
Ohio Network for Innovation

# [HIPAA POLICY MANUAL]

*Policies governing confidentiality of the information regarding the Individuals we serve, their privacy rights, and our computer security.*

ADOPTED: January 2024

REVISED:

# Contents

# INTRODUCTION

## Health Insurance Portability and Accountability Act of 1996 (HIPAA)

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations restrict ONI's abilities to use and disclose protected health information (PHI). The Health Insurance Portability and Accountability Act of 1996 (HIPAA) details the following:

| | |
|---|---|
| HIPAA Privacy Rule | Patients must have access to and control over their own health information, and covered entities must have measures to protect that data and the transmission of that data. |
| HIPAA Security Rule | Healthcare providers and covered entities must meet the administrative, physical, and technical standards for the storage and protection of PHI and ePHI. |
| HIPAA Omnibus Rule | All HIPAA-covered entities must provide a notice of privacy practices to their patients. |
| HIPAA Breach Notification Rule | Covered entities are required to notify individuals when there is an unauthorized use or disclosure of their PHI. |
| HIPAA Enforcement Rule | Covered entities must have a process in place to investigate and address any complaints of noncompliance. |

Individuals have the following rights regarding their medical information:

- to request to inspect and obtain a copy of their medical records, subject to certain limited exceptions;
- to request to add an addendum to or correct their medical record;
- to request an accounting of ONI's disclosures of their medical information;
- to request restrictions on certain uses or disclosures of their medical information;
- and to request that we communicate with them in a certain way or at a certain location.

*Protected Health Information (PHI).* Protected health information means information that is created or received by ONI and relates to the past, present, or future physical or mental health 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 for which there is a reasonable basis to believe the information can be used to identify the Individual. Protected health information includes information of persons living or deceased.

Some examples of PHI are:

- Individual's medical record number
- Individual's demographic information (e.g. address, telephone number)
- Information doctors, nurses and other health care providers put in an Individual's medical record
- Images of the Individual
- Conversations a provider has about an Individual's care or treatment with nurses and others
- Information about an Individual in a provider's computer system or a health insurer's computer system
- Billing information about an Individual
- Any health information that can lead to the identity of an Individual or the contents of the information can be used to make a reasonable assumption as to the identity of the Individual

## ONI's HIPAA Policy

The policies set forth and adopted within this HIPAA Policy Manual supersede all previous written and unwritten HIPAA policies of ONI except as specifically delineated by the Executive Director.

This HIPAA Policy Manual is to comply with the Administrative Safeguards of HIPAA Privacy, to secure and maintain the confidentiality of Protected Health Information, maintain sensitive organizational information at ONI and prevent and detect inappropriate and illegal uses and disclosures. In the event there is a conflict between the contents of this HIPAA Policy Manual or any applicable laws, those applicable laws shall prevail.

This HIPAA Policy Manual is designed as a tool and guide for supervisors and staff. Questions regarding the interpretation and application of these policies should be directed to your supervisor who will seek clarification through the chain of command. Every effort will be made to ensure that such decisions are made objectively, with the general intent of the policy in mind. Detailed procedures regarding HIPAA policies are available in the HIPAA Procedures Manual.

As conditions shift within ONI or the law, it may be necessary to add, delete or revise specific policies affected by such change. Updated policies will be communicated, and employees may be asked to sign an Acknowledgement of HIPAA Policies and Procedures form. Upon hire, employees shall be asked to sign an Acknowledgement of HIPAA Policies and Procedures form as documentation that they have received and read the HIPAA Policy Manual.

## OBJECTIVES

ONI recognizes that a personnel system that recruits and retains competent, dependable personnel is indispensable for the effective delivery of services served by ONI.

The policies and procedures set forth in this HIPAA Policy Manual are designed:

1. To set forth the standards currently established by ONI for the work carried out by the employees.
2. To ensure that all operations and programs are conducted in an ethical and legal manner to promote ONI's reputation as an efficient, progressive organization with its customers.
3. To comply with the Administrative Safeguards of HIPAA Privacy, the HITECH Act of 2009, the Breach Notification Rule, the HIPAA Omnibus Rule, and the Ohio Revised Code.
4. To secure and maintain the confidentiality of Protected Health Information, maintain sensitive organizational information, and prevent and detect inappropriate and illegal uses and disclosures of such information.

## DISCLAIMER

This HIPAA Policy Manual is not a contract, either expressed or implied. ONI reserves the right to change any policy without consultation or notice. Any statements in conflict with these policies made by anyone else are unauthorized, expressly disallowed, and should not be relied upon by anyone.

# DEFINITIONS

The following terminology is used throughout these HIPAA Policies.

The definitions below are adapted from the federal HIPAA regulations and Ohio Revised Code (ORC). Definitions from ORC § 5126.044, the Ohio law on confidentiality (effective 9/22/2000) for County Boards of DD and their service providers are also included. Definitions from HIPAA for "treatment", "payment" and "Individual" are modified based on this ORC citation.

| Term | Meaning |
|---|---|
| *Shall, must and/or will* | The behavior is mandatory |
| *Should* | The behavior is a best practice, is recommended and usually expected, although it is not mandatory |
| *May* | The behavior is optional, and the individual is empowered to take the specific action |

1) **Access** – ability or means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.
2) **Administrative Safeguards** – administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information (ePHI), and to manage the conduct of the Covered Entity's workforce in relation to the protection of that information.
3) **Applicable Requirements** – applicable federal law and contracts between ONI and other persons or entities which conform to federal law.
4) **Authentication** – confirmation that a person is the one claimed.
5) **Availability** – the property that data or information is accessible and usable upon demand by an authorized person.
6) **Breach** – the acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted by the HIPAA Privacy Rules which compromises the security or privacy of the protected health information.
    a) Breach *excludes*:
        i) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a Covered Entity or a Business Associate, if such acquisition, access, or use was made in good faith and within the scope of authority

and does not result in further use or disclosure in a manner not permitted by the HIPAA Privacy Rules.

ii) Any inadvertent disclosure by a person who is authorized to access protected health information at a Covered Entity or Business Associate to another person authorized to access protected health information at the same Covered Entity or Business Associate, or organized healthcare arrangement in which the Covered Entity participates, and the information received as a result of the disclosure is not further used or disclosed in a manner not permitted by the HIPAA Privacy Rules.

iii) A disclosure of protected health information where a Covered Entity or Business Associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

b) Except for the exclusions above, any unintentional acquisition, access, use, or disclosure of PHI that is a violation of the Privacy Rule is PRESUMED TO BE A BREACH, unless a risk assessment demonstrates that there is a low probability that the PHI has been compromised. The risk assessment must include at least the following factors:

i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification.

ii) The unauthorized person who used the PHI or to whom the disclosure was made.

iii) Whether the PHI was acquired or viewed; and

iv) The extent to which the risk to the PHI has been mitigated.

7) **Business Associate (BA)** – a Business Associate is a person or entity which creates, uses, receives, or discloses PHI held by a Covered Entity to perform functions or activities on behalf of the Covered Entity.

a) DD COGs are Business Associates of their County Board members. A subcontractor of a Business Associate can also be a Business Associate. COGs are obligated to identify and place any "Business Associate" under a contract that meets the specifications of the HIPAA regulations. Business Associates are directly regulated by the HIPAA regulations and are subject to the same civil and criminal penalties for any failures to comply with the portions of the HIPAA regulations that apply to them.

8) **Confidentiality** – The property that data or information is not made available or disclosed to unauthorized persons or processes.

9) **Covered Entity** – a health plan, healthcare clearinghouse, or healthcare provider who transmits any health information in electronic form in connection with a transaction covered by HIPAA Privacy Rules.
    a) DD COGs are *Business Associates* of their County Board members.
10) **Destruction** – physical destruction of a record or removal of personal identifiers from information so that the information is no longer personally identifiable.
11) **Disclosure** – the release, transfer, provision of access to, or divulging in any manner (orally, written, electronically, or other) of information outside the Entity holding the information.
12) **Employee** – any person employed by ONI, volunteers, interns, board members, and other persons whose conduct, in the performance of work for ONI, is under the direct control of ONI, whether they are paid by ONI.
13) **Encryption** – the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.
14) **Facility** – the physical premises and the interior and exterior of a building(s).
15) **Family Member** – with respect to an individual:
    a) A dependent (as such term is defined in 45 CFR 144.103), of the individual; or
    b) Any other person who is a first-, second-, third-, or fourth-degree relative of the individual or of a dependent of the individual. Relatives by affinity (such as by marriage or adoption) are treated the same as relatives by consanguinity (that is, relatives who share a common biological ancestor). In determining the degree of the relationship, relatives by less than full consanguinity (such as half-siblings, who share only one parent) are treated the same as relatives by full consanguinity (such as siblings who share both parents).
    c) First-degree relatives include parents, spouses, siblings, and children.
    d) Second-degree relatives include grandparents, grandchildren, aunts, uncles, nephews, and nieces.
    e) Third-degree relatives include great-grandparents, great-grandchildren, great aunts, great uncles, and first cousins.
    f) Fourth-degree relatives include great-great grandparents, great-great grandchildren, and children of first cousins.
16) **Healthcare Operations** – any of the following activities of the Covered Entity to the extent that the activities are related to covered functions:

a) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in 42 CFR 3.20); population-based activities relating to improving health or reducing healthcare costs, protocol development, case management and care coordination, contacting of healthcare providers and patients with information about treatment alternatives; and related functions that do not include treatment;

b) Reviewing the competence or qualifications of healthcare professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of healthcare learn under supervision to practice or improve their skills as healthcare providers, training of non-healthcare professionals, accreditation, certification, licensing, or credentialing activities.

c) Except as prohibited under §164.502(a)(5)(i), underwriting, enrollment, premium rating, and other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for healthcare (including stop-loss insurance and excess of loss insurance), provided that the requirements of §164.514(g) are met, if applicable;

d) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs.

e) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development, or improvement of methods of payment or coverage policies; and

f) Business management and general administrative activities of the entity, including, but not limited to:

   i) Management activities relating to implementation of and compliance with the requirements of this subchapter.

   ii) Resolution of internal grievances.

   iii) The sale, transfer, merger, or consolidation of all or part of the Covered Entity with another Covered Entity, or an Entity that following such activity will become a Covered Entity and due diligence related to such activity; and

   iv) Consistent with the applicable requirements of §164.514, creating de-identified health information or a limited data set, and fundraising for the benefit of the Covered Entity,

17) **HIPAA** – the Health Insurance Portability and Accountability Act of 1996, cited in Pub.L. 104–191 and 110 Stat. 1936 and its regulations in 45 CFR Parts 160, 162 and 164.

18) **HIPAA Officer(s)** – individual(s) responsible for HIPAA policies and procedures as outlined. May also be called HIPAA Officer.

19) **Incidental Disclosure** – an unintentional disclosure of PHI that occurs as a result of a use or disclosure otherwise permitted by the HIPAA Privacy Rule. An Incidental Disclosure is NOT a violation of the Privacy Rule. However, for incidental disclosures to not be a violation, the Covered Entity must be in compliance with the requirement for implementation of the minimum necessary principle, and also in compliance with the requirement to implement physical, technical, and administrative safeguards to limit incidental disclosures.

20) **Individual, Individual receiving services, or Individual served** – Means a person who receives services from ONI, or a County Board served by ONI. [This shall have the same meaning as "Eligible person" as in section ORC 5126.03.] Note that parents or minors, guardians and other "personal representatives" may exercise any right or privilege available to an Individual served.

21) **Individually Identifiable Health Information** – the subset of health information, including demographic information, collected from an individual, and

    a) Is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse; and

    b) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual; and

        i) That identifies the individual; or

        ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

22) **Information System** – an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

23) **Integrity** – the property that data or information have not been altered or destroyed in an unauthorized manner.

24) **Malicious Software** – software, for example, a virus, designed to damage or disrupt a system.

25) **Manifestation or manifested** – with respect to a disease, disorder, or pathological condition, that an individual has been or could reasonably be diagnosed with the disease, disorder, or pathological

condition by a healthcare professional with appropriate training and expertise in the field of medicine involved. For purposes of this subchapter, a disease, disorder, or pathological condition is not manifested if the diagnosis is based principally on genetic information.

26) **Marketing** –

a) Except as provided in paragraph (B) of this definition, marketing means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.

b) Marketing does not include a communication made:

i) To provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by the Covered Entity in exchange for making the communication is reasonably related to the Covered Entity's cost of making the communication.

ii) For the following treatment and healthcare operations purposes, except where the Covered Entity receives financial remuneration in exchange for making the communication:

(1) For treatment of an individual by a healthcare provider, including case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, healthcare providers, or settings of care to the individual.

(2) To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the Covered Entity making the communication, including communications about: the entities participating in a healthcare provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; or

(3) For case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.

27) **ORC –** Ohio Revised Code

28) **Parent** – either parent. If the parents are separated or divorced, "parent" means the parent with legal custody of the child. "Parent" also includes a child's guardian, custodian, or parent surrogate. At age eighteen, the participant must act in his or her own behalf, unless he/she has a court-appointed guardian

29) **Password** – confidential authentication information composed of a string of characters.

30) **Patient** – has the same meaning as "Individual" or Individual Served". [While the term "patient" is not typically used in the context of DD services, the term is retained since some definitions from the HIPAA regulations use this term.]

31) **Payment** – means, in the context of a DD COG,:

a) Both:

i) Activities undertaken by a County Board, COG, or other service provider to obtain reimbursement for services rendered, for example, from Medicaid, for services provided to Individuals by a County Board, COG, or other service provider.

ii) Activities undertaken by a County Board to provide reimbursement to providers under contract with the County Board.

b) The activities in paragraph (a) of this definition relate to the Individual to whom health care is provided and include, but are not limited to:

i) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;

ii) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;

iii) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;

iv) Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services.

32) **Personal Representative** – a person who has authority under applicable law to make decisions related to healthcare on behalf of an adult or an emancipated minor, or the parent, guardian, or other person acting *in loco parentis* who is authorized under law to make healthcare decisions on behalf of an unemancipated minor, except where the minor is authorized by law to consent, on his/her own or via court approval, to a healthcare service, or where the parent, guardian, or person acting *in loco parentis* has assented to an agreement of confidentiality between the healthcare provider and the minor.

33) **Physical Safeguards** – are physical measures, policies, and procedures to protect a Covered Entity's electronic information systems, and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

34) **Portable Devices** – electronic or mobile devices including but not limited to the following: smart phones, tablets, flash memory devices (e.g. USB flash drives, personal media players), portable hard disks, and laptop/notebook/netbook computers.

35) **Protected Health Information or PHI** – PHI, short for "Protected Health Information," means individually identifiable health information that is: (i) transmitted by electronic media; (ii) maintained in electronic media; or (iii) transmitted or maintained in any other form or medium. PHI does not include (i) information in employment records held by a Covered Entity in its role as an employer or (ii) Records of individuals deceased for more than 50 years.

36) **Provider** – a person or Entity which is licensed or certified to provide services, including but not limited to healthcare services. This includes physicians, hospitals, home health agencies, ambulance companies, physical therapists, nurses, and any other licensed individual or Entity who provides "healthcare". A Covered Provider is a healthcare provider who transmits any health information in electronic form.

37) **Public Health Authority** – an ONI or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public ONI, including the employees or agents of such public ONI or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

38) **Security or Security Measures** – all of the administrative, physical, and technical safeguards in an information system.

39) **Security Incident** – the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information, or interference with system operations in an information system.

40) **Social Engineering** – "an outside hacker's use of psychological tricks on legitimate users of a computer system, in order to obtain information he needs to gain access to the system" (Palumbo), or "getting needed information (for example, a password) from a person rather than breaking into a system" (Berg). Social engineering is generally a hacker's clever manipulation of the natural human tendency to trust. The hacker's goal is to obtain information that will allow him/her to gain unauthorized access to a valued system and the information that resides on that system.

41) **Subcontractor** – a person to whom a Business Associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such Business Associate.

42) **System Owner** – means the individual in an organization with primary accountability for the use and operation of a software application. The specific duties of the System Owner may be defined in the organization's system and data governance policy.

43) **Technical Safeguards** – the technology and the policies and procedures for its use that protect electronic protected health information and control access to it.

44) **TPO** – treatment, payment, or healthcare operations under HIPAA Rules.

45) **Treatment** – means the provision, coordination, or management of services by a County Board or other provider to an Individual. This definition includes the coordination or management of support services; consultation between the County Board, the COG and support service provider relating to an Individual; or the referral of an Individual from one service provider to another.

46) **Unsecured Protected Health Information** – protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized patients using a technology or methodology in guidance specified by the Secretary of the Department of HHS in guidance published on the HHS Web site.

47) **Use** – with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

48) **User** – a person or entity with authorized access.

49) **Violation** – there are different types of violations, with different contexts:

    a) Privacy Violation. Making a use or disclosure of PHI not permitted by HIPAA policies, the violation of a patient right established by HIPAA, or the failure to perform an administrative procedure required by the HIPAA regulations.

    b) Employee Security Procedure Violation. The failure of an employee to comply with one or more of the policies and procedures described in the HIPAA Security Policies section of the policies and procedures manual.

50) **Workstation** – an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

# 100 HIPAA – GENERAL RULES

1) Staff of ONI may use or disclose PHI only as follows:
    a) For treatment, payment, or healthcare operations. An employee may only use or disclose PHI for an Individual when they are involved in the delivery of services relating to this Individual on behalf of a community partner.
    b) To the Individual.
    c) In accordance with an authorization to release information of the Individual with policies and procedure outlined in this HIPAA Policies Manual and the HIPAA Procedures Manual.
2) The minimum amount of information necessary shall be used or disclosed for any task.
3) Employees are responsible for safeguarding the information regarding Individuals as detailed in the company policy and procedures.
    a) As such, upon hire, staff will review and sign a HIPAA Policy Manual acknowledgement and complete annual training.
    b) Any updates to the HIPAA policy will be communicated with staff members with subsequent training(s), policy review, and/or policy acknowledgement.
4) Rights of Individuals served by ONI's member community partners may be exercised by parents, guardians, and personal representatives as detailed in the company policy and procedures.
5) Employees must review the entire HIPAA Policy Manual and follow any policy relevant to their job duties.
6) Employees must not use PHI for marketing purposes or to sell PHI to third parties.
7) ONI shall maintain appropriate physical, technical, and administrative safeguards to secure paper and oral PHI.

# 200 COMPLIANCE

## DOCUMENTATION

Required documentation of compliance activities, such as incident reports and complaints, shall be maintained by the designated HIPAA Officer(s).

## RETENTION OF POLICIES AND PROCEDURES

The HIPAA Officer(s) shall maintain HIPAA Policies and Procedures to be sufficient for compliance with the HIPAA Privacy, HIPAA Security, and HIPAA Breach Notification regulations. Policies must be reviewed and updated annually and updated as necessary in response to environmental or

operational changes which affect the security of ePHI. Policies shall be made available to all staff. A 6-year audit trail of these HIPAA Policies shall be maintained.

### REPORTING

Any employee who becomes aware of a violation or potential violation of ONI's HIPAA policies and procedures must report the violation to his/her supervisor. Any employee who becomes aware of a potential security incident must immediately report the incident. Employees who violate these policies and procedures are subject to sanctions.

1. Upon learning of an incident, the HIPAA Officer(s) and/or other individuals responsible shall follow ONI procedures relating to security incident response.
2. If a security incident is determined to be a breach, ONI shall notify its clients regarding breaches of protected health information in accordance with identified procedures.
3. ONI will mitigate, to the extent reasonable and practical, harm that is done to Individuals as a result of our violations of these HIPAA policies.

# 300 HUMAN RESOURCES AND ACCESS CONTROL

1. ONI shall manage the employee onboarding, offboarding, and job change processes with attention to the HIPAA requirements, rules, and regulations, as well as ONI's policy and procedures.
2. ONI will conduct training for staff to ensure effective operation of its security program, including, but not limited to, HIPAA policies, cybersecurity awareness, and role-based training upon hire, annually, and when deemed necessary based on updates to national and/or state rules, regulations, and guidelines.
3. Access to PHI will be granted based on the employee's or contractor's role. The HIPAA Officer(s) shall ensure that appropriate access controls are configured in all ONI systems.
4. System access will be granted to employees in a manner consistent with the HIPAA minimum necessary principle and the need-to-know principle. System access will be granted only upon request from an authorized individual. Access terminations will be handled promptly. The HIPAA Officer(s) may deviate from established procedures in the event of an emergency.

# 400 ACCEPTABLE USE OF COMPUTER SYSTEMS AND DEVICES

Each staff member is responsible for understanding and following ONI guidelines regarding permitted and acceptable use of ONI's IT resources under ONI's policy manual under *Use of Equipment*.

## PORTABLE DEVICES

Employees using portable devices must follow these safeguards:

1. Keep equipment with you at all times or store them in a secured location when not in use. Do not leave devices unattended in public locations (coffee shops, libraries, restaurants, conferences, unattended vehicles).
2. Employees must not use standard text messaging to transmit PHI. Only the use of apps approved by ONI for transmitting PHI may be used to transmit PHI.

## INTERNET USE

Employees shall be cautious and follow ONI policy and procedures when downloading and installing programs. If an employee has questions, they shall be directed to the HIPAA officer or Information Technology. Employees must not download, view text or images, or otherwise engage in communications which involve pornographic or racist materials; obscene material, derogatory, inflammatory or profane material; any other objectionable material. Copyrighted materials such as software or music files must not be downloaded in violation of copyright law.

## EMAIL USE

**1.** Any email containing PHI or confidential information should be encrypted using Microsoft Outlooks Encryption Service (OME). Alternative methods to transmit this information are acceptable, such as the use of Microsoft OneDrive, when necessary precautions are in place.

**2.** Whenever possible, avoid transmitting highly sensitive PHI by email.

3. Limit the information provided via email to the minimum necessary.

**4.** Use of standard email to transmit any PHI is prohibited except in the limited case specified in the HIPAA regulations and outlined in the company policy and procedures, such as when an Individual requests that an electronic copy of their record be sent via email. Be sure to include a privacy statement notifying the recipient of the insecurity of email and providing instructions for any misdirected messages.

**5.** For example: Please be aware that e-mail communication can be intercepted in transmission or misdirected. Please consider communicating any sensitive information by telephone, fax, or mail.

**6.** Use only ONI-supplied e-mail accounts, including Microsoft and G-mail. The use of internet-based e-mail accounts such as Yahoo mail is prohibited.

**7.** Individuals served can send their own information in any way that they deem appropriate, which may include unencrypted email. When a ONI staff member is responding to an individual's unencrypted email, they can:

8. Respond to the individual using encrypted email.
9. Respond to the individual using unencrypted email without including any PHI, which may involve deleting any PHI that the individual sent initially. In the initial response, it would be advisable to confirm that the patient would like to continue sending PHI via unencrypted email.

## USER IDS, PASSWORDS, AND MULTI-FACTOR AUTHENTICATION

1. Each employee is assigned their own account/User ID for each IT asset that they access. Inappropriate use of IT assets attributable to an employee's User ID may result in employee sanctions, including termination, and in the event of violation of laws, civil and criminal prosecution.
2. Multi-Factor Authentication (MFA) and/or Single Sign-On technology must be used as appropriate for access to sensitive information, such as banking or financial data.
3. For laptops and computer applications, the use of RoboForm Password Manager is required for all passwords. It is recommended to use the Password Generator to develop secure passwords. Employees accessing secure information shall have RoboForm downloaded to their phone and RoboForm shall be used to store all passwords.
4. Users are not permitted to allow others to access systems with their User ID. If a password is shared between multiple users, it shall be shared via RoboForm.
5. Should a password be compromised in any manner, the employee should use RoboForm Password Manager to update their password.

## DATA STORAGE IN APPROVED LOCATIONS

All data must be stored on an approved server, cloud service, or other approved location. Data includes but is not limited to word processing files, spreadsheets, and other files. Please note that data saved to your computer alone is not backed up and, should something occur, may not be retrievable.

## ONI-APPROVED APPS AND CLOUD SERVICES ONLY

Employees must use only ONI-approved smartphone tablet/apps and/or cloud services for any function, including but not limited to instant messaging.

## ONI-APPROVED HARDWARE ONLY

Only ONI-approved and ONI-installed hardware should be utilized. Should additional hardware be needed during the course of your duties, please contact IT. Personally owned smartphones, laptops, and tablets may be used only as detailed by the company policy and procedures.

### STORAGE OF PHI OR CONFIDENTIAL MATERIAL TO REMOVABLE MEDIA OR UNAUTHORIZED CLOUD SERVICE PROHIBITED.

Personnel may not copy to removable media, such as Flash drives, CDs, DVD, portable hard drives or unauthorized cloud service, any ONI confidential information or Protected Health Information, except when specifically authorized for ONI purposes.

### ALL USAGE IS LOGGED

ONI reserves the right to monitor all usage of ONI devices through the logging and storage of all activity, including emails, websites browsed, and other activity. All logs of employee activity are property of ONI. Employees will be held accountable for all computer usage performed using their User IDs.

# 500 SOCIAL MEDIA

1. Under no circumstances may PHI be posted or shared on social media.
2. Employees must not use social media for ONI communications involving PHI. Use of personal social media for any communications of ONI business matters is discouraged.
3. ONI expects employees to maintain an acceptable professional boundary with Individuals served and their families.

# 600 INTERACTIONS WITH AND RECORDS OF INDIVIDUALS SERVED

### VERIFICATION

ONI and its employees will take reasonable steps to verify the identity and the authority of the person requesting protected health information (PHI) for an Individual.

### SPEAKING WITH THE FAMILY AND FRIENDS OF INDIVIDUALS

Staff may disclose protected health information (PHI) to family, friends and other individuals involved with the care of an Individual, in specific situations, in accordance with ONI's policies and procedures.

### MINORS, PERSONAL REPRESENTATIVES, GUARDIANS, AND DECEASED INDIVIDUALS

All staff will follow appropriate guidelines in situations with Individuals who are minors or are deceased, and when dealing with their "Personal Representative(s)" or Guardian(s). A Personal Representative(s) has the same authority as the Individual to access the Individual's records, to authorize release of PHI, and to exercise any other rights granted to an Individual under the HIPAA regulations.

ONI recognizes the following persons to be personal representatives:

The parent of a child younger than 18 years old, except if:

State law allows the minor to consent to treatment without parental approval, and the

adolescent exercises this right,

When someone other than the parent is authorized by law (such as a court) and consents to the provision of care,

When the parent agrees to allow a healthcare provider to have a confidential relationship with their child,

The non-custodial parent of a child younger than 18 years old,

An individual who is recognized through durable power of attorney to have authority to act on the behalf of the Individual,

The legal guardian of the Individual,

If the Individual is deceased, a person with legal authority to act on behalf of the decedent or the estate,

Any other person authorized by law.

PHI can be disclosed for deceased individuals according to ONI procedures and verification of identity.

## DISCLOSURES REQUIRED OR PERMITTED BY LAW

ONI employees may use and disclose PHI in specific situations authorized by state and federal statute. In these cases, the Individual's authorization is not required. Staff will carefully follow specific requirements for these unusual and infrequent disclosures. These disclosures include:

a) Health oversight activities, such as investigations, audits, and inspections

b) Judicial and administrative proceedings

c) Law enforcement purposes

d) Research

e) Specialized government functions

f) Workers' compensation or other similar programs if applicable.

## RIGHT OF INDIVIDUAL SERVED TO ACCESS RECORDS

ONI will cooperate with community partners to ensure that Individuals are provided access to any information maintained by ONI which is in a community partner's designated record set. ONI personnel will provide information directly to Individuals only as expressly permitted in the written MOU with community partner.

### RIGHT OF INDIVIDUAL SERVED TO REQUEST AMENDMENT OF RECORDS

An Individual has the right to request correction of errors in a community partner's records about an Individual. When ONI services to a community partner involve maintaining official records for an Individual, ONI personnel will cooperate with the community partner process for correcting record inaccuracies.

### RIGHT OF INDIVIDUAL SERVED TO RECEIVE AN ACCOUNTING OF DISCLOSURES

ONI shall cooperate with its community partners in fulfilling any Individual requests in accordance with the Individual rights granted by HIPAA to provide an Accounting of Disclosures.

# 700 BUSINESS ASSOCIATE CONTRACTS

ONI will obtain satisfactory assurance that Business Associates will appropriately safeguard PHI.

All HIPAA Business Associate Agreements and service agreements with community partners shall be reviewed and HIPAA Officer(s) shall take any necessary steps to ensure compliance with both. ONI will use best practices when accessing electronic record and/or billing software of community partners.

# 800 SECURITY

### FACILITY

All employees shall be aware of and follow facility security and access policies to ensure that only authorized personnel have physical access to the facility and its equipment.

### ASSETS

ONI employees shall be aware of and follow ONI Remote Work policies and procedures that can be found in ONI's Policy Manual.

- Computers and other devices must be positioned so that the display monitors cannot be viewed by unauthorized individuals. Should an individual be in public, the computer and/or device should not be left unattended.

### DATA

ONI will ensure that a data backup regimen shall be always in place and operational, and the procedures shall be consistently maintained with the assistance of an Informational Technology vendor.

# 900 DISASTER RECOVERY

ONI will ensure that Disaster Recovery plan(s) shall be in place and operational to prepare for any system failures that may affect critical operations in the event of such failure.

# REFERENCES

45 CFR § 164 & 45 CFR § 160, HIPAA Privacy and Security Rules
45 CFR Part 164, Subpart D HIPAA Breach Notification Rule

ORC, Ohio Revised Code
- ORC § 5126.044 Ohio law on confidentiality

OAC 5123:2-2-02 Background investigations for employment

NIST SP, National Institute of Standards and Technology Special Publications
NIST CSF, National Institute of Standards and Technology Cybersecurity Framework

CERT, Carnegie Mellon Software Engineering Institute CERT Division
SANS Institute (SysAdmin, Audit, Network and Security)
CIS, Center for Internet Security
OIG LEIE, Ohio Inspector General List of Excluded Individuals and Entities (LEIE) Online Search
SAM, GSA System for Award Management (SAM) Exclusion Records
ExclusionCheck.com by ProviderTrust, Simultaneous searches of LEIE, SAM and all state Medicaid Exclusion Databases
Medicare Managed Care Manual Chapter 21, Element VI: Effective System for Routine Monitoring, auditing and Identification of Compliance Risks

# CHANGE LOG

| Date | Policy | Description |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |