Office of Management and Enterprise Services

Information Services Division

Policy

Effective March 1, 2013

Health Insurance Portability and Accountability Act

(HIPAA)

and

Health Information Technology for Economic and Clinical Health Act

(HITECH)

Table of Contents

Introduction

The Information Services Division ("ISD") was created pursuant to 62 O.S. § 34.3 (Supp. 2010) as a division of the Oklahoma Office of Management Enterprises and Services ("OMES"). OMES has designated itself as a hybrid entity under the Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA") and has designated ISD as a health care component that provides covered functions.

ISD is responsible for the maintenance and storage of electronic protected health information ("ePHI") for certain agencies of the State of Oklahoma and is committed to protect the security of ePHI. As defined in 45 C.F.R. §160.103, ePHI means individually identifiable health information that is transmitted by or maintained in electronic media, excluding education records covered by FERPA[1], certain records related to health services provided to college students[2], employment records held by a covered entity in its role as an employer and records regarding a person who has been deceased more than fifty (50) years. Set forth herein are the policies of ISD with regard to the Security Standards for the Protection of Electronic PHI found at 45 C.F.R. §164.302 et seq, the applicable implementing regulations of HIPAA. These policies are applicable to all ISD employees, business associates of ISD and any other person who performs business functions on behalf of ISD in which access to locations containing ePHI is granted.

1. Administrative Safeguards

1.1. Security Management Process (45 C.F.R. § 164.308[a][1])

1.1.1. Risk Analysis Policy – ISD-SEC-H-001

i. ISD shall conduct an assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by ISD.

ii. ISD shall, in accordance with Section 34.12 of Title 62 of Oklahoma State Statutes, conduct an assessment of potential risks no less than annually.

iii. **Procedure:** State Information Security Policies, Procedures, Guidelines sections 4.0, 4.1 and 4.2

1.1.2. Risk Management Policy – ISD-SEC-H-002

i. ISD shall establish a Risk Management minimum standard for all information systems that use or store ePHI.

ii. ISD shall implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

iii. **Procedure:** State Information Security Policies, Procedures, Guidelines sections 4.0, 4.1 and 4.2

[1] Federal Educational Rights and Privacy Act, as amended, codified at 20 U.S.C. §1232g

[2] 20 U.S.C. §1232g

1.1.3. Sanction Policy – ISD-SEC-H-003

i. Failure to comply with any security policy or procedure by an ISD 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.

1.1.4. Information System Activity Review – ISD-SEC-H-004

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

ii. **Procedure:** State Information Security Policies, Procedures, Guidelines section 9.14

1.2. Assigned Security Responsibility (45 C.F.R. § 164.308[a][2])

1.2.1. Assigned Security Responsibility – ISD-SEC-H-005

i. ISD assigns the responsibility and authority to the ISD Information Security Officer for the development and implementation of information security policies, procedures, and practices.

ii. **Procedure:** State Information Security Policies, Procedures, Guidelines section 2.3

1.3. Workforce Security (45 C.F.R. § 164.308[a][3])

1.3.1. Workforce Security – ISD-SEC-H-006

i. ISD 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.

ii. **Procedure:** State Information Security Policies, Procedures, Guidelines sections 2.1, 2.2 and 2.3

1.3.2. Authorization and/or Supervision – ISD-SEC-H-007

i. ISD shall authorize employee access to information systems or locations that contain or store ePHI, based upon “Need to Know” and the job role held by the employee requesting access; remove access to ePHI by employees who no longer require access to ePHI; and document a regular review of employee access to ePHI.

ii. **Procedure:** State Information Security Policies, Procedures, Guidelines sections 2.1, 2.2 and 2.3

1.3.3. Workforce Clearance Procedure – ISD-SEC-H-008

i. ISD shall validate job roles that have access to systems that contain or store ePHI

ii. **Procedure:** State Information Security Policies, Procedures, Guidelines sections 2.1, 2.2 and 2.3

1.3.4. Termination Procedures – ISD-SEC-H-009

i. ISD shall establish a method to report, process, and remove information system access by employees who separate from employment with ISD within an appropriate timeframe after the ISD Service Desk is notified of the separation.

ii. **Procedure:**

a. State Information Security Policies, Procedures, Guidelines section 2.3

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

1.4. Information Access Management (45 C.F.R. § 164.308[a][4])

1.4.1. Isolating Healthcare Clearinghouse function – NOT APPLICABLE

1.4.2. Access Authorization – ISD-SEC-H-010

i. Workforce Security – see ISD-SEC-H-006
ii. Authorization and/or Supervision – see ISD-SEC-H-007
iii. Workforce Clearance Procedure – see ISD-SEC-H-008

1.4.3. Access Establishment and Modification – ISD-SEC-H-011

i. Authorization and/or Supervision – see ISD-SEC-H-007

1.5. Security Awareness and Training (45 C.F.R. § 164.308[a][5])

1.5.1. Security Awareness and Training – ISD-SEC-H-012

i. ISD shall maintain a security awareness and training program for all ISD employees.
ii. **Procedure:** State Information Security Policies, Procedures, Guidelines section 5.2

1.5.2. Security Reminders – ISD-SEC-H-013

i. ISD shall maintain a security reminder process for all ISD employees.
ii. **Procedure:** State Information Security Policies, Procedures, Guidelines section 5.2

1.5.3. Protection from Malicious Software – ISD-SEC-H-014

i. ISD shall provide procedural and technical mechanisms to guard against, detect, and report malicious software.
ii. **Procedure:** State Information Security Policies, Procedures, Guidelines sections 9.19, 9.20 and 9.21

1.5.4. Log-in Monitoring – ISD-SEC-H-015

i. ISD shall maintain adequate system audit logs and regularly review information system audit logs for log-in discrepancies. Discrepancies must follow Security Incident reporting procedures.
ii. **Procedure:** State Information Security Policies, Procedures, Guidelines section 3.5

1.5.5. Password Management – ISD-SEC-H-016

i. ISD shall establish, maintain, and enforce procedures for creating, changing, and safeguarding information system passwords.
ii. **Procedure:** State Information Security Policies, Procedures, Guidelines sections 2.1 and 2.4

1.6. Security Incident Procedures [45 C.F.R.§ 164.308[a][6])

1.6.1. Response and Reporting – ISD-SEC-H-017

i. ISD 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.

ii. All ISD employees and applicable third parties shall report non-compliance of ISD HIPAA-related policies and procedures to the ISD Service Desk. Individuals that report violations in good faith may not be subjected to intimidation, threats, coercion, discrimination against, or any other retaliatory action as a consequence.

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

iv. **Procedure:**

a. State Information Security Policies, Procedures, Guidelines section 3.4

b. Appendix E – Computer (Cyber) Incident Reporting Procedures

c. Appendix E- Incident Management Procedure

d. ISD Security 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.

1.7. Contingency Plan (45 C.F.R. § 164.308[a][7])

1.7.1. Data Backup Plan – ISD-SEC-H-018

i. ISD shall maintain retrievable copies of ePHI and shall direct any request for a copy of ePHI to the agency that owns the ePHI.

ii. **Procedure:** State Information Security Policies, Procedures, Guidelines section 7.3

1.7.2. Disaster Recovery Plan – ISD-SEC-H-019

i. ISD shall maintain 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.

ii. ISD shall maintain an applications and data criticality analysis process to assess the criticality of information systems, applications, and data.

iii. ISD shall maintain procedures to restore ePHI data and access to information systems that contain ePHI within an established timeframe for recovery.

iv. **Procedure:** State Information Security Policies, Procedures, Guidelines sections 7.3, 8.0 and 8.2

1.7.3. Emergency Mode Operation Plan – ISD-SEC-H-020

i. ISD shall establish a process to grant authorized physical access to information systems that contain ePHI in the event of an emergency or unplanned event.

ii. ISD shall maintain procedures to enable continuation of critical business process for protection of the security of ePHI while operating in an emergency mode.

iii. **Procedure:** State Information Security Policies, Procedures, Guidelines sections 8.0 and 8.1

1.7.4. Testing and Revision Procedure – ISD-SEC-H-021

i. ISD shall periodically test and revise the Data Backup, Disaster Recovery, and Emergency Mode Operations plan(s)

ii. **Procedure:** State Information Security Policies, Procedures, Guidelines sections 8.0, 8.1 and 8.2

1.8. Evaluation (45 C.F.R. § 164.308[a][8])

1.8.1. Evaluation – ISD-SEC-H-022

i. ISD shall periodically evaluate the extent to which ISD's security policies and procedures meet the requirements of the HIPAA regulations.

ii. **Procedure:** Evaluations will be based upon implemented security standards and in response to environmental or operational changes that affect the security of ePHI.

1.9. Business Associate Contracts (45 C.F.R. § 164.308[b][1])

1.9.1. Written Contract or Other Arrangement – ISD-SEC-H-023

i. 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.

2. Physical Safeguards

2.1. Facility Access Controls (45 C.F.R. § 164.310[a][1])

2.1.1. Contingency Operations – ISD-SEC-H-024

i. See Contingency Plan, Disaster Recovery Plan and Emergency Mode Operation Plan, ISD-SEC-H-018, ISD-SEC-H-019 and ISD-SEC-H-020 respectively.

2.1.2. Facility Security Plan – ISD-SEC-H-025

i. ISD shall adequately safeguard the facility and equipment therein from unauthorized physical access, tampering and theft.

ii. ISD shall maintain a process to grant authorized physical access to information systems that contain ePHI.

iii. **Procedure:** State Information Security Policies, Procedures, Guidelines sections 7.0, 7.1, 7.4 and 7.5

2.1.3. Access Control and Validation Procedures – ISD-SEC-H-026

i. ISD shall develop procedures to control and validate physical access to facilities and physical access to software programs and libraries.

ii. **Procedure:**

a. Physical access will be based on the employee's role or function.

b. State Information Security Policies, Procedures, Guidelines sections 7.4, 7.5, 7.7, 9.4, and 9.16

2.1.4. Maintenance Records – ISD-SEC-H-027

i. ISD shall document repairs and modifications related to the security of the physical facility which houses ePHI.

ii. **Procedure:** No reference

2.2. Workstation Use and Security (45 C.F.R. § 164.310[b][c])

2.2.1. Workstation Use and Security – ISD-SEC-H-028

i. ISD shall develop procedures for the proper use, functions and physical safeguard of deployed workstations and the conditions of its surroundings to access ePHI.

ii. **Procedure:** State Information Security Policies, Procedures, Guidelines sections 5.0 and 5.3

2.3. Device and Media Controls (45 C.F.R. § 164.310 [d][1])

2.3.1. Media Disposal and Re-use – ISD-SEC-H-029

i. ISD shall develop procedures for the re-use or secure disposal of hardware or electronic media on which ePHI is stored.

ii. **Procedure:**

a. State Information Security Policies, Procedures, Guidelines section 9.10

b. Appendix E – Media Sanitization Procedures

2.3.2. Media Accountability – ISD-SEC-H-030

i. ISD shall maintain a record of hardware and electronic media movement outside the ISD data center, including designation of the person(s) responsible for such move.

ii. **Procedure:** No reference

2.3.3. Data Backup and Storage (during transfer) – ISD-SEC-H-031

i. See Data Backup Plan Policy – ISD-SEC-H-018

3. Technical Safeguards

3.1. Access Control (45 C.F.R. § 164.312 [a][1])

3.1.1. Unique User Identification – ISD-SEC-H-032

i. ISD shall assign unique user name or numbers to individually track and identify users or process system activity.

ii. **Procedure:** State Information Security Policies, Procedures, Guidelines sections 2.1 and 2.4

3.1.2. Emergency Access Procedure – ISD-SEC-H-033

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

ii. **Procedure:** See Disaster Recovery Plan and Emergency Mode Operation Plan – ISD-SEC-H-019 and ISD-SEC-H-020

3.1.3. Automatic Logoff – ISD-SEC-H-034

i. ISD shall maintain technical procedures that terminate an electronic session after a predetermined time of inactivity.

ii. **Procedure:** State Information Security Policies, Procedures, Guidelines section 2.4

3.1.4. Encryption and Decryption of Removable Media Devices – ISD-SEC-H-035

i. ISD shall maintain procedures to comply with State Information Security Policies, Procedures, Guidelines.

ii. **Procedure:**

a. State Information Security Policies, Procedures, Guidelines section 7.7

b. Appendix E, Section 4 – Removable Media – Acceptable Use Procedures

3.2. Audit Controls (45 C.F.R. § 164.312 [b])

3.2.1. Audit Controls – ISD-SEC-H-036

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

ii. **Procedure:** State Information Security Policies, Procedures, Guidelines section 9.14

3.3. Integrity (45 C.F.R. § 164.312 [c][1])

3.3.1. Integrity of ePHI – ISD-SEC-H-037

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

ii. **Procedure:** No Reference

3.4. Person or Entity Authentication (45 C.F.R. § 164.312 [d])

3.4.1. Person or Entity Authentication – ISD-SEC-H-038

i. ISD shall maintain mechanisms to verify an entity or person seeking to access ePHI is the one that is claimed.

ii. **Procedure:** No Reference

3.5. Transmission Security (45 C.F.R. § 164.312 [e][1])

3.5.1. Transmission Security – ISD-SEC-H-039

i. ISD shall maintain mechanisms to protect against unauthorized access of ePHI when in transit over unsecure networks or where Risk Analysis shows undue risk in the transmission methods.

ii. **Procedure:** No Reference

3.5.2. Integrity Controls – ISD-SEC-H-040

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

ii. **Procedure:** No Reference

3.5.3. Encryption (FTP and Email over Internet) – ISD-SEC-H-041

i. ISD shall maintain mechanisms to encrypt ePHI when Risk Analysis identifies undue risk in the transmission of ePHI.

ii. **Procedure:** No Reference

4. Breach Rule

4.1. Breach Assessment (45 C.F.R. § 164.402)

4.1.1. Breach Assessment – ISD-SEC-H-042

i. All ISD employees and applicable third parties shall report a suspected breach of unsecured ePHI to the ISD Service Desk. Individuals that report a suspected breach in good faith may not be subjected to intimidation, threats, coercion, discrimination against, or any other retaliatory action as a consequence.

ii. ISD 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.

iii. **Procedure:**

a. State Information Security Policies, Procedures, Guidelines section 3.4

b. Appendix E – Computer (Cyber) Incident Reporting Procedures

c. Appendix E – Incident Management Procedure

d. 74 O.S. §3113.1

e. Title 24 O. S. §§161-166

f. ISD Security 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.

4.2. Breach Notification (45 C.F.R. § 164.404; 164.406 and 164.408)

4.2.1. Breach Notification – ISD-SEC-H-043

i. 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 ISD with its HIPAA-related security policies, ISD shall coordinate with the agency 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.

ii. **Procedure:**

a. State Information Security Policies, Procedures, Guidelines section 3.4

b. Appendix E – Computer (Cyber) Incident Reporting Procedures

c. Appendix E – Incident Management Procedure

d. 74 O.S. § 3113.1

e. Title 24 O. S. § 161-166