



602 7TH STREET - ROOM 210
 PORTSMOUTH, OH 45662
 P: 740.355.8358
 F: 740.354.8623
SCHD@SCIOTOCOUNTY.NET

POLICY AND PROCEDURE	
SUBJECT/TITLE:	Employee HIPAA Protected Health Information and Privacy Policy
Distributed to:	All Employees
HEALTH COMMISSIONER	Michael E. Martin, M.D.
APPROVAL DATE:	2/14/2020
REVIEW FREQUENCY:	5 years
BOARD APPROVAL DATE:	N/A
REFERENCE NUMBER:	G-3

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) PRIVACY

Purpose: The purpose of the HIPAA Privacy Policy is to summarize, in writing, the methods and procedures that the Scioto County Health Department follows to assure compliance to federal laws regarding the protection of our clients' health information.

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 was introduced by the U.S. Department of Health and Human Services (HHS). As a requirement of HIPAA, the U.S. Department of Health and Human Services issued the Privacy Rules in order to develop standards to address the use and disclosure of individuals' Protected Health Information (PHI) when that information is stored, maintained, accessed, disclosed, or transmitted electronically. As an organization that must comply with the HIPAA Privacy Rule, this policy outlines our usage of and adherence to the HIPAA Privacy Rule.

Scope of this Policy:

As a provider of health care services who maintains and transmits health information in paper and electronic forms, the health district is considered a Covered Entity under HIPAA and must abide by the Privacy Rule requirements. Additionally, Business Associates should be aware of and should comply with the Privacy Rule. All health district employees and contracted individuals or groups are required to maintain compliance with the Privacy Rule, in regards to patient information, at all times.

Public Health Exception:

Under 45 CFR 164.512(b), the Privacy Rule permits covered entities to disclose protected health information, without the written consent of the individual or his/her authorized representative, both within and outside the health department, for the following purposes:

1. **Treatment:** The provision, coordination, or management of health care, health care services, or supplies related to an individual and related services by or among providers, providers and third parties, and referrals from one provider to another.
2. **Payment:** Activities undertaken by health district to obtain payment or determine responsibility for coverage, or activities of a health care to obtain reimbursement for the provision of health care.

- Payment activities include, but are not limited to, billing, claims management, collection activities, eligibility determination, and utilization review.
- 3. Health Care Operations: Activities of the health department to the extent such activities are related to the daily operations, including quality assessment and improvement activities; credentialing health care professionals; insurance activities; conducting or arranging for medical review; legal services and auditing functions, including compliance programs; business planning such as conducting cost-management and planning analyses to managing and operating the health district; business management and general administration activities; due diligence in connection with the sale or transfer of assets to a potential successor in interest if the potential successor is a covered entity or will become a covered entity; consistent with privacy requirements, creating deidentified health information, fundraising for the benefit of the covered entity and marketing for which an individual authorization is not required.
- 4. As required by, or to comply with, law.
- 5. For public health and safety activities.
- 6. About victims of abuse, neglect, or domestic violence.
- 7. To health oversight agencies in connection with health oversight activities.
- 8. For judicial and administrative proceedings, or to comply with a lawfully issued subpoena.
- 9. For law enforcement purposes.
- 10. Regarding decedents to coroners, medical examiners, and funeral directors.
- 11. For research if a waiver of authorization has been obtained.
- 12. To prevent serious and imminent harm to the health or safety of a person or the public.
- 13. For specialized governmental functions.
- 14. Military and veterans' activities.
- 15. National security and intelligence.
- 16. Protective services for the President and others.
- 17. To the Department of the State to make medical suitability determinations.
- 18. To correctional institutions and law enforcement officials regarding an inmate.
- 19. Workers' compensation if necessary to comply with the laws relating to workers' compensation and other similar programs.
- 20. To Business Associates for the purpose of assisting the health district in completing healthcare functions.
- 21. Immunization records may be provided to schools upon request for verification of immunization requirements.

Definitions:

- 1. Protected Health Information (PHI)— individually identifiable health information that can be linked to a particular person; such as, the patient's name, birth date, date of medical treatment, contact information, social security number, photographs, medical conditions and treatment, etc.
- 2. Covered Entity — A health care provider, health care clearinghouse or health plan that transmits health information in electronic form.
- 3. 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 involves the use or disclosure of individually identifiable health information.

Policy:

The Scioto County Health Department strives to protect the confidentiality, integrity and availability of clients' Protected Health Information by adhering to the requirements of HIPAA. The policies and rules outlined by HIPAA, when adhered to, maximize the security of individuals' health information. Clients' health information may be collected and used by doctors, nurses, technicians, volunteers/interns and other staff members in the course of business, and these individuals and/or groups are required to adhere to the policies and rules outlined by HIPAA. The health information used must be protected and utilized only as necessary. Staff members and other necessary individuals should be made aware of and have access to the Department of Health and Human Services' HIPAA Privacy Rule, any modifications to the Privacy Rule and the health district's Notice of Privacy Practices.

Procedure:

1. A Notice of Privacy Practices (NPP) will be maintained by the health department that outlines:
 - a. Patient's rights and allowable uses of their Protected Health Information as indicated by HIPAA.
 - i. The NPP will be made available to every client, and their acknowledgment of being offered a copy of the notice should be documented.
 - ii. The NPP will be updated, as needed, to align with changes and modifications to the HIPAA Privacy Rules and other applicable laws. The notice shall adequately inform individuals of their rights to:
 1. Request restrictions on certain uses and disclosures of PHI;
 2. Request the communication of confidential information by some reasonable alternative means or at an alternative location;
 3. Inspect and copy records or receive a summary of specific information;
 4. Request that PHI be amended;
 5. Request an accounting of certain disclosures of PHI; and
 6. Receive a paper copy of the notice upon request.
2. The health department shall take reasonable steps to limit the use and/or disclosure of and requests for PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request and to determine the extent to which various classifications of employees need access to such information. The health department shall also implement reasonable administrative, technical, and physical safeguards to protect Individually Identifiable health information from any intentional or unintentional use or disclosure and that mitigate, to the extent practicable, any harmful effect that is known to the health department as a result of a use or disclosure of PHI in violation of this policy or the HIPAA privacy and security standards. The health department's security measures shall include the following:
 - a. Administrative procedures to guard data integrity, confidentiality, and availability, including documented, formal practices to manage the selection and execution of security measures to protect data and to manage the conduct of personnel in relation to the protection of data;
 - b. Physical safeguards to protect data integrity, confidentiality, and availability including the protection of physical computer systems and related buildings and equipment from fire and other natural and environmental hazards and from intrusion and the use of locks, keys, and other administrative measures to control access to confidential files as well as computer systems and facilities;
 - c. Technical security services to protect data integrity, confidentiality, and availability including processes put in place to protect information and to control individual access to information;
 - d. Technical security mechanisms including processes put in place to protect against unauthorized access to data that is transmitted over a communications network; and
 - e. The optional use of an electronic digital signature.

3. The health department HIPAA Privacy Officer and the HIPAA Security Officer have general responsibility for and will oversee the development of the health department's HIPAA Privacy Policy and Notice of Privacy Practices. The officers will also ensure that the policies and procedures are up to date, by performing periodic reviews, and that staff members are fully aware of any changes made.
4. The health department shall not disclose PHI for purposes other than those set forth in the above policy without a valid authorization. A valid authorization is a document signed by the individual that gives the health department permission to use specified health information for a specified purpose and time frame. To be valid, an authorization shall contain at least the following elements:
 - a. A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;
 - b. The name or other specific identification of the person(s) or class of person(s) authorized to make the requested use or disclosure;
 - c. The name or other specific identification of the person(s) or class of person(s) to whom the health plan and/or the health department may make the requested use or disclosure;
 - d. An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure;
 - e. A statement of the individual's right to revoke the authorization in writing and the exceptions to the right to revoke, together with a description of how the individual may revoke the authorization;
 - f. A statement that information used or disclosed pursuant to the authorization may be subject to re-disclosure by the recipient and no longer be protected by this rule; and
 - g. Signature of the individual and date and, if the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual.
 - h. The health department shall offer the individual a copy of the signed authorization. An authorization for the use or disclosure of PHI may not be combined with any other document to create a compound authorization.
 - i. An authorization is not valid if the document submitted has any of the following defects:
 - i. The expiration date has passed or the expiration event is known to have occurred;
 - ii. Any required element is missing or has not been filled out;
 - iii. The authorization is known to have been revoked;
 - iv. The authorization has been improperly combined with another document;
 - v. The health department has violated the rules on making the authorization a condition; or
 - vi. Any material information in the authorization is known to be false.
 - j. An individual may revoke an authorization at any time, provided the revocation is in writing.
5. Prior to releasing any PHI for the purposes set forth above, the health department's representative disclosing the information shall verify the identity and authority of the individual to whom disclosure is made. This verification may include the examination of official documents, badges, driver's licenses, workplace identity cards, credentials, or other relevant forms of identification or verification.
6. Individuals shall have the following rights with regard to their PHI:
 - a. Access. Individuals shall have the right to access their own PHI that is maintained by the health department and its Business Associates.

- b. Restrictions. Individuals shall have the right to request restrictions on how the health department will use or disclose the individual's own PHI for treatment, payment or health care operations and how the individual's information will be disclosed or not disclosed to family members or others involved in the individual's care. The health department shall comply with the individual's reasonable request to receive communications of PHI by alternative means or at alternative locations.
- c. Amendment. Individuals shall have the right to amend erroneous or incomplete PHI unless the information:
 - a. Was not created by the health department;
 - b. Is not stored in the health department or is not otherwise available for inspection;
 - c. Is accurate and complete; or
 - d. Is not subject to the right of access.

A request to amend PHI must be submitted to the Privacy Officer in writing. The Privacy Officer shall review the request and respond in writing within thirty calendar days. If a request to amend is denied, the individual may appeal the denial using the complaint procedure set forth in this policy. The denial must be written in plain language and contain:

- i. The basis for the denial;
- ii. A statement of the individual's right to submit a written statement disagreeing with the denial and how it may be filed;
- iii. A statement that if the individual does not submit a statement of disagreement, his/her right to request that the request for amendment and its denial be provided with any future disclosure of the PHI that is the subject of the request for amendment;
- iv. A description of how the individual may appeal the denial; and
- v. The right of the health department to reasonably limit the length of the statement of disagreement.
- vi. The health department may also choose to prepare a written rebuttal to the statement of disagreement and provide a copy to the individual. All of the statements related to the amendment denial shall become part of the individual's record and shall be linked to the individual's PHI.
- d. Accounting. Individuals shall have the right to an accounting of disclosures of their own PHI that is maintained in their record of the health department and its Business Associates. Such accounting can include a period of six years prior to the request.

7. The health department may adopt corresponding policies and procedures, including necessary forms, to implement and administer these participant rights.

- a. Upon hire, all new staff will be oriented to the confidentiality and privacy policies, and will sign a confidentiality statement, to be maintained in the employee's personnel file.
- b. All students, interns, and/or volunteers affiliated with the Scioto County Health Department will be affiliated with the Confidentiality and HIPAA policies at the start of their affiliation, and will sign a confidentiality statement, to be maintained by the department supervisor.
- c. All health department personnel that handle patients' confidential health information will undergo annual training in confidentiality and HIPAA privacy policy. The training provided will be determined by the Director of Nursing or the HIPAA Privacy Officer. A record of completed annual training will be maintained in each staff member's personnel file.
- d. Upon termination, resignation or separation of service the employee will be removed from all data systems by the Security Officer to avoid loss of data.
- e. All leased equipment and other IT devices that are to be returned or destroyed will have the memory or hard disks wiped or destroyed.

8. The health department, its officers, employees, and agents shall not disclose PHI to any Business Associate in the absence of a written contract with the Business Associate that assures that the Business Associate will use the information only for the purposes for which it was engaged by the health district; will safeguard the information from misuse; and will assist the health district in complying with its duties to provide individuals with access to health information about them and a history of certain disclosures. The health department shall disclose PHI to a Business Associate for the sole purpose of assisting the health department in completing healthcare functions (for example, insurance billing), not for the independent use by the Business Associate.
9. The health department shall enter into a contract with each Business Associate, which shall be a document separate from the service agreement, if any. The nursing department billing clerk shall be responsible for managing all Business Associate contracts and ensuring that they are current and in compliance with the requirements of this policy and HIPAA.
 - a. All employees and Business Associates shall receive training regarding the health department privacy policies and procedures as necessary and appropriate to carry out their job duties as they may relate to the administration of the Plan. Training shall also be provided when there is a material change in the health department's privacy practices or procedures.
 - b. Documentation shall be maintained in support of the policies and procedures of the health district, consistent with the parts of HIPAA privacy regulations that directly require documentation, including, but not limited to, all authorizations and revocations of authorizations and complaints and disposition of complaints. All documentation shall be kept in written or electronic form for a period of six years from the date of creation or from the date when it was last in effect, whichever is later.
 - c. The HIPAA compliance officers will conduct risk assessment and security analysis yearly, complete HIPAA security evaluation, document and act upon a remediation plan.
10. Client complaints concerning HIPAA issues will be directed to either the HIPAA Privacy or Security officer. If the Privacy/Security Officer determines that there has been a breach of this privacy policy or the procedures of the health department, he/she shall make a determination of the potential harmful effects of the unauthorized use or disclosure and decide upon a course of action to minimize the harm. Any individual responsible for the unauthorized use or disclosure shall be referred to the Health Commissioner for appropriate disciplinary action and to the supervisor and/or Privacy/Security Officer for additional training, if applicable. If the Privacy/Security Officer or a Business Associate determines that there has been a breach of unsecured PHI, as defined in the HI TECH Act, the health department and/or the Business Associate shall provide the required breach notifications to impacted individuals, the media and the Secretary of Health and Human Services, as necessary and required.
11. Violations of the HIPAA privacy or security policies are subject to disciplinary action. Additionally, any complaints or concerns in regards to violations of HIPAA should be brought to the attention of the Privacy/Security Officer. There will be no attempts made to retaliate against or punish a person for reporting a violation.

RESPONSIBILITY: HIPAA Privacy Officer, HIPAA Security Officer

SUPPLIES: Notice of Privacy Practices

RELATED POLICIES: Confidentiality

PERFORMED BY: All health department classified and unclassified employees, contractors, students, interns and volunteers

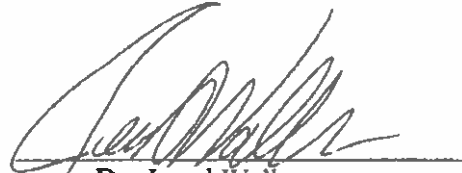


612 6TH STREET, SUITE D
PORTSMOUTH, OH 45662
P: 740.355.8358
F: 740.354.8623
SCHD@SCIOTOCOUNTY.NET
SCIOTOCOUNTYHEALTH.COM

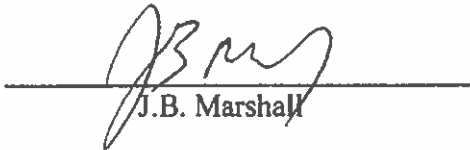
Board Approval:



Laura Miller,
Board President



Dr. Jerod Walker




J.B. Marshall



Christy Sherman

Sean Sturgill



Dr. Michael Martin,
Health Commissioner

Date: 2/4/2020