State of Oklahoma
Office of Management and Enterprise Services
Policies and Procedures

HIPAA Privacy and Security Policy

Effective Date of Policy: 04/01/2019	**Next Scheduled Review: 04/01/2020**
Effective Date of Original Policy: 02/20/ 2014	**Policy Number: OMES - 002**
Last Reviewed: 02/25/2019	**Replaces Policy Number: NA**
Date Policy Last Revised: 04/18/2018	
Approved: Dana Webb, as Designee of OMES Director John Budd	**Approval Date: 02/25/2019**

Policy

The Covered Components of the Office of Management and Enterprise Services shall operate in conformance with the requirements of the Health Insurance Portability and Accountability Act of 1996 (as amended) and the requirements for Confidential Information provided for under 74 O.S. § 1322.

Purpose

The purpose of this policy is to establish strict measures to ensure the safe handling and protection of Confidential Information entrusted to OMES.

Implementation

Implementation of this policy is divided into the following sections:

Section 1: Definitions
Section 2: Intent and Scope of Policy
Section 3: Uses and Disclosures of PHI Section 4: Participant's Rights Regarding PHI
Section 5: Security of ePHI
Section 6: Business Associates
Section 7: Other Privacy/Security Policies Section 8: HIPAA Violations

Section 1: Definitions

Business Associate: As defined under the Privacy Rule, including, but not limited to, 45 CFR §

160.103.

CFR: Code of Federal Regulations.

Confidential Information: Protected health information, employee personal information, Participant files and other OMES information deemed confidential by OMES that is communicated and/or stored in any manner, including verbally, fax or other telecommunication means, on paper, or in any other electronic form. [74 O.S. § 1322]

Covered Component: The components of OMES, as designated by its director, that are required to comply with the Administrative Simplification Provisions of HIPAA because the component performs a covered health care function.

Covered Entity: An entity subject to HIPAA Administrative Simplification mandates including health plans, clearinghouses and providers as indicated in 45 CFR § 160.103.

Covered Function: Functions that make an entity a health plan, a health care provider or a health care clearinghouse, as described under 45 CFR § 164.103.

De-identified Health Information: Health information which has had all 18 HIPAA identifiers removed. The identifiers are described at 45 CFR § 164.514(b)(2).

Designated Record Set: A group of records maintained by or for OMES that includes: the enrollment, payment, medical management and claims adjudication record of a Participant maintained by or for OMES; or other PHI used, in whole or in part, by or for OMES to make coverage decisions concerning a Participant.

Enforcement Rule: 45 CFR § 160 subsections C-E governing the compliance responsibilities of covered entities with respect to the HIPAA enforcement process.

ePHI: PHI in electronic form.

Health Information: Any information, whether oral or recorded in any form or medium: (1) that relates to the past, present or future physical or mental condition of a Participant; the provision of health care to a Participant; or the past, present or future payment for the provision of health care to a Participant; and (2) that identifies the Participant or with respect to which there is a reasonable basis to believe the information can be used to identify the Participant.

HIPAA: The Health Insurance Portability and Accountability Act of 1996, as amended.

Hybrid Entity: Under the Privacy Rule, an entity that has some covered and some non-covered functions as described under 45 CFR Section 164.103.

Limited Data Set: Data sets stripped of certain direct identifiers that are specified in the Privacy Rule. They are not De-identified Health Information under the Privacy Rule.

OMES: Office of Management and Enterprise Services [62 O.S. 34.3 et seq.]. As used in this policy, references to OMES shall always refer to the Covered Components of OMES unless specifically stated otherwise.

Participant: Any individual participating in any plan authorized by or through the Oklahoma Employees Insurance and Benefits Act and/or the Oklahoma State Employees Benefit Act.

Participating Entity: Any employer or organization whose employees are eligible to be Participants in any plan authorized by or through the Oklahoma Employees Insurance and Benefits Act and/or the Oklahoma State Employees Benefit Act.

Privacy Officer: The individual designated by OMES with responsibility for the overall implementation and oversight of OMES's *HIPAA Privacy and Security Policy*.

Privacy Rule: As used in this policy, the Health Insurance Portability and Accountability Act of 1996 (as amended), regulations found at 45 C.F.R. Part 160 and Subparts A and E of Part 164 (as amended), and associated sub-regulatory guidance.

PHI: Protected Health information, as specified in the Privacy Rule. [45 CFR § 164.103]

PII: Personally identifiable information is information that can be used alone or with other information to identify, contact or locate a single person or to identify an individual in context. [National Institute of Standards and Technology, Special Publication 800-122]

Re-identified Health Information: A code, or other means of record identification, to allow De-identified Health Information to be re-identified only by the Covered Entity.

Security Officer: The individual designated by OMES with responsibility for the overall implementation and oversight of OMES' efforts to prevent, detect, contain and correct data security violations of the Security Rule.

Security Rule: 45 CFR § 160 and subsections A and C of § 164 that apply only to ePHI, requiring covered entities to implement certain administrative, physical and technical safeguards to protect the electronic information.

Section 2: Intent and Scope of Policy

2.1. OMES Commitment to Privacy and Confidentiality

OMES is committed to ensuring the safe handling and protection of Confidential Information provided to OMES by its Participants, employers, employees, and contractors. Confidentiality of personal records and information is taken very seriously by OMES, and strict measures shall be taken to safeguard that information.

Although the Privacy Rule is applicable to health plan benefits, some Covered Components of OMES may be subject to more encompassing confidentiality requirements such as required under 74 O.S. §1322.

2.2. Requirements for a Covered Entity with Multiple Covered and Non-Covered Functions

Pursuant to 45 CFR 164.105(a) OMES is designated as a hybrid entity for purposes of complying with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The confidentiality, privacy and security of information policies shall apply to all OMES components which have access to protected health information. The following components are considered Covered Components, or as performing the equivalent of Business Associate functions to the Covered Components:

a. The, Employees Group Insurance Division (EGID), and;
b. The Legal Division; and
c. The Information Services Division (IS) as it applies to maintenance and storage of PHI.

While each Covered Component may not perform all functions described in this policy, this policy shall apply to the extent that the component does perform the function. Each Covered Component shall implement procedures to accomplish the required functions. These procedures must be consistent with this policy and are subject to review by the OMES Privacy Officer.

OMES shall maintain such procedures as necessary to restrict the accessibility, use and disclosure of Confidential Information, including PHI, to non-Covered Components of OMES except as permitted by the Privacy Rule.

2.3. Status of OMES as an Employer

OMES Covered Components shall not disclose PHI to non-Covered Components within OMES without the authorization of the Participant, except under the circumstances disclosed within this policy. OMES shall not disclose PHI for the purpose of employment-related actions or decisions.

2.4. The HIPAA Privacy and Security Policy

The *HIPAA Privacy and Security Policy* establishes a framework within which OMES complies with state and federal requirements to achieve confidentiality and security of OMES Confidential Information.

All persons involved with the creation, collection, handling, or dissemination of OMES Confidential Information are subject to the conditions of this policy. This includes all employees, temporary workers, insurance/benefit coordinators, board members, Business Associates, contractors and anyone who may access or view OMES Confidential Information.

This policy shall be reviewed annually, or whenever statutory or regulatory changes affecting Confidential Information occur.

OMES shall maintain revised policies and procedures in written or electronic form according to Oklahoma law for at least six years from the date last in effect.

Whenever there is a change in federal or state law or regulation that necessitates a change to the OMES *HIPAA Privacy and Security Policy*, the OMES *HIPAA Privacy and Security Policy* is deemed revised to comply with the required change.

Section 3: Uses and Disclosures of PHI

3.1 General Rules

OMES shall use and disclose PHI only as permitted or required under the Privacy Rule, and other federal or state laws and regulations.

3.2. Family Members and Friends

OMES may, but is not required to, disclose limited relevant PHI to a family member or friend who has been specifically identified by the Participant or who is directly involved in the care of the Participant or the payment for care. Disclosure should only occur after verification of identity and authority, and should utilize the minimum necessary rule defined herein.

3.3. Authorizations

OMES may disclose PHI pursuant to an authorization provided by the Participant that satisfies all of the Privacy Rule's requirements for a valid authorization. All uses and disclosures must be consistent with the terms and conditions of the authorization.

3.4. Legal, Specialized Government Functions, Workers' Compensation or Public Health Requests

PHI may be disclosed in the following situations without a Participant's authorization, when certain requirements are satisfied in accordance with 45 CFR 164.512. OMES shall have procedures describing the specific requirements that must be met before these types of disclosures may be made. The requirements shall include prior approval of the OMES Privacy Officer or legal counsel. These disclosures are:

a. Regarding victims of abuse, neglect or domestic violence.
b. For treatment purposes.
c. For judicial and administrative proceedings.
d. For law enforcement purposes.
e. For public health activities.
f. Regarding an individual who has died.
g. For cadaveric organ-, eye- or tissue-donation purposes.
h. For certain limited research purposes.
i. To avert a serious threat to health or safety.
j. For specialized government functions.
k. That relate to workers' compensation programs.

3.5. Limited Data Sets

OMES may release Limited Data Sets for purposes of research, public health or health care operations in accordance with procedures developed to implement 45 CFR 164.514(e)(3).

3.6. Protected Health Information and De-Identification

Release of individually identifiable PHI is restricted under HIPAA. Determinations by OMES as to whether health information is individually identifiable shall be made based upon the standards contained in the Privacy Rule. Health information that meets the standards for de-identification is not subject to the Privacy Rule.

OMES shall adopt such procedures as necessary to ensure that re-identified PHI meets the standards

of the Privacy Rule.

3.7. Maintaining Confidentiality of Health Information

OMES shall not use or disclose PHI except as permitted or required by federal and state statutes or rules. Disclosure of PHI shall be performed by trained personnel in accordance with applicable laws, regulations and OMES' policies and procedures.

3.7.1. Defining, Requesting and Maintaining Access to PHI

For all Confidential Information, OMES shall develop procedures to define the levels of access of users based upon their roles and responsibilities, process and review requests made for access, and ensure the users compliance with applicable policies to maintain access to the information.

3.7.2. Visitors and Vendors

OMES shall designate which workplace areas shall be considered non-secured, semi-secured, or secured. Non-secured areas are those areas in which no Confidential Information is accessible or discussed. Semi- secured areas may have some PHI in the vicinity but it is expected that non-employees will be in the area from time-to-time, and OMES employees must be alerted as to their presence.

Only a Covered Component's current employees, subcontractors or business associates, or other persons approved by the Covered Component's Senior Management should be allowed in the Covered Component's secured or semi-secured areas. Any other person, invited or otherwise authorized to enter the Covered Component's secured or semi-secured areas, but not formally associated with the Covered Component, must be accompanied and/or supervised by a Covered Component's representative at all times. The representative is responsible for the actions of the visitor.

3.8. Verification of Identity and Authority

Prior to disclosing PHI, OMES personnel shall verify the identity and authority (where applicable) of the person or entity requesting the information.

3.9. Minimum Necessary Rule

OMES shall make reasonable efforts to limit disclosures and requests for PHI to the minimum necessary information needed to accomplish the intended purpose of the disclosure or request. For recurring processes, OMES shall develop procedures and protocols that limit disclosures to the reasonably minimum amount required. All other requests shall be reviewed on an individual basis to meet the minimum necessary requirement.

The minimum necessary rule is not required to be applied under the following circumstances:

a. For treatment.

b. For disclosure to the involved Participant;
c. In accordance with the Participant's valid authorization.
d. To the Office of Civil Rights for HIPAA compliance purposes; and
e. As required by law.

3.10. Status of Participating Entities

OMES shall not disclose PHI for the purpose of employment-related actions or decisions.

Section 4: Participant's Rights

4.1. The Notice of Privacy Practices

The OMES Privacy Officer is responsible for developing and maintaining a notice of privacy practices for Covered Components containing those provisions required by the Privacy Rule. The Notice of Privacy Practices outlines how OMES and its business associates shall use and disclose individuals' PHI and how individuals may gain access to that information.

OMES shall maintain procedures and processes ensuring the availability and timely distribution of the notices, and that uses and disclosures of PHI are consistent with the contents of the notice.

4.2. Access to Personal Health Records

Except as provided by law, Participants have a right to access and obtain copies of their PHI that OMES (or its Business Associates) maintains in Designated Record Sets. OMES shall review such requests and approve or deny access based upon procedures approved by the OMES Privacy Officer.

4.3. Restricting Use and Disclosure of PHI

Participants may request restrictions on the use and disclosure of their PHI. Except as otherwise required under 45 CFR § 164.522, OMES does not have to grant these restrictions, but if it agrees to a restriction, it may not use or disclose the PHI in violation of the restriction, except in emergency situations. Any agreed-to restriction shall not be effective to prevent uses and disclosures to the Participant or as required by law. OMES and/or the Participant may also prospectively terminate the agreed-to restriction.

4.4. Requesting a More Confidential Method of Communications

Participants have a right to request reasonable accommodations in receiving communications regarding their health information by alternative means or at an alternative location.

4.5. Amendment of Records

Participants have a right under HIPAA to request that their PHI contained in a Designated Record Set be amended. OMES shall review such requests and, based upon the factors involved, either accept or deny the amendment.

4.6. Filing a Privacy Complaint

Participants have the right to file a formal complaint with OMES or with the Office of Civil Rights if the Participant believes that their privacy rights have been violated.

OMES shall provide a process for individuals to file complaints about the OMES policies, procedures, practices and compliance with the Privacy Rule.

4.7. Accounting for Disclosures

A Participant has the right to obtain an accounting of certain disclosures of his or her own PHI within the last six years.

Section 5: Security of ePHI

5.1. Facility Access Controls

OMES shall adequately safeguard ePHI from unauthorized physical access, tampering and theft. OMES shall develop procedures to grant, control and validate physical access to such facilities containing equipment, software programs and libraries that contain ePHI. Physical access shall be based on the employee's role or function.

OMES shall document repairs and modifications related to the security of a physical facility which houses ePHI maintained by OMES.

5.2. Workstation Use and Security Access Controls

OMES shall implement procedures for the proper use, functions, physical safeguard and the surrounding conditions of workstations used to access ePHI.

5.3. Workforce Policies for Access to Systems with PHI

OMES shall validate job roles that have access to systems that contain or store ePHI. OMES shall procedurally and technically ensure that employees have appropriate access to ePHI when properly granted access and shall prohibit employees who are not granted such access from obtaining access to ePHI.

OMES shall authorize employee access to information systems or locations that contain or store ePHI, based upon the minimum necessary rule and the job role held by the employee requesting access.

OMES shall remove access to ePHI by employees who no longer require access to ePHI. OMES shall document a regular audit of employee access to ePHI.

OMES shall establish a method to report, process and remove information system access by employees who separate from employment within an appropriate timeframe of the separation.

OMES shall set automatic account expirations for temporary, contract and vendor accounts based on the timeframe of the contract or services provided to OMES. The account expiration date must be set for the date to coincide with the date of the services or contract expiration.

5.4. User Access Control

OMES IS shall assign unique user name or numbers to individually track and identify users or process system activity. OMES shall maintain technical procedures that terminate an electronic session after a predetermined time of inactivity.

OMES shall maintain emergency access procedures to ePHI during emergencies or unplanned events.

OMES shall maintain adequate system audit logs and regularly review information system audit logs for log-in discrepancies. Discrepancies must follow Information Services' security incident reporting procedures.

OMES shall establish, maintain and enforce procedures for creating, changing and safeguarding information system passwords.

5.5. Audit Controls

OMES IS shall maintain mechanisms to record and examine system activity in information systems that contain or use ePHI.

5.6. Device and Media Controls

OMES shall implement control procedures relating to OMES devices and media containing ePHI. The procedures shall cover:

a. The re-use or secure disposal of hardware or electronic media.
b. Tracking and recording hardware and electronic media movement outside the IS data center, including designation of the person(s) responsible for such move; and.
c. Encryption and decryption of removable media devices.

All procedures shall meet the minimum requirements established by the OMES Security Officer.

5.7. Data Transmission Security

OMES shall maintain policies, procedures and mechanisms for appropriate technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network. Security measures shall be based upon appropriate risk analysis of the transmission methods and networks involved. Encryption of ePHI shall be employed in all situations identified with undue risk.

OMES shall maintain mechanisms to detect electronically transmitted ePHI that has been improperly modified in transit.

5.8. Risk Assessments

OMES shall implement procedures for the appropriate risk assessments of potential vulnerabilities to the confidentiality, integrity and availability of ePHI held by OMES, and the purchase of systems and services necessary to protect ePHI.

OMES shall, in accordance with 62 O.S. 34.12, conduct an assessment of potential risks no less than annually. OMES shall establish a risk management minimum standard for all information systems that use or store ePHI and implement measures to reduce identified risks and vulnerabilities.

5.9. Protecting ePHI From Improper Alteration or Destruction

OMES shall maintain mechanisms to authenticate ePHI and to corroborate that ePHI has not been improperly altered or destroyed.

OMES shall provide procedural and technical mechanisms to guard against, detect and report malicious software.

5.10. Evaluating, Selecting and Implementing Authentication Mechanisms

OMES shall maintain appropriate authentication mechanisms and procedures to verify an 5.11 entity or person seeking to access ePHI.

5.11. Periodic Security Evaluations

OMES shall periodically evaluate the extent to which security policies and procedures meet the requirements of the HIPAA regulations. Evaluations shall be based upon implemented security standards and in response to environmental or operational changes that affect the security of ePHI.

OMES shall regularly review information system activity reports such as security incident reports, access reports and audit logs.

5.12. Disaster Recovery/Contingency Planning/Emergency Mode Operation

OMES shall designate ISD as having the primary responsibility for implementing procedures and processes regarding ePHI in the event of disaster recovery. OMES shall periodically test and revise the Data Backup, Disaster Recovery, and Emergency Mode Operations plan(s). These plans shall include, but are not limited to:

a. Continuation of critical business process for protection of the security of ePHI while operating in an emergency mode.
b. An applications and data criticality analysis process to assess the criticality of information systems, applications and data.
c. A contingency planning process to identify procedures for responding to an emergency or other unplanned event that damages information systems or access to information systems that contain ePHI.

d. Restoring ePHI data and access to information systems that contain ePHI within an established timeframe for recovery.
e. Granting authorized physical access to information systems that contain ePHI in the event of an emergency or unplanned event.

Although OMES shall maintain retrievable copies of ePHI as part of its disaster recovery process, OMES shall direct any request for a copy of ePHI to the entity that owns the ePHI.

5.13. Security Incident Responses, Reporting and Mitigation

OMES shall identify and respond to suspected or known security incidents and shall mitigate to the extent practicable harmful effects of known security incidents and document the outcome of security incidents.

All OMES employees (including non-Covered Components) and applicable third parties shall report non- compliance of OMES HIPAA-related policies and procedures to the following:

1. For technical security incidents (e.g., computer intrusions, denial of service to authorized users, etc.): OMES Service Desk (see 7.2).

2. For non-technical security incidents (e.g., administration and physical incidents including, but not limited to theft, unlocked doors, unauthorized facility entry, unauthorized computer access: OMES Privacy Officer (see 7.1.).

Employees that report violations in good faith may not be subjected to intimidation, threats, coercion, discrimination against or any other retaliatory action as a consequence.

OMES must promptly facilitate an investigation of all reported violations of OMES HIPAA-related security policies and procedures and take appropriate steps to prevent recurrence of the violation when possible and feasible.

OMES shall maintain all documentation of the investigation, sanctions provided and actions taken to prevent reoccurrence for a minimum of seven years after the conclusion of the investigation.

5.14. Healthcare Clearinghouse Function

OMES does not currently perform any healthcare clearinghouse function. In the future event that OMES begins to perform this function, policies and procedures shall be implemented.

Section 6: Business Associates

6.1. Safeguarding PHI

OMES shall ensure that Business Associates implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the PHI that it creates, receives, maintains, or transmits on behalf of OMES. The Business Associate

shall ensure that proper security is in place to protect electronically stored health information.

All relationships with Business Associates shall be evidenced by a written agreement providing appropriate safeguards of ePHI that the Business Associate may create, receive, maintain, or transmit.

6.2. Uses of PHI by the Business Associate

The Business Associate may only use and disclose the Participant's PHI for the purposes of a Participant's treatment, to facilitate payment for benefits or for Business Associate business operations on behalf of the Participant. The Business Associate may not use or further disclose a Participant's PHI other than permitted by OMES policies, or as described in a written contract between OMES and the Business Associate, or as required by law.

The Business Associate shall establish procedures to protect a Participant's Confidential Information and account for disclosures not authorized by these policies.

6.3. Access to PHI by Business Associate Employees

The Business Associate shall identify employees who have a business need and authority to access PHI, and ensure that access is limited to those identified employees.

6.4. Safeguarding PHI by Agents or Subcontractors

Business Associates shall ensure that any agent or subcontractor to whom it provides PHI agrees to implement reasonable and appropriate safeguards to protect PHI.

6.5. Disclosure for Employment Related Actions

The Business Associate shall not use or disclose PHI for employment-related actions, unless required by law.

6.6. Notification of Breach

The Business Associate shall notify the OMES Privacy Officer within five [5] working days from when the Business Associate becomes aware of any use or disclosure of PHI that is inconsistent with this policy and make an accounting of these disclosures available for OMES and each affected Participant.

6.7. Access by Participants and Amendment of Records

The Business Associate shall allow a Participant to access and review health information on file with the Business Associate and submit amending statements for inclusion in their health information file.

6.8. Availability of Policies and Records to Authorities

The Business Associate shall make internal practices, books and records concerning uses and

disclosures of protected health information available for inspection by the appropriate authority. A written contract between OMES and the Business Associate shall not limit the Business Associate's protection of a Participant's PHI to an extent less than described in this policy.

6.9. Accounting for Disclosures of PHI

The Business Associate shall make available the information required to provide an accounting of disclosures in accordance with 45 CFR § 164.528.

6.10. Disposal of PHI

The Business Associate shall destroy or return a Participant's PHI to OMES when no longer required by the Business Associate. If not feasible, the Business Associate shall limit the use or disclosure to the required purposes.

Section 7: Other Privacy/Security Policies

7.1. Appointment of a Privacy Officer

In accordance with 45 CFR §164.530(a)(1), OMES shall designate a Privacy Officer who is responsible for the overall implementation and oversight of OMES' *HIPAA Privacy and Security Policy*.

7.2. Appointment of a Security Officer

In accordance with 45 CFR §164.308(a)(2), OMES shall designate a Security Officer who is responsible for the development and implementation of information security policies, procedures and practices and overall implementation and oversight of OMES efforts to prevent, detect, contain and correct security violations.

7.3. Fund Raising

OMES shall not use or disclose PHI for purposes of fundraising.

7.4. Storing, Access and Destruction of Confidential Records

All confidential records in all formats must be stored so that they are available for use, but also physically and technologically secure. Information and records must be protected from unauthorized access, physical damage or other reasonably foreseeable hazards.

OMES shall have procedures and processes in place to destroy confidential records in accordance with applicable standards.

7.5. Awareness and Training

OMES shall train its workforce on its *HIPAA Privacy and Security Policy.* Training shall occur upon hiring and annually thereafter. Appropriate training shall also occur as necessary in a reasonably

prompt timeframe for those employees whose job function has been affected as a result of material changes in the *HIPAA Privacy and Security Policy* or its associated procedures.

OMES' Privacy Officer is charged with the overall responsibility of developing training programs and schedules to ensure that employees receive the training that is necessary and appropriate to perform their job functions in accordance with this policy.

On an ongoing basis, OMES shall use a variety of modalities to maintain the awareness of employees regarding the confidentiality, privacy, and security of Confidential Information.

All OMES Covered Component employees shall sign a confidentiality agreement upon hiring which states the importance, understanding and the need for confidentiality. Employees agree not to disclose Confidential Information learned during the course of their employment with OMES, and further understand that Confidential Information disclosed during or after employment with OMES can result in legal actions.

Section 8: HIPAA Violations

8.1. Requirement to Report Violations to Privacy or Security Officer

All OMES employees, and all Business Associates who have access to PHI, are required to report to the Privacy Officer any incidents involving possible breaches.

All OMES employees and applicable third parties shall report a suspected breach of unsecured ePHI to the OMES Security Officer.

8.2. Risk Assessment of Breach

OMES shall maintain procedures to properly investigate a suspected breach of unsecured ePHI and assess whether a notification is required under applicable Oklahoma law or under HIPAA.

8.3. Required Notifications for Privacy Breaches

If notification of a breach of unsecured ePHI is required under applicable Oklahoma law or HIPAA and the breach has occurred as a result of non-compliance by OMES IS with its HIPAA-related security policies, OMES shall coordinate with the entity that owns the ePHI to notify the Secretary of the U.S. Health and Human Services as appropriate and to notify affected individuals within applicable mandatory timeframes set forth in regulations implementing HIPAA, subject to an appropriate law enforcement request for a delay in notification.

For privacy breaches requiring notification, the Privacy Officer shall notify the affected individual without unreasonable delay, and in no case later than 60 days after discovery of a breach. An exception applies in the case of delays requested by law enforcement.

8.3.1. Notification to the Media

Except in situations of law enforcement delays, breaches of unsecured PHI involving more than 500 individuals shall be reported to prominent media outlets without unreasonable delay, and in no case later than 60 days after discovery of a breach.

8.3.2. Notification to the Secretary of HHS

OMES shall report all breaches of unsecured PHI to the Secretary of the U. S. Department of Health and Human Services as appropriate.

The Privacy Officer shall evaluate each reported HIPAA in accordance with standards set forth by the Privacy Rule for the violation’s impact to the individual and as to whether it is a breach that must be reported to the Secretary of the U. S. Department of Health and Human Services.

8.3.3. Law Enforcement Delay of Notification

OMES shall delay required notification of a breach at the request of a law enforcement official when such notification would impede a criminal investigation or cause damage to national security.

8.4. Notification by a Business Associate

OMES shall ensure that a process exists that specifies how, when and to whom a Business Associate should provide notification of a breach in order to expedite notification of affected individuals if necessary.

8.5. Burden of Proof

OMES shall maintain documentation of the evaluation of each reported breach and copies of the notifications that were made.

OMES shall maintain all documentation of the investigation, notifications provided, if any, and actions taken to prevent reoccurrence for a minimum of seven years after the conclusion of the investigation.

8.6. Disclosures by Whistleblowers

In a whistleblower disclosure of PHI by an OMES employee or of a Business Associate, OMES shall evaluate whether the particular disclosure is exempt from the Privacy Rule. [45 CFR § 160.502(j)(1)]

8.7. Disclosures by Employees Who Are Victims of a Crime

An OMES employee who is the victim of a criminal act such as assault or battery may disclose limited PHI regarding the perpetrator to a law enforcement official, provided that the PHI disclosed is about the suspected perpetrator of the criminal act. [45 CFR § 160.502(j)(2)]

8.8. Sanctions

OMES shall apply appropriate sanctions against employees who fail to comply with the policies and procedures of this *HIPAA Privacy and Security Policy.*

Failure to comply with any privacy or security policy or procedure by an OMES employee or an applicable third party may result in corrective disciplinary action, up to and including termination of employment or termination of the relationship and associated privileges of the third party. Such failure may also result in civil and criminal penalties as determined by federal and state laws and regulations.

Recommended sanctions for violations of HIPAA Privacy

Level of Violation	Examples of Violations	Recommended Actions
Level I Errors in handling Restricted or Sensitive information, or maintaining workstation security measures that are **unintentional** and result from lack of training, inexperience, poor judgment or poor process.	• Leaving PHI/PII, in any format, unattended in public areas. • Discussing PHI/PII in public or other inappropriate areas. • Leaving an active computer screen with access to PHI/PII unattended. • Disclosing PHI/PII without identity verification. • Mistakenly sending PHI/PII to wrong postal, email or fax location. • Placing non-shredded documents in inappropriate waste receptacles. • Failure to report that his/her password has been potentially compromised. • Sharing computer access codes. • Failing /refusing to cooperate with Compliance Officer, ISD Security • Officer or authorized designees	• Retraining and reevaluation. • Specialized training and evaluation. • Discussion of policy and procedures. • Verbal warning or oral reprimand. • New Confidentiality Statement signed
Level II Breach in the terms of the Confidentiality Statement and/or OMES policies concerning use and disclosure of Restricted or Sensitive Information due to **intentional but non-malicious** curiosity, concern, etc.	• Failure to complete required Privacy Training and/or to sign the OMES Confidentiality Statement. • Accessing the record of any person, including coworkers, friends, or family, without professional Need- to-Know, including searches for addresses or phone numbers. • Using someone else's computer account. • Copying information as a favor. • Installing unauthorized software with potential to harm systems. • Adding, deleting or altering electronic information without authorization. • Repeated Level I violations (does not have to be the same offense).	• Letter of Reprimand requiring written corrective action plan in response. • Suspension of information system user privileges. • Suspension of employment.
Level III **Intentional** breach in the terms of the Confidentiality Statement and/or OMES policies concerning use and disclosure of Restricted or Sensitive Information, **for personal gain, revenge, to effect harm on another person or gross negligence.**	• Access and unauthorized disclosure of PHI/PII for personal gain or to affect harm on another person. • Unauthorized access of VIP PHI/PII for any reason. • Malicious alteration, deletion or removal of PHI/PII from OMES. • Unauthorized publication or broadcasting of PHI/PII. • Repeated Level I or II violations (does not have to be the same offense). • Failing/refusing to comply with a corrective action plan.	• Final written warning and/or termination of information system user privileges. • Termination of employment: ineligible for rehire and future information systems access.

8.9. Mitigation

OMES shall mitigate, to the extent practicable, any harmful effect from a use or disclosure of protected health information by OMES or a Business Associate that is in violation of its policies and procedures. Factors which shall be considered in the mitigation shall include: whether any damage occurred; the nature and amount of damage, if it did occur; the nature of the PHI that was disclosed and the cause of disclosure; and the extent to which the harm can be mitigated.

8.10. Refraining from Intimidating or Retaliatory Acts

OMES shall not intimidate, threaten, coerce, discriminate against, or take any other retaliatory action against any individual who exercises any PHI privacy right under the Privacy Act, including the filing of a complaint with OMES or the Secretary of Health and Human Services and testifying, assisting or participating in an investigation, compliance review, proceeding or hearing associated with such complaint.

RELATED POLICY

OMES -001 OMES HIPAA Hybrid Policy