 164.501 - Definitions

  - 45 CFR 164.502(b) – Uses and disclosures of protected health information: General rules
  - 45 CFR 164.514 (d)(1) – Other requirements relating to uses and disclosures of protected health information
- PHAB Standards
- Related Policies
  - HIPAA Sanctions Policy

Forms

N/A

Permitted Uses and Disclosures of PHI Policy

Purpose

To define and limit the circumstances in which an individual's PHI is permitted to be used or disclosed by IDOH covered components without authorization or permission of the individual.

Policy Statement

IDOH covered components are permitted, but not required, to use and disclose PHI, without an individual's authorization or permission, for the following purposes or situations:

- Disclosures to the Individual (unless required under requests for access or accounting of disclosures)
- Treatment, Payment, or Health Care Operations
- Opportunity to Agree or Object
- Incident to an otherwise permitted use and disclosure
- Public interest and benefit activities
- Limited data set for the purposes of research, public health, or health care operations

To the Individual

An IDOH covered component may disclose PHI to the individual who is the subject of the information.

Treatment, Payment or Health Care Operations

An IDOH covered component may use and disclose PHI for its own treatment, payment, and health care operations. An IDOH covered component also may disclose PHI for the treatment activities of any health care provider. An IDOH covered component may disclose the minimum

necessary PHI for the payment activities of another covered entity and of any health care provider, or the health care operations of another covered entity.

Opportunity to Agree or Object
This involves "informal" permission to use or disclose PHI, more relevant to covered health care providers than health plans.

Incident to an otherwise permitted use and disclosure
A use or disclosure by an IDOH covered component that occurs as a result of, or as "incident to," an otherwise permitted use or disclosure is permitted as long as the covered entity has adopted reasonable safeguards, and the information being shared was limited to the minimum necessary, as required by the Privacy Rule.

Public interest and benefit activities
IDOH covered components may use or disclose PHI, without an individual's authorization or permission, for several national priority purposes, including the following:

- Required by law (including by statute, regulation, or court orders)
- Public health activities
- Victims of abuse, neglect, or domestic violence
- Health oversight activities
- Judicial and administrative proceedings
- Law enforcement purposes
- Decedents
- Cadaveric organ, eye, or tissue donation
- Research
- Serious threat to health or safety
- Essential government functions
- Worker's Compensation

However, if any of the proposed uses or disclosures of PHI relates to a communicable disease under 410 IAC 1-2.3, then the PHI may not be released except as allowed under IC 16-41-8-1.

Limited Data Set
See separate Limited Data Set Policy, included below.

Procedures and Responsibilities

Workforce members in IDOH covered components shall contact their Program Privacy Coordinator with any questions about whether a particular use or disclosure is permitted under the Privacy Rule. The Program Privacy Coordinator will forward the question to the Privacy Officer for a response.

Failure to comply with requirements of this policy may subject the employee to discipline, per the HIPAA Sanctions Policy.

Legal Authorities and References

- Laws
  - IC 16-41-8-1 – Potentially disease transmitting offense
- Regulations
  - 31 IAC 5-12 – Disciplinary Actions & Separations
  - 410 IAC 1-2.5 – Disease Reporting and Control
  - 45 CFR 164.501 - Definitions
  - 45 CFR 164.502(a) (1) – Uses and disclosures of protected health information: General rules
- PHAB Standards
- Related Policies
  - HIPAA Limited Data Set Policy
  - HIPAA Sanctions Policy

Forms

N/A

Personal Representatives and Rights of Minors Policy

Purpose

To issue instruction to all IDOH workforce members about the policy and procedures for disclosures of PHI to a participant's personal representative and the rights of a minor.

Policy Statement

The IDOH will treat a personal representative as the participant. The personal representative must provide documentation that proves the relationship and authority to serve as personal representative of the participant. The type of documentation required may vary so if workforce

members are not certain what documentation they need, they should contact the Privacy Officer.

A designated personal representative of a participant has the right to inspect and obtain a copy of the participant's PHI in the designated record set, except as indicated in the Privacy Rule for unemancipated minors who may lawfully obtain health care service without the consent of a parent or guardian, and in situations of abuse, neglect, or endangerment. All requests for access received will be documented, reviewed, and responded to within the timeframes required by the Privacy Rule.

In the state of Indiana, a parent, guardian, or other court appointed representative is entitled to exercise the participant's rights on the participant's behalf if the participant is an unemancipated minor. The IDOH must treat such an individual as a personal representative with respect to PHI. A custodial parent and noncustodial parent of a child have equal access to the child's health records unless the following apply:

- a court has issued an order that limits the noncustodial parent access to the child's health records, and
- the IDOH has received a copy of the court order or has actual knowledge of the court order.

If under applicable law, a person has authority to act on behalf of a participant who is an adult or an emancipated minor in making decisions related to health care, the IDOH must treat such person as a personal representative with respect to PHI. Notwithstanding a State law or any other contrary requirement in the Privacy Rule provisions on personal representatives, the IDOH may elect not to treat a person as the personal representative of a participant if the IDOH has a reasonable belief that:

- the participant has been or may be subjected to domestic violence, abuse, or neglect by such person; or
- treating such person as the personal representative could endanger the participant; and
- the IDOH, in the exercise of professional judgment, decides that it is not in the best interest of the participant to treat the person as the participant's personal representative.

Procedures and Responsibilities

Workforce members in IDOH covered components shall contact their Program Privacy Coordinator with any questions about the status of a personal representative. The Program Privacy Coordinator will forward the question to the Privacy Officer for a response.

Failure to comply with requirements of this policy may subject the employee to discipline, per the HIPAA Sanctions Policy.

Legal Authorities and References

- Laws
- Regulations
    - 31 IAC 5-12 – Disciplinary Actions & Separations
    - 45 CFR 160 – General Administrative Requirements
    - 45 CFR 164 – Security and Privacy
- PHAB Standards
- Related Policies
    - HIPAA Access Request for PHI Policy
    - HIPAA Sanctions Policy
    - IDOH Confidentiality Policy

Forms

N/A

PHI Safeguards Policy

Purpose

To issue instructions to workforce members in IDOH covered components about the policy and procedures relating to the administrative, technical, and physical safeguards to protect Protected Health Information (PHI).

Policy Statement

IDOH covered components will implement and comply with reasonable and appropriate administrative, physical, and technical safeguards to protect the privacy of PHI against any intentional or unintentional use or disclosure in violation of these IDOH Privacy Policies and Procedures or the HIPAA Privacy Rule. These safeguards will include reasonable limits to incidental uses or disclosures of PHI made as a result of otherwise permitted uses and disclosures.

Any unauthorized use or disclosure by an IDOH workforce member is subject to the sanctions set forth by IDOH for breach of security or privacy.

Procedures and Responsibilities

Workforce members in IDOH covered components must use the password protect function on computers left unattended. Any passwords for a computer and/or any software or web applications must not be stored on or near the computer. All fax machines must be located in an attended and/or secure area, minimizing the risk of inadvertent disclosure of PHI to an unintended recipient. Information requested by fax must be retrieved from the fax machine immediately by the intended recipient or delivered to the recipient by an authorized staff member. If a staff member is faxing information to an authorized recipient of the PHI, the fax machine must be attended during the faxing. The workforce member must also confirm the fax number of the recipient prior to sending the fax.

The workforce member of the IDOH covered component must retrieve printed PHI from the printer or copier at the time of printing. PHI, including an original document for copying, must not be left unattended at the printer or copier.

PHI must not be left unattended on the top of filing cabinets, on the floor, or in an open work area. The risk of incidental disclosure must be minimized to meet HIPAA Privacy requirements. At the end of the workday, IDOH workforce members must ensure that PHI in open work areas (including any remote workspace) is stored securely, in a locked cabinet or desk if appropriate. PHI (paper and electronic PHI) must be secured when it is transported from one workspace to another, for example from IDOH premises to a remote workspace. Lock PHI in your vehicle or other secure space as necessary to minimize the risk of disclosure.

Failure to comply with requirements of this policy may subject the employee to discipline, per the HIPAA Sanctions Policy.

Legal Authorities and References

- Laws
- Regulations
    - 31 IAC 5-12 – Disciplinary Actions & Separations
    - 45 CFR 160 – General Administrative Requirements
    - 45 CFR 164 – Security and Privacy
- PHAB Standards
- Related Policies
    - HIPAA Sanctions Policy
    - IDOH Confidentiality Policy

Forms

N/A

Privacy of PHI Policy

Purpose

To ensure that all PHI created, used, or disclosed by the IDOH is maintained and released in compliance with the HIPAA Privacy Rule.

Policy Statement

It is the policy of the IDOH to ensure that all workforce members comply with the applicable requirements of the HIPAA Privacy Rule. The HIPAA Privacy Rule covers all PHI in written, electronic, or oral form, maintained or transmitted by IDOH covered components.

Procedures and Responsibilities

IDOH covered components may not disclose PHI to external entities or IDOH non-covered components in circumstances in which the Privacy Rule would prohibit such disclosure. When receiving, using, or transmitting PHI originating from an IDOH covered component, all IDOH workforce members have the responsibility to make reasonable efforts to comply with IDOH policies and procedures designed to protect PHI.

If an individual performs duties as a workforce member of both an IDOH covered component and an IDOH non-covered component, that individual must not use or disclose PHI created or received in the course of or incident to the member's work for the covered component in a way prohibited by the Privacy Rule. It is a condition of employment that the IDOH workforce complies with the HIPAA federal rules regarding privacy and security.

Failure to comply with requirements of this policy may subject the employee to discipline, per the HIPAA Sanctions Policy.

Legal Authorities and References

- Laws
- Regulations
    - 31 IAC 5-12 – Disciplinary Actions & Separations
    - 45 CFR 164.504 – Uses and Disclosures: Organizational requirements
- PHAB Standards
- Related Policies
    - HIPAA PHI Safeguards Policy

- HIPAA Sanctions Policy
- IDOH Confidentiality Policy

Forms

N/A

Removal of PHI from IDOH Premises Policy

Purpose

To ensure that no workforce members remove PHI from IDOH premises without a necessary, legitimate, work-related purpose and to ensure the preservation of the confidentiality and integrity of such records when removed from IDOH premises.

Policy Statement

It is the policy of the IDOH to prohibit the removal of any documents, portable electronic devices or media that contain PHI from IDOH premises without a necessary, legitimate, work-related purpose and without proper authorization.

Procedures and Responsibilities

IDOH workforce members must obtain written authorization from their Program Director or his/her delegate prior to removing PHI from IDOH premises.

Except for authorization to work remotely as allowed by the Work Schedules Policy, an authorization to remove PHI from IDOH premises must have an expiration period commensurate with the workforce member's necessary, legitimate, work-related purpose for removing such records from IDOH premises which may not exceed three (3) months. If the workforce member's necessary, legitimate, work-related purpose for removing such records from IDOH premises will extend beyond 3 months, the authorization must be renewed.

Approval of a request for an Alternate Work Schedule, that includes remote work, authorizes IDOH workforce members to remove PHI from IDOH premises, including electronic PHI, as necessary to perform their job duties. PHI may be removed by the IDOH workforce member for the days they are approved to work remotely. The PHI shall be returned to the IDOH premises as soon as possible and practical.

When removing PHI from IDOH premises, IDOH workforce members have the responsibility to make reasonable efforts to comply with IDOH policies and procedures designed to protect PHI. All IDOH workforce members must secure PHI while it is in transit from IDOH premises to an authorized remote work location. They also need to securely store any PHI while it is at the

remote work location, so that PHI will not be visible by or accessible to any unauthorized people.

A record of all PHI leaving IDOH premises, whether in written form, on a portable electronic device or media, must be kept and should, at a minimum, describe the nature of the PHI, the purpose for removing the PHI from IDOH premises, and the workforce member responsible for safeguarding that PHI while it is off IDOH premises.

In the event a document, portable electronic device, or media containing PHI become lost or stolen, the workforce member must report the incident to their Program Director and the Privacy Officer (317-233-7655 and IDOHPrivacyOfficer@isdh.in.gov) within two (2) hours of noticing it is missing. The Privacy Officer will inform the Security Officer about any incidents that involve or may involve ePHI.

Failure to comply with requirements of this policy may subject the employee to discipline, per the HIPAA Sanctions Policy.

Legal Authorities and References

- Laws
- Regulations
  - 31 IAC 5-12 – Disciplinary Actions & Separations
  - 45 CFR 164.310 – Physical Safeguards
- PHAB Standards
- Related Policies
  - HIPAA PHI Safeguards Policy
  - HIPAA Sanctions Policy
  - IDOH Confidentiality Policy

Forms

N/A

Required Uses and Disclosures of PHI Policy

Purpose

To define and limit the circumstances in which an individual's PHI is required to be disclosed by covered components within the IDOH.

Policy Statement

An IDOH covered component is required to disclose PHI in only two situations:

a) to individuals (or their personal representatives) specifically when they request access to, or an accounting of disclosures of, their PHI (subject to applicable exceptions); and
b) to the Office for Civil Rights within the U.S. Department of Health and Human Services when it is undertaking a compliance investigation or enforcement action.

Procedures and Responsibilities

Workforce members in IDOH covered components shall follow existing procedures for Requests for Access and Accounting of Disclosures.

All communications from the Office for Civil Rights shall be directed to the Program Privacy Coordinator and immediately forwarded to the Privacy Officer.

Failure to comply with requirements of this policy may subject the employee to discipline, per the HIPAA Sanctions Policy.

Legal Authorities and References

- Laws
- Regulations
    - 31 IAC 5-12 – Disciplinary Actions & Separations
    - 45 CFR 164.501 - Definitions
    - 45 CFR 164.502(a)(2) – Uses and disclosures of protected health information: General rules
- PHAB Standards
- Related Policies
    - HIPAA Access Request for PHI Policy
    - HIPAA Accounting of Disclosures of PHI Policy
    - HIPAA Sanctions Policy

Forms

N/A

Request for Amendment of PHI Policy

Purpose

To ensure a consistent and efficient implementation of policy and procedures to respond to requests for amendment of PHI.

Policy Statement

IDOH covered components will allow a program participant to request amendment of his or her PHI, or a record about the individual in a designated record set, for as long as an IDOH covered component, or its business associate maintains the PHI in the designated record set.

An IDOH covered component may only deny an amendment request if one of the following conditions applies:

- The IDOH covered component did not create the PHI or record that is the subject of the request (unless the individual provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment).
- The information to be amended is not part of a designated record set maintained by an IDOH covered component or by a business associate on its behalf.
- The information is accurate and complete.
- The information to be amended may be withheld from an individual's right of access under the Privacy Rule (see Access Request of PHI Policy).

Procedures and Responsibilities

The program participant, or the participant's personal representative, must make a written request to the Privacy Officer. The request must contain a statement providing a reason for the amendment, the records to be amended, the IDOH covered component who has the records, and whom the participant wants the program to notify about the amendment.

After preliminary review of the Amendment Request to ensure that it has been submitted properly and completely, the Privacy Officer will coordinate with the appropriate covered component to, within 30 days, identify and collect the PHI or record(s) that the participant has requested be amended. The Privacy Officer and officials within the covered component will determine whether the request to amend should be granted or denied.

The Privacy Officer will send (by mail or encrypted email at the requester's preference) a response to the requester within 60 days of receipt of the request. If the Privacy Officer and affected covered component are unable to act on the amendment request within the 60-day

time period, one 30-day extension can be used to complete the request. However, the Privacy Officer must notify the requester or the requester's personal representative of the reasons for the delay and the date when the request will be complete.

If the request is accepted, the following will occur:

- The IDOH covered component will make the appropriate amendment to the PHI or record that is the subject of the request by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment.
- The IDOH covered component will make reasonable efforts to inform and provide the amendment within a reasonable time to:
    - entities identified by the participant as having PHI about the individual and needing the amendment; and
    - entities, including business associates, that the IDOH covered component knows have the PHI that is the subject of the amendment and that may have relied, or could conceivably rely, on such information to the detriment of the participant.
- The Privacy Officer will inform the participant that the amendment has been accepted by preparing and mailing a Participant Amendment Request Approval letter.
- The Privacy Officer will document the amendment request in the Amendment Tracking System.

If the request is denied, the following will occur:

- The Privacy Officer will forward a completed Participant Amendment Request Denial letter to the participant, which includes the following:
    - the basis for the denial;
    - the individual's right to submit a statement of disagreement;
    - a statement that, in lieu of the statement of disagreement, the individual may request that the relevant IDOH covered component provide the individual's request for amendment and denial with any future disclosures of the PHI that is the subject of the amendment; and
    - a description of options for filing a complaint with the IDOH or Office for Civil Rights (OCR).
- The Privacy Officer will document denial of the amendment request in the Amendment Tracking System.
- The Privacy Officer will mail a completed Notice of Denial to Amend Records and a copy of the Participant Amendment Request Denial letter to persons identified by the participant. In addition:

- The participant has the right to submit to the IDOH covered component a written statement of disagreement concerning the denial of all or part of the requested amendment and the basis for such disagreement.
- The IDOH covered component may prepare a written rebuttal statement to a participant's disagreement statement. Whenever such a rebuttal is prepared, the Privacy Officer will provide a copy to the individual who submitted the disagreement statement.
- The IDOH covered component will, as appropriate, identify the record or PHI in the designated record set that is the subject of the disputed amendment and append or otherwise link:
  - the individual's request for an amendment;
  - the IDOH covered component's denial of the request;
  - the individual's statement of disagreement, if any; and
  - the IDOH covered component's rebuttal, if any, to that designated record set.

Future disclosures after amendment denial

- The following provisions apply for future disclosures of the PHI of which amendment was denied:
  - If a disagreement statement has been submitted by the individual, the IDOH covered component will include the amendment denial material appended to the designated record set (or at the election of the covered component, a summary of the information), with any subsequent disclosure of the PHI to which the disagreement refers;
  - If the individual did not submit a written disagreement statement, the IDOH covered component must include the individual's amendment request and its denial, or an accurate summary of such information, with any subsequent disclosure of the PHI, but only if the individual has requested such action in response to the terms specified in the Participant Amendment Request Denial letter.
- When a subsequent disclosure as described above is made using a standard transaction under 45 CFR 162 that does not permit the additional material to be included with the disclosure, the IDOH covered component may separately transmit the required material to the recipient of the standard transaction.

IDOH covered components that are informed by another covered entity of an amendment to an individual's PHI must amend the PHI in designated record sets as provided above in provisions for accepting an amendment.

IDOH covered components will document the titles of the persons or offices responsible for receiving and processing requests for amendments by individuals and retain the documentation for six years from the date of its creation or the date when it last was in effect, whichever is later.

Failure to comply with requirements of this policy may subject the employee to discipline, per the HIPAA Sanctions Policy.

Legal Authorities and References

- Laws
- Regulations
    - 31 IAC 5-12 – Disciplinary Actions & Separations
    - 45 CFR 164.526 – Amendment of protected health information
- PHAB Standards
- Related Policies
    - HIPAA Sanctions Policy

Forms

N/A

B. Business Associate Policy

Business Associate Policy

Purpose

To establish and issue instructions about the standards for PHI uses and disclosures involving IDOH business associates.

Policy Statement

It is the policy of the IDOH not to disclose PHI to a business associate, nor to allow a business associate to create, receive, maintain, or transmit PHI on the IDOH's behalf, unless the Privacy Officer or the Office of Legal Affairs confirms that the business associate has entered into a written contract with the IDOH that contains HIPAA-required business associate language.

The business associate contract requirement does not apply:

- With respect to disclosures by the IDOH to a health care provider concerning treatment, payment, or health care operations involving the individual.

- With respect to disclosures to a plan sponsor of a group health plan that the IDOH services.
- With respect to uses and disclosures by IDOH health plans providing public benefits if eligibility for, or enrollment in, the plan is determined by an agency other than the IDOH health plan, or if the PHI used to determine enrollment in or eligibility for the plan is collected by an agency other than the IDOH, and that collection activity is authorized by law.

IDOH programs may not serve as business associates of covered entities unless approved by the Privacy Officer. When an IDOH program serves as a business associate, a business associate agreement will be established with the covered entity. The IDOH will fully comply with the terms of each business associate contract entered into as a business associate of a covered entity.

Procedures and Responsibilities

The Program Privacy Coordinator is responsible for notifying the Privacy Officer immediately if a business associate is suspected of breaching or violating a business associate agreement with an IDOH covered program. The Privacy Officer will notify the Security Officer as soon as possible about any breaches or violations that involve or may involve ePHI

If the IDOH learns of a pattern of activity or practice of a business associate that constitutes a material breach or violation of its business associate's obligations under the contract, IDOH will take reasonable steps to cure the breach or end the violation and, if such steps are unsuccessful, will terminate the contract, if feasible. If termination of the contract is not feasible, IDOH will report the business associate's breach to the U.S. Department of Health and Human Services, Office of Civil Rights.

The Privacy Officer will conduct annual audits of all business associate agreements involving IDOH programs.

Failure to comply with requirements of this policy may subject the employee to discipline, per the HIPAA Sanctions Policy.

Legal Authorities and References

- Laws
- Regulations
    - 31 IAC 5-12 – Disciplinary Actions and Separations

  - 45 CFR 160.103 - Definitions
  - 45 CFR 164.502(e) – Uses and disclosures of protected health information
  - 45 CFR 164.504(e) – Uses and disclosures: Organizational requirements
- PHAB Standards
- Related Policies
  - HIPAA Sanctions Policy

Forms

N/A

C. Complaint Policy

Complaint Policy

Purpose

To ensure that an effective complaint process is in place to deal with suspected violations of HIPAA regulations. The process should include, without limitation: identification of a designee responsible for receiving complaints, a method for documenting receipt of complaints and their resolution, assurance that no individual will be required to waive their rights to file a complaint with the Privacy Officer or with the Department of Health and Human Services.

Policy Statement

It is the policy of the IDOH to make certain that compliance efforts are in place for PHI, as well as to ensure that such information is used and disclosed in accordance with all applicable laws and regulations. Any concerned individual has the right to file a formal complaint concerning any suspected violation of the HIPAA regulations including workforce members. Any concerned individual has the right to file a formal complaint concerning issues without fear of reprisal. Such issues could include but are not limited to, allegations that:

- PHI was used/disclosed improperly;
- Access or amendment rights were wrongfully denied; or
- The IDOH Notice of Privacy Practices does not reflect current practices accurately.

Procedures and Responsibilities

1. All program participants or their personal representatives have been informed of their right to file a complaint with the Privacy Officer or the Department of Health and Human Services in the IDOH Notice of Privacy Practices.

2. All concerns may be registered by telephone, mail, or in person.
3. Upon notification of a suspected HIPAA violation or a possible violation of the IDOH HIPAA policies or the law, the Program Privacy Coordinator will immediately inform the Privacy Officer. The complaint will be recorded on the Complaint Log. The *IDOH HIPAA Complaint form* will be forwarded to the concerned individual to complete.
4. The completed complaint form will be sent to the Privacy Officer.
5. The Privacy Officer will advise the Security Officer about the complaint if the complaint involves or may involve ePHI. The Security Officer may collaborate with the Privacy Officer on the investigation and the Privacy Officer's findings.
6. The Privacy Officer will develop and coordinate an investigation plan. The Privacy Officer will either personally investigate the complaint or will direct a designee to investigate the allegations. The investigator will review and investigate to determine if a violation of the law or policies has occurred and shall submit the findings to the Privacy Officer for final review.
7. The Privacy Officer shall determine the substance of the findings and will coordinate the method of response.
    a. Document the resolution of the complaint.
    b. Communicate the outcome of the complaint with the individual filing the complaint in a timely manner. The Privacy Officer will send a Complaint Response letter to the complainant at the conclusion of the investigation.
8. The Privacy Officer shall maintain documentation of all complaints received and their disposition for a period of at least six years (from the date of disposition) in accordance with federal regulations.

Failure to comply with the requirements of this policy may subject the employee to discipline per the HIPAA Sanctions Policy.

Legal Authorities and References

- Laws
- Regulations
    - 31 IAC 5-12 – Disciplinary Actions & Separations
    - 45 CFR 164.501 - Definitions
    - 45 CFR 164.508 – Uses and disclosures for which an authorization is required
- PHAB Standards
- Related Policies
    - HIPAA Sanctions Policy

Forms

IDOH HIPAA Complaint form

D. Computer Transfer and Disposal Policy

Computer Transfer and Disposal Policy

Purpose

To ensure that computer equipment at the IDOH containing PHI is transferred, removed, or disposed of in compliance with established IDOH procedures.

Policy Statement

The IDOH prohibits the transfer, removal, or disposal of any computer that contains ePHI (e.g., desktop, laptop, PDA, fax machine) from an IDOH covered component without proper authorization and notification.

Procedures and Responsibilities

- The removal of any computer that is not normally assigned to a specific IDOH workforce member and contains ePHI must be authorized by the program director responsible for that ePHI, prior to removal from the program area.
- Any member of the IDOH workforce, including individuals who are responsible for maintaining, repairing, and protecting agency computers must obtain prior authorization from a program director or his/her designee before removal of a computer from a HIPAA covered component, if the computer contains ePHI. Approval for a remote work schedule under IDOH policies provides a member of the IDOH workforce with the necessary authorization to properly remove a computer from the program area to an authorized remote work location.
- In cases where prior authorization is not required or in an emergency (e.g., virus attack) when a computer containing ePHI must be removed, subsequent notification must be provided within 24 hours to the responsible program director containing the following information:
    - The location from which the computer was removed
    - Serial number of the computer

  - The purpose of the removal
  - The location to which the computer was moved
  - The information technology services contact person for communication on additional matters, such as repair status, extent of damage, special security measures needed.
- Anyone who discovers an unauthorized removal of a computer containing ePHI from an IDOH covered component must immediately report that removal to the responsible program director, the Privacy Officer, and the Security Officer.

It is a condition of employment that the IDOH workforce complies with the HIPAA federal rules regarding privacy and security.

Failure to comply with requirements of this policy may subject the employee to discipline, per the HIPAA Sanctions Policy.

Legal Authorities and References

- Laws
- Regulations
  - 31 IAC 5-12 – Disciplinary Actions and Separations
- PHAB Standards
- Related Policies
  - HIPAA Sanctions Policy

Forms

N/A

E. Communications Policies

Confidential Communication of PHI Policy

Purpose

To ensure that individual requests to use alternative means or an alternative location when communicating PHI receive responses in a consistent and efficient manner.

Policy Statement

IDOH covered components will permit requests, and will accommodate reasonable requests, from individuals to use alternative means or an alternative location for communicating PHI. The

requester should clearly state that the disclosure of all or part of his or her PHI, without the granting of the request, could endanger the individual.

Procedures and Responsibilities

Participants must submit requests for confidential communications by alternative means or to alternative locations to the Privacy Officer in writing. Any IDOH workforce member who receives a request for confidential communications from a participant should forward the request to the Privacy Officer. A request should include the participant's contact information, the name of the IDOH covered component involved, a description of the alternative means or location that the requestor wants to use, and that the disclosure of all or part of his or her PHI, without the granting of the request, could endanger the individual.

Once the Privacy Officer or designee determines the request to be complete and verifies the requester's identity, the Privacy Officer or designee will coordinate with the relevant covered component to determine the reasonableness of the request. IDOH covered components may condition the provision of a reasonable accommodation on:

- when appropriate, information as to how payment, if any, will be handled; and
- specification of an alternative address or other method of contact.

The Privacy Officer or designee will send a written response to the requester with the decision whether or not the IDOH covered component will accommodate the request. The IDOH covered component will notify all affected business associates of necessary adjustments for any confidential communication request that is granted.

Failure to comply with requirements of this policy may subject the employee to discipline, per the HIPAA Sanctions Policy.

Legal Authorities and References

- Laws
- Regulations
    - 31 IAC 5-12 – Disciplinary Actions and Separations
    - 45 CFR 164.501 - Definitions
    - 45 CFR 164.522(b) – Rights to request privacy protection for protected health information
- PHAB Standards
- Related Policies
    - HIPAA Policy on Permitted Uses and Disclosures
    - HIPAA Sanctions Policy

Forms

N/A

Identification and Authority Verification Policy

Purpose

To ensure a consistent and efficient manner confirming identity and authority of individuals submitting requests regarding PHI.

Policy Statement

The IDOH covered component must verify the identity of the person requesting PHI and the authority of the person to have access to PHI, if the identity or such authority of the person is not known to the IDOH. Also, the IDOH covered component must obtain any documentation, statements, or representations (written or oral) from the person requesting the PHI when the documentation, statement, or representation is required for the PHI disclosure.

Procedures and Responsibilities

IDOH covered components must obtain appropriate identification and, if the person is not the individual who is the subject of the requested PHI, evidence of authority. If the IDOH covered component questions whether verification presented is sufficient, consult the Privacy Officer before making any disclosure. Any member of the IDOH workforce who receives a request regarding PHI from an individual should forward the request to the Privacy Officer.

The Privacy Rule provides specific procedures for the verification of identity and authority of public officials:

- **Verification of Identity**: When a public official requests PHI, IDOH covered components may reasonably rely on any of the following to verify identity:
    - *If request is made in person*, presentation of an agency identification badge, other official credentials, or other proof of government status;
    - *If the request is in writing*, the request is on appropriate government agency letterhead; or
    - *If request is from person on behalf of a public official,* a written statement on appropriate government agency letterhead says that the person is acting under the government's authority or other evidence or documentation of agency that establishes that the person is acting on behalf of the public official.

- **Verification of Authority**: An IDOH covered component may reasonably rely on any of the following to verify authority when the disclosure of PHI is to a public official:
    - A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority;
    - A request made pursuant to legal process, warrant, subpoena, order or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority.

Failure to comply with requirements of this policy may subject the employee to discipline, per the HIPAA Sanctions Policy.

Legal Authorities and References

- Laws
- Regulations
    - 31 IAC 5-12 – Disciplinary Actions & Separations
    - 45 CFR 160 – General Administrative Requirements
    - 45 CFR 164.514 (h) – Other requirements relating to uses and disclosures of protected health information
- PHAB Standards
- Related Policies
    - IDOH Confidentiality Policy
    - HIPAA Sanctions Policy

Forms

N/A

Restricted Communication of PHI Policy

Purpose

To ensure participants in IDOH Covered Components have a method for requesting restrictions on the use and disclosure of PHI.

Policy Statement

IDOH covered components will allow program participants to request restrictions of the following:

- Uses or disclosures of PHI about the individual to carry out treatment, payment, or health care operations; and
- Disclosures permitted under the Privacy Rule to persons involved in the individual's care or for notification purposes.

The IDOH covered component is under no obligation to agree to requests for restrictions. A covered component that does agree must comply with the agreed restrictions, except that the covered component may use the restricted PHI, or may disclose it to a health care provider, for purposes of treating the individual in a medical emergency.

A restriction agreed to by an IDOH covered component does not prevent uses or disclosures permitted or required as follows:

- When required by the U.S. Dept. of Health and Human Services Office for Civil Rights to determine compliance with the Privacy Rule.
- In the context of an opportunity to agree or object to use and disclosure of PHI for facility directories, under 45 CFR 164.510(a).
- When permitted under 45 CFR 164.512 (See Permitted Uses and Disclosures Policy).

An IDOH covered component may terminate its agreement to a restriction, if:

- The individual agrees to or requests the termination in writing;
- The individual orally agrees to the termination and the oral agreement is documented; or
- The IDOH covered component informs the individual that it is terminating its agreement to a restriction, except that such termination is only effective with respect to PHI created or received after it has informed the individual.

Procedures and Responsibilities

Individuals will direct requests for restrictions of uses and disclosures to the Privacy Officer in writing. Any IDOH workforce member in a covered component who receives a request for restriction of PHI should forward it to the Privacy Officer. A request for restriction as allowed under this Policy must include the name and contact information of the requester, the name of the IDOH covered component affected by the restriction, and the disclosures that are to be restricted.

Once the Privacy Officer determines the request to be complete and verifies the requester's identity, the Privacy Officer will coordinate with the relevant covered component to determine whether or not the restriction request will be granted. The relevant covered component will

notify all affected business associates of any restriction requests granted by the covered component. The Privacy Officer will send a written response to the requester with the decision whether or not the IDOH covered component will grant a restriction request.

An IDOH covered component that agrees to a restriction must document the restriction for six years from the date of its creation or the date when it was last in effect, whichever is later.

Failure to comply with requirements of this policy may subject the employee to discipline, per the HIPAA Sanctions Policy.

Legal Authorities and References

- Laws
- Regulations
    - 31 IAC 5-12 – Disciplinary Actions & Separations
    - 45 CFR 164.502(c) – Uses and disclosures of protected health information subject an agreed upon restriction
    - 45 CFR 164.510(a) – Uses and disclosures requiring an opportunity for the individual to agree or to object
    - 45 CFR 164.512 – Uses and disclosures for which an authorization or opportunity to agree or object is not required
    - 45 CFR 164.522(a) – Rights to request privacy protection for protected health information
- PHAB Standards
- Related Policies
    - HIPAA Access Request for PHI Policy
    - HIPAA Permitted Uses and Disclosures of PHI Policy
    - HIPAA Sanctions Policy

Forms

N/A

F. Deceased Individuals Policy

Deceased Individuals Policy

Purpose

To issue instruction to all IDOH workforce members about the policy and procedures for acceptance of, response to, and documentation of requests for PHI for deceased members.

Policy Statement

The IDOH will protect the PHI of a deceased individual for 50 years as required by the HIPAA Privacy Rule.

The IDOH recognizes that an executor, administrator, or other persons, authorized by applicable law to act on behalf of a deceased individual or the deceased individual's estate, has the same rights that would have been accorded the individual. A designated personal representative of the deceased individual has the right to inspect and obtain a copy of the participant's PHI in the designated record set. The IDOH will require that a personal representative of the deceased participant make the request in writing. All requests for access received will be documented, reviewed, and answered within the timeframes required by the Privacy Rule.

IDOH covered components must comply with the requirements of the Privacy Rule with respect to the PHI of a deceased member. IDOH covered components are required to protect PHI about deceased members for as long as they maintain the information. The accounting of disclosures for a deceased participant's PHI is treated the same as a living participant's PHI. The decedent's personal representative has the right to request and receive the disclosure accounting.

Procedures and Responsibilities

IDOH covered components shall consult with the Privacy Officer regarding non-routine requests for PHI relating to deceased participants.

Failure to comply with requirements of this policy may subject the employee to discipline, per the HIPAA Sanctions Policy.

Legal Authorities and References

- Laws
- Regulations
    - 31 IAC 5-12 – Disciplinary Actions & Separations
    - 45 CFR 160 – General Administrative Requirements
    - 45 CFR 164 – Security and Privacy

- PHAB Standards
- Related Policies
    - HIPAA Sanctions Policy
    - IDOH Confidentiality Policy

Forms

N/A

G. De-Identified and Limited Data Policies

De-Identified Health Information Policy

Purpose

To ensure a consistent and efficient manner in the process of de-identification of PHI and the use of de-identified health information.

Policy Statement

Health information that meets the standards of de-identified health information is not individually identifiable health information. De-identified health information neither identifies nor provides a reasonable basis to identify an individual. IDOH covered components may use and disclose de-identified health information without restriction.

IDOH covered components may use PHI and disclose it to a business associate to create de-identified health information. IDOH covered components may assign a code or other means of record identification to allow de-identified health information to be re-identified, if

- the code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated to identify the individual; and
- the IDOH covered components do not use or disclose the code or other means of record identification for any purpose, and do not disclose the mechanism for re-identification.

Requirements for De-identification of Health Information: The IDOH determines that the requirements for de-identification of health information are satisfied if either of the following conditions is met:

1) A qualified statistician makes a formal determination that the risk is very small that the information could be used to identify the subject of the information; or

2) The removal of the following identifiers of the individual and of the individual's relatives, household members, and employers. This removal of specified identifiers is adequate only if IDOH covered components have no actual knowledge that the remaining information could be used to identify the individual.
   - Names
   - Geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geocodes (except for the first three digits of a zip code in specific circumstances)
   - All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
   - Telephone numbers
   - Fax numbers
   - Electronic mail (email) addresses
   - Social Security Numbers
   - Medical Record Numbers
   - Health plan beneficiary numbers
   - Account Numbers
   - Certificate/license numbers
   - Vehicle identifiers and serial numbers, including license plate numbers
   - Device identifiers and serial numbers
   - Web Universal Resource Locators (URLs)
   - Internet Protocol (IP) address numbers
   - Biometric identifiers, including finger and voice prints
   - Full face photographic images and any comparable images
   - Any other unique identifying number, characteristic, or code, except as otherwise permitted under the Privacy Rule.

Procedures and Responsibilities

Any IDOH covered component that receives a request for access to PHI that might require de-identification must forward the request to the Privacy Officer. If the Privacy Officer or designee determines that de-identification of the requested PHI is required before disclosure is permitted, the Privacy Officer or designee will coordinate with the affected IDOH covered component(s) to ensure that the de-identification is completed in compliance with the Privacy Rule. The Privacy

Officer or designee will review all de-identified health information prior to disclosure to ensure that all of the identifying data elements have been removed prior to release of the information.

The Privacy Officer has the discretion, as appropriate, to establish guidelines permitting an IDOH covered component to perform the de-identification of PHI, and to disclose that de-identified health information.

Failure to comply with requirements of this policy may subject the employee to discipline, per the HIPAA Sanctions Policy.

Legal Authorities and References

- Laws
- Regulations
  - 31 IAC 5-12 – Disciplinary Actions and Separations
  - 45 CFR 164.501 - Definitions
  - 45 CFR 164.514 – Other requirements relating to uses and disclosures of PHI
- PHAB Standards
- Related Policies
  - HIPAA Sanctions Policy

Forms

N/A

Limited Data Set Policy

Purpose

To ensure the creation and use of limited data sets created from PHI in a consistent manner.

Policy Statement

It is the policy of the IDOH to comply with all HIPAA regulations governing our duties and responsibilities. The IDOH workforce shall follow procedures established by the Privacy Officer and IDOH HIPAA Covered Components when developing or using limited data sets derived from PHI.

A limited data set is PHI that excludes the same direct identifiers that are excluded from de-identified health information, except for the following identifiers that can be included:

- town or city, state, and zip code; and

- elements of dates related to a person (e.g., years, birth dates, admission dates, discharge dates, and dates of death).

An IDOH covered component may use or disclose a limited data set derived from PHI only for the purposes of research, public health, or health care operations.

An IDOH covered component may use PHI to create a limited data set that satisfies the requirements of the Privacy Rule or may disclose PHI to a business associate for such purpose, whether or not the limited data set is to be used by the IDOH.

Recipients of IDOH limited data sets must enter into a data use agreement for the limited purposes described above. The data use agreement may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate the terms of the Privacy Rule if done by the IDOH covered component. The data use agreement also must establish who is permitted to use or receive the limited data set. In addition, the data use agreement must provide that the limited data set recipient will:

- not use or disclose the information other than as permitted by the agreement or as otherwise required by law;
- use appropriate safeguards to prevent uses or disclosures of the information that are inconsistent with the data-use agreement;
- report to the IDOH covered component, who is the source of the limited data set, any use or disclosure of the information that violates the agreement of which it is or becomes aware;
- ensure that any agents to whom it provides the limited data set agree to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and
- not attempt to re-identify the information or contact the individual.

If any of the PHI includes communicable disease information protected by IC 16-41-8-1, an epidemiologist must be consulted before release to ensure the information meets all confidentiality requirements of state law.

All requests for PHI must be reviewed by the Privacy Officer to determine if disclosure of the requested information is permissible under the Privacy Rule, or if the use or disclosure can be accomplished by the use of a limited data set.

Disclosure of a limited data set is not subject to the accounting of disclosures requirement. The limited data set disclosure is required to satisfy the minimum necessary standards of the Privacy Rule.

Procedures and Responsibilities

Any IDOH covered component that receives a request for access to PHI that might require disclosure through a limited data set must forward that request in writing to the Privacy Officer. If the Privacy Officer or designee determines that disclosure of the requested PHI requires the establishment of a limited data set, the Privacy Officer or designee will coordinate efforts with the affected IDOH covered component(s) to ensure that the limited data set is created, and a data use agreement established, in compliance with the Privacy Rule. The Privacy Officer or designee will review all limited data sets prior to disclosure to ensure that the specified direct identifiers have been removed.

The Privacy Officer has the discretion, when appropriate, to establish guidelines permitting an IDOH covered component to perform certain functions related to the creation of a limited data set, the entry into (or confirmation of) a data use agreement, and the disclosure of a limited data set to a recipient.

Failure to comply with requirements of this policy may subject the employee to discipline, per the HIPAA Sanctions Policy.

Legal Authorities and References

- Laws
  - IC 16-41-8 – Communicable Disease: Confidentiality Requirements
- Regulations
  - 31 IAC 5-12 – Disciplinary Actions & Separations
  - 45 CFR 164.501 - Definitions
  - 45 CFR 164.514 – Other requirements relating to uses and disclosures of protected health information
- PHAB Standards
- Related Policies
  - HIPAA De-identified Health Information Policy
  - HIPAA Sanctions Policy

Forms

N/A

H. Notice of Privacy Practices Policy

Notice of Privacy Practices Policy

Purpose

To issue instruction to IDOH workforce members about the policy and procedures relating to creation, revision, and mailing of the HIPAA Notices of Privacy Practices to IDOH participants.

Policy Statement

IDOH covered components are responsible for issuing a Notice of Privacy Practices (NPP) document to each participant in that covered component.

The NPP provides notice of the uses and disclosures of PHI that may be made by the covered component, the participant's rights, and the covered component's legal duties with respect to PHI. The NPP document for each IDOH covered component contains all information required by the Privacy Rule that is applicable to that entity. IDOH covered components shall use and disclose PHI consistently with their respective NPPs.

Procedures and Responsibilities

Initial NPPs were mailed in March 2003 to the most recent address on file for all individuals identified by IDOH covered components as enrolled program participants. Each IDOH covered component will follow its established procedures to ensure the provision of an NPP to all newly enrolled participants in the program.

A Spanish version of each covered component's NPP is available and will be provided upon a participant's request, as documented in both English and Spanish on the initial notice mailed to all participants. Each IDOH covered component with a web site that provides information about customer services or benefits has its NPP prominently posted and available, in English and Spanish, on that website.

IDOH covered components will provide a revised NPP document to all then-enrolled participants within 60 days of a material revision to the notice. At least once every three years, IDOH covered components will notify then-enrolled participants of the availability of the notice and how to obtain the notice.

Failure to comply with requirements of this policy may subject the employee to discipline, per the HIPAA Sanctions Policy.

Legal Authorities and References

- Laws
- Regulations
  - 31 IAC 5-12 – Disciplinary Actions & Separations
  - 45 CFR 160 – General Administrative Requirements
  - 45 CFR 164.520 – Notice of privacy practices for protected health information
- PHAB Standards
- Related Policies
  - IDOH Confidentiality Policy
  - HIPAA Sanctions Policy

Forms

N/A

I. Workforce Policies

Disclosures by Whistleblowers and Workforce Member Crime Victims Policy

Purpose

To issue instruction to IDOH workforce members about the policy and procedures relating to PHI disclosure by whistleblowers and workforce member crime victims.

Policy Statement

Disclosures by Whistleblowers: Workforce members in IDOH covered components, and their business associates, have the right to disclose PHI if they believe in good faith that another workforce member in an IDOH covered component or business associate has engaged in conduct that is unlawful or otherwise violates professional standards. It may also be that the services or conditions provided by the covered component or business associate endanger one or more participants, workers, or the public.

IDOH covered components and their business associates will not be considered to have violated the Privacy Rule if the disclosure is made to one of the following entities:

- A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the IDOH;
- An appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the IDOH; or

- An attorney retained by or on behalf of the workforce member or business associate to determine the legal options with regard to the conduct in question.

Disclosures by Workforce Member Crime Victims: A workforce member in an IDOH covered component who is a victim of a criminal act has the right to disclose PHI to law enforcement officials. Such a disclosure will not constitute a violation of the Privacy Rule by the IDOH if the following conditions apply:

- The PHI disclosed is about the suspected perpetrator of the criminal act; and
- The PHI disclosed is limited to the following information:
    - Name and address
    - Date and place of birth
    - Social Security Number
    - ABO blood type and rh factor
    - Type of injury
    - Date and time of treatment
    - Date and time of death, if applicable; and
    - A description of distinguishing physical characteristics.

IDOH covered components are not required to account for disclosures by whistleblowers and workforce member crime victims.

Procedures and Responsibilities

In addition to federal HIPAA protections, an IDOH workforce member in an IDOH covered component who considers himself or herself a whistleblower must follow IC 4-15-10-4 to receive protection under Indiana state law.

If an IDOH workforce member in an IDOH covered component considers himself or herself a workforce crime victim, he/she should consult immediately with one of the following:

- His/her immediate supervisor
- IDOH Human Resource Division (contact one of the following):
    - Labor Relations Manager
    - Affirmative Action Officer
    - Human Resource Director
- Privacy Officer

Upon disclosure of the whistleblower or workforce crime victim issue, the Privacy Officer or supervisor shall immediately notify the IDOH Human Resource Department who shall coordinate with the appropriate authorities in the investigation and resolution of the issue.

Failure to comply with requirements of this policy may subject the employee to discipline, per the HIPAA Sanctions Policy.

Legal Authorities and References

- Laws
  - IC 4-15-10-4 – Protection of employees reporting violations of state or federal laws
- Regulations
  - 31 IAC 5-12 – Disciplinary Actions & Separations
  - 45 CFR 160 – General Administrative Requirements
  - 45 CFR 164.502(j) – Uses and disclosures of protected health information: General rules
- PHAB Standards
- Related Policies
  - HIPAA Sanctions Policy
  - IDOH Confidentiality Policy

Forms

N/A

Sanctions Policy

Purpose

To establish a sanction policy for IDOH workforce members who fail to comply with IDOH policies and procedures established under the HIPAA Privacy and Security Rules.

Policy Statement

It is the policy of the IDOH to comply with all HIPAA regulations governing our duties and responsibilities. IDOH is required by the HIPAA Privacy Rule to establish and apply appropriate sanctions against members of its workforce who fail to comply with IDOH HIPAA policies. It is a condition of employment that the IDOH workforce complies with IDOH HIPAA policies regarding privacy and security.

Procedures and Responsibilities

Failure to comply with IDOH HIPAA policies will be addressed in accordance with the applicable union settlement, the State's policies as cited within IDOH Standardized Policies and Procedures, and/or other IDOH specific policies. Those authorities prescribe the procedures for investigation, standards for decision-making, and process for third party review of outcomes. Determinations

of the severity of misconduct (categorization as minor, serious, or severe) will include consideration of factors identified in the state and federal laws identified with this policy (e.g., severity, intent, and patterns). Sanctions for contracted staff should be based on the provisions indicated in the applicable contracts and/or agreements.

Federal penalties for violations of the HIPAA Privacy Rule can result in fines up to $250,000 and/or up to ten years imprisonment. Any potential violation of the IDOH HIPAA policies should be reported in writing by the next business day to the Privacy Officer for further investigation.

In accordance with the State's policies as cited within IDOH Standardized Policies and Procedures, all discipline shall be documented. Sanctions imposed by the IDOH for HIPAA violations must be documented. The Privacy Officer will retain a copy of documentation regarding any imposed sanctions for six years. A copy of the sanction imposed should also be added to the workforce member's file (as applicable for IDOH employees) within Human Resources.

The HIPAA regulations prohibit the imposition of sanctions in certain situations (e.g., disclosure by whistleblowers or workforce member crime victims, or as intimidating and retaliatory acts).

Failure to comply with the requirements of this policy may subject the employee to discipline.

Legal Authorities and References

- Laws
- Regulations
    - 31 IAC 5-12 – Disciplinary Actions & Separations
    - 45 CFR 160 – General Administrative Requirements
    - 45 CFR 164 – Security and Privacy
- PHAB Standards
- Related Policies
    - IDOH Confidentiality Policy

Forms

N/A

Workforce Training Policy

Purpose

To ensure that all members of the IDOH workforce are aware of HIPAA and obtain appropriate training regarding HIPAA regulations, and IDOH's HIPAA Policies.

Policy Statement

It is the policy of the IDOH to comply with all regulations governing our duties and responsibilities. We wish to ensure that the IDOH workforce understands the duties and responsibilities imposed on IDOH by HIPAA. All workforce members in IDOH covered components who may access, use, or disclose PHI will receive training on IDOH HIPAA Privacy Policies and Procedures, as necessary and appropriate for the workforce member to carry out his or her job functions.

Newly hired workforce members in IDOH covered components must receive privacy training before they may access, use, or disclose PHI. Ongoing privacy training will take place as needed due to changes in the Privacy Rule or IDOH privacy policies and procedures. Documentation confirming completion of training will be retained for six years.

It is a condition of employment that the IDOH workforce complies with all applicable HIPAA Regulations regarding privacy and security.

Procedures and Responsibilities

In order to comply with the HIPAA federal rules regarding privacy and security of health information, all members of the IDOH workforce must receive appropriate training on HIPAA. The Privacy Officer will work with HIPAA covered components of IDOH to ensure that required training is completed by IDOH covered components' staff through an acceptable medium (e.g., computer-based training, video, live presentation, text).

Failure to comply with the requirements of this policy may subject the employee to discipline, per the HIPAA Sanctions Policy.

Legal Authorities and References

- Laws
- Regulations
    - 31 IAC 5-12 – Disciplinary Actions & Separations
    - 45 CFR 160 – General Administrative Requirements
    - 45 CFR 164 – Security and Privacy

- 45 CFR 164.530 – Administrative requirements
- PHAB Standards
- Related Policies
  - HIPAA Sanctions Policy

Forms

N/A