South Dakota

Department of Human Services

HIPAA Security Policies and Procedures Manual

August 2019

Policy Title:	HIPAA Security Policies and Procedures		
Policy Number:	**DHS-**	**Version:**	1.0
Approved By:			
Effective Date:	August 1, 2019		
Reviewed Date:			

Table of Contents

Risk Management Policy

Purpose

To establish the security risk management process of South Dakota Department of Human Services (DHS), as required by the HIPAA Security Regulations, by implementing policies and procedures to prevent, detect, contain, and correct security violations. To accurately assess, and implement security measures to reduce risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI) held by DHS.

Responsible for Implementation: Security Officer, Risk Management Team members

Risk Management Team members: Security Officer, Privacy Officer, representatives of the Bureau of Information & Telecommunications (BIT) of the State of South Dakota

Policy

1. This Policy shall work in accordance with the Risk Management policy of the Information Technology (IT) Security Policy developed by BIT.

2. DHS periodically conducts, reviews, and updates an assessment of the potential risks to the confidentiality, integrity, and availability of DHS's ePHI, and implements security measures to reduce identified risks to a reasonable and appropriate level.

3. Risk analysis and risk management are recognized as important parts of DHS's security compliance program, in accordance with the requirements in the HIPAA Security Regulations.
   A. To the extent possible, risk assessments are done before the purchase or integration of new technologies, prior to changes made to physical safeguards, and while integrating technology and making physical security changes.
   B. DHS performs periodic technical and non-technical assessments of the HIPAA Security requirements in response to environmental or operational changes affecting the security of ePHI.

4. DHS implements security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to:
   A. Ensure the confidentiality, integrity, and availability of all ePHI that DHS creates, receives, maintains, or transmits.
   B. Protect against any reasonably anticipated Threats or hazards to the security or integrity of ePHI.

C. Protect against any reasonably anticipated uses or disclosures of ePHI that are not permitted or required.
D. Ensure Workforce compliance with security requirements.

5. All Workforce members are expected to fully cooperate with all persons charged with doing risk management work.

6. All risk management efforts, including decisions made on what controls to put in place as well as those to not put into place, are documented and the documentation is maintained for six years.

Procedures

1. The Security Officer and the Risk Management Team oversee the security risk analysis and risk management process.

2. **Risk Assessment**
   A risk assessment is performed to determine the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by DHS. The following steps from the risk assessment methodology found in NIST Special Publication 800-30 are used to conduct risk assessments. Some of the steps may also be used when purchasing, upgrading, or moving ePHI systems and as needed to assist in the risk management efforts of DHS.
   - Step 1. System Characterization: Define the scope of the effort, including the operating environment and boundaries of the Information System. Identify where ePHI is created, received, maintained, processed, or transmitted. Consider remote work force and telecommuters, as well as removable media and portable computing devices.
   - Step 2. Threat Identification: Identify and document potential Threats, which are anything that can have a negative impact on ePHI. A Threat, which may be intentional or unintentional, exists when there is the potential for a Threat Source to successfully exploit a Vulnerability. Threat Sources can be natural, human, or environmental.
   - Step 3. Vulnerability Identification: Develop a list of technical and non-technical system vulnerabilities (flaws or weaknesses) that could be exploited by potential Threat Sources. Vulnerabilities may include incomplete information security policies, insufficient safeguards to protect facilities and equipment housing ePHI, and lack of Workforce security training.
   - Step 4. Control Analysis: Document and assess the effectiveness of technical and non-technical controls that have been or will be implemented by DHS to minimize or eliminate the likelihood of a Threat Source exploiting a Vulnerability.

- Step 5. Likelihood Determination: Determine the probability that a Vulnerability may be exploited by a Threat Source given the existing or planned security controls.
- Step 6. Impact Analysis: Determine the level of adverse impact that would result from a Threat Source successfully exploiting a Vulnerability. Factors to consider include the importance to the mission of DHS; sensitivity and criticality of the ePHI; associated costs; and loss of confidentiality, integrity, and availability of systems and data.
- Step 7. Risk Determination: Determine risk level by multiplying the ratings from the likelihood determination and impact analysis. This represents the level of risk to which an IT system may be exposed if a Vulnerability were to be successfully exploited by a Threat Source.
- Step 8. Control Recommendations: Identify controls that could mitigate the identified risks, to reduce risk to the IT system and its ePHI to an acceptable level. Factors to consider when developing controls may include system compatibility, organizational policy, operational impact, safety/reliability, and cost effectiveness (i.e. cost-benefit analysis).
- Step 9. Results Documentation: Document results of the risk assessment (Threat Sources and Vulnerabilities identified, risks assessed, security controls recommended, etc.) in a report and provide to senior leadership to assist with decisions on policy, procedure, budget, and system operational and management changes.

3. **Risk Mitigation**
   Risk mitigation involves evaluating, selecting, and implementing the appropriate risk-reducing controls recommended from the risk assessment process to ensure the confidentiality, integrity and availability of ePHI. The following steps may be utilized to make determinations of the appropriate controls to put into place. Some of the steps may also be utilized when purchasing, upgrading, or moving ePHI systems and as needed to assist in the risk management efforts of DHS.
   - Step 1. Risk Analysis Results: The results from Step 7 of the Risk Assessment, ranked from high to low, form the basis of the risk management efforts of DHS.
   - Step 2. Evaluation of Control Options: Review recommended control(s) and alternative solutions for reasonableness and appropriateness. The feasibility and effectiveness of the recommended controls should be evaluated. Select potential control options for each identified risk and document reasons for selection.
   - Step 3. Cost-Benefit Analysis: Determine the extent to which a potential control is cost-effective. Compare the benefit (amount of risk reduction) of applying a control with its cost of application/ implementation.

- Step 4. Selection of Control(s): Based on the cost-benefit analysis, select the most reasonable, appropriate, and cost-effective controls to reduce identified risks to the information system and to the confidentiality, integrity, and availability of ePHI. Controls selected may consist of a mix of administrative, physical, and/or technical safeguards.
- Step 5. Responsibility: Identify the Workforce member(s) or team with the skills necessary to implement each of the selected controls and assign their responsibilities. Identify the equipment, training and other resources needed for the successful implementation of controls.
- Step 6. Implementation: The responsible Workforce member(s) or team properly implements the selected security control(s). Document the date controls are put into place and provide regular status reports to senior leadership.
- Step 7. Ongoing Evaluation: Evaluate and revise, as necessary and appropriate, the selected and implemented security controls to verify that needs and expectations are being met. If risk reduction expectations are not met, then repeat all or a part of the risk management process so that additional controls needed to lower risk to an acceptable level can be identified.

4. **Risk Management Schedule**
   Risk Assessment and Risk Mitigation are carried out according to the following schedule to ensure the continued adequacy and continuous improvement of the information security program:
   - Annually: A risk assessment of DHS's information system infrastructure and policies and procedures safeguarding the confidentiality, integrity and availability of ePHI will be conducted, or reviewed and updated, on an annual basis.
   - Throughout a System's Development Life Cycle: From a new information system's selection/ implementation and until its disposal, ongoing assessments of the potential security Threats and vulnerabilities to the system are done (e.g. when purchasing, upgrading, or moving ePHI systems).
   - As Needed: A full or partial risk assessment may be performed in response to environmental or operational changes affecting the security of ePHI (e.g. when experience a security incident, turnover in key workforce members/management, or other things that impact how ePHI is stored or transmitted).

5. **Documentation**. Documentation of all risk assessment and risk mitigation efforts must be maintained for a minimum of six years.

6. **Compliance.** Violation of this policy and its procedures by Workforce members may result in corrective disciplinary action, up to and including termination of employment.

Resources:

1. BIT Information Technology Security Policy, Risk Management Policy
2. WHITEC Risk Management Policy
3. HIPAA COW Risk Management Policy
4. NIST Risk Management Guide for Information Technology Systems, Special Publication 800-30, July 2002.
5. NIST Security Self-Assessment Guide for Information Technology Systems 800-26

Applicable Standards/Regulations:

1. 45 CFR § 164.308(a)(1)(i) HIPAA Security Rule Security Management Process
2. 45 CFR § 164.308(a)(1)(ii)(A) HIPAA Security Rule Risk Analysis
3. 45 CFR § 164.308(a)(1)(ii)(B) HIPAA Security Rule Risk Management
4. 45 CFR § 164.308(a)(8) HIPAA Security Rule Evaluation

Contingency Plan Policy

Purpose

To protect the confidentiality, integrity, and availability of ePHI by taking reasonable and appropriate steps to establish (and implement as needed) documented emergency response procedures in order to prepare for and respond to emergencies and disasters that may damage or otherwise disable ePHI systems, and to ensure that ePHI will survive a disaster or other emergency.

Responsible for Implementation: The Contingency Plan, Disaster Recovery Plan, and this policy is developed, overseen, activated, and maintained by the Security Officer, in conjunction with BIT.

Policy

1. This Policy shall work in accordance with the Business Contingency Plan policy and associated contingency planning controls developed by BIT.

2. It is the policy of DHS to have systems containing ePHI available during an emergency or a Disaster as needed and feasible to provide standard quality of care.

3. DHS maintains a current ePHI information system Contingency Plan and Disaster Recovery Plan that supports timely restoration and recovery of interrupted critical clinical and business operations during an emergency or Disaster situation.

4. It is the policy of DHS to minimize possible adverse clinical outcomes, as well as financial and business impacts, to DHS as a result of an interruption of normal business operations through manual and automated methods of accessing needed information during an emergency.

5. EPHI must continue to be protected to the extent possible during emergencies and Disasters.

Procedures

1. ***Contingency Plan.*** DHS shall implement a Contingency Plan which establishes the policies and procedures for responding to an emergency or disaster such as fire, vandalism, terrorism, system failure, or natural disaster affecting systems containing ePHI, and shall include:
    A. A documented data backup plan (see *Data Management Policy*) to create and maintain retrievable exact copies of ePHI to ensure that DHS can recover from the loss of data.

B. A documented Disaster Recovery Plan (DRP) to restore any loss of ePHI if impacted by a disaster or other emergency.
C. A documented Emergency Mode Operations Plan to take reasonable steps to ensure the continuance of critical business processes that protect the security of ePHI while operating in emergency mode.
D. Testing, review, and revision of the Disaster Recovery Plan and Emergency Mode Operations Plan, as needed. DHS shall complete testing of its Disaster Recovery Plan and, if necessary, take reasonable steps to ensure that it is up-to-date and effective.
E. A process to analyze and document the criticality of applications and data on ePHI systems.
F. Annual testing of the Contingency Plan and retention of the test results.

2. ***Data backup plan.*** See *Data Management Policy*

3. ***Disaster Recovery Plan.*** DHS shall implement a DRP which shall include:
   A. The conditions under which the DRP may be activated.
   B. Workforce members' roles and responsibilities in executing the DRP.
   C. Procedures to timely restore ePHI and return ePHI systems to normal operations.
   D. The order in which ePHI will be restored and the ePHI systems will be returned to operation.
   E. Reporting and notification procedures to the Security Officer or designated workforce members.
   F. Procedures for appropriate specified Workforce members, in the event of a disaster or other emergency, to have physical access to facilities, and to any backup media on which ePHI is stored (whether onsite or offsite) in order to carry out the recovery plan.
   G. Procedures specifying how and when the DRP will be tested and maintained.

4. ***Emergency Mode Operation Plan.*** DHS shall implement an Emergency Mode Operation Plan which shall:
   A. Define and categorize reasonably foreseeable emergencies that could have an impact on the confidentiality, integrity, and availability of ePHI systems.
   B. Specify how DHS will respond to emergencies impacting the confidentiality, integrity, and availability of ePHI.
   C. Outline how security processes and controls will be maintained to ensure the confidentiality, integrity, and availability of ePHI during and immediately following an emergency.
   D. Authorize specified workforce members to enter DHS, and offsite location(s) where backup storage media may be stored, to assist in restoring access to ePHI and maintaining the security of ePHI while functioning in emergency mode.

E. Identify and document processes and controls that protect the confidentiality, integrity, and availability of ePHI while functioning in emergency mode.

5. ***Applications and Data Criticality Analysis***
   A. DHS will analyze and document the criticality of ePHI and ePHI systems.
   B. The purpose of this criticality analysis is to assess the relative impacts if a disaster or other emergency causes ePHI systems to become unavailable for a period of time.
   C. The criticality analysis will serve as the basis for the prioritization of ePHI and ePHI systems in support of other Contingency Plan components.

6. ***Environmental controls*** are in place to reduce the amount of time systems may be down. The Security Officer ensures that any server rooms and/or data wiring rooms/closets are locked with appropriately limited access, and are reasonably and appropriately protected by safety measures such as the following:
   A. Uninterrupted power supply (UPS)
   B. Generator
   C. Cooling system
   D. Backup cooling system
   E. Fire suppression system
   F. Electrical fire rated fire extinguisher
   G. Temperature and fire alarms/paging

7. ***Oversight and authority.*** The Security Officer oversees and has the authority and overall responsibility for the implementation, activation, coordination, and documentation of contingency plan and Disaster recovery operations, including the following:
   A. Maintaining a contact list, including key workforce members, vendors and other individuals that help support and recover systems, for each system with the current Contingency Plan/DRP.
   B. Obtaining Contingency Plans/DRPs from vendors and other business associates when they are necessary to be incorporated into DHS's contingency and Disaster recovery plans.
   C. Maintaining a current and detailed asset inventory list to include each system, application, server, hardware, IS equipment (workstations, portable devices, etc.), network information/ specifications, etc. that are used to access, store, or transmit ePHI.
   D. Assigning a Data Criticality Level for each system, application, server, hardware, IS equipment, network information/specifications, etc., including all software applications and data points that store, maintain, or transmit ePHI.
   E. Maintaining a current network diagram of all servers, systems, interfaces, etc.

F. Creating and maintaining a list of the most significant types of Threat sources most likely to damage systems containing or affect the availability of ePHI and/or critical systems.
G. Maintaining a list of Disaster recovery supplies needed and ensures that they are readily available.
H. Making arrangements for a recovery facility for the IS Disaster Recovery command center (the centralized location for IS Disaster recovery processes), as needed to provide patient care and provide critical services, and which has the necessary critical resources and equipment required for Disaster recovery. Types of recovery facilities include:
    i) Cold Site: A basic facility with adequate space and infrastructure (electrical power, telecommunications connections, environmental controls) to support the DHS information systems. The site would not contain information technology or office equipment.
    ii) Warm Site: A partially equipped facility containing all or some of the system hardware, telecommunications and power sources. The site would be maintained in operational status ready to receive relocated staff. The site may exist as a normal operational facility for another system or function, or it may need to be prepared to receive relocated staff and equipment.
    iii) Hot Site: A fully equipped facility ready to begin preparing for system arrival within hours. More costly than cold or warm sites.

8. ***Emergencies: Activation of the Contingency Plan and Disaster Recovery Plan***
    A. The Security Officer activates the Contingency Plan/DRP, as necessary and appropriate, in conjunction with BIT.
    B. During emergencies all users must continue to protect ePHI to the extent possible, and users may not share passwords or allow others to utilize systems logged in by the user unless properly authorized and instructed to do so.

9. ***Contingency Plan Testing and Maintenance***
    A. Contingency Plan/DRP testing is done on an annual basis, at a minimum.
        i) A scenario-based walk-through or "mock" drill is periodically conducted to examine the plans and determine the need for changes.
        ii) When recovery process has been completed, document why the system was down and how the system was recovered, and maintain this documentation as a part of the Contingency Plan/DRP testing files.
    B. Maintenance and Revision
        i) The Security Officer is responsible for maintenance and revision of the Contingency Plans/DRP, in conjunction with BIT.
            (a) The Contingency Plans/DRP are reviewed and revised on an annual basis and when needed to ensure that the information it contains is current.

(b) The Contingency Plans/DRP is reviewed and revised to address issues identified after each Disaster incident, whether a planned drill or actual Disaster.

ii) All revisions are provided to those that need to follow the plans.

10. ***Workforce Training***
    A. Training for Workforce members with contingency plan responsibilities is provided at least annually, with new hires with plan responsibilities receiving training shortly after hire.
    B. Users of critical ePHI systems are trained on how to access necessary ePHI during an emergency and continue to protect ePHI during emergencies.

11. ***Documentation***
    A. Copies of the Contingency Plan and Disaster Recovery Plans are maintained securely on and offsite and are readily available in the event of an emergency to workforce members responsible for activating the Disaster recovery plan and recovering ePHI and ePHI systems.
    B. Contingency Plans/DRP information, including the controls in place, testing, and revisions are maintained for 6 years.

12. ***Compliance.*** Violation of this policy and its procedures by Workforce members may result in corrective disciplinary action, up to and including termination of employment.

Resources:

1. BIT Information Technology Security Policy, Business Continuity Policy
2. WHITEC Contingency Plan Policy
3. HIPAA COW Contingency Planning Whitepaper
4. HIPAA COW Risk Analysis & Risk Management Toolkit

Applicable Standards/Regulations:

1. 45 CFR § 164.308(a)(7) HIPAA Security Rule Contingency Plan
2. 45 CFR § 164.308(a)(7)(ii)(B) HIPAA Security Rule Disaster Recovery Plan
3. 45 CFR § 164.308(a)(7)(ii)(C) HIPAA Security Rule Emergency Mode Operation Plan
4. 45 CFR § 164.308(a)(7)(ii)(D) HIPAA Security Rule Testing and Revision Procedure
5. 45 CFR § 164.308(a)(7)(ii)(E) HIPAA Security Rule Applications and Data Criticality Analysis
6. 45 CFR § 164.310(a)(2)(i) HIPAA Security Rule Facility Access Controls/Contingency Operations
7. 45 CFR § 164.312(a)(2)(ii) HIPAA Security Rule Access Control/Emergency Access Procedure

Data Management Policy

Purpose

Back up and proper storage of Electronic Protected Health Information (ePHI) are an important part of the day to day operations of DHS's information security. Backups are done so that the minimum necessary ePHI is available when needed during system failures and emergencies. Guidelines are established to track the movement of Hardware and Electronic Media containing ePHI help maintain the confidentiality, integrity, and availability of ePHI.

Responsible for Implementation: Security Officer is responsible for implementing and overseeing this policy, in conjunction with BIT.

Security Officer and BIT are responsible for overseeing and delegating ePHI data Backups and logging and monitoring of movements of Hardware and Electronic Media containing ePHI.

Policy

1. This Policy shall work in accordance with the Data Backup policies developed and implemented by BIT.

2. It is the policy of DHS to establish and implement procedures to create and maintain retrievable exact copies of ePHI.

3. To assure that complete, accurate, retrievable, and tested back-ups of ePHI are available for all information systems used by DHS, as needed.

4. To create a retrievable exact copy of ePHI before movement of equipment.

5. To maintain a record/log of movements of Hardware and Electronic Media containing ePHI.

Procedures

1. ***ePHI Data Backup***
   A. DHS shall take reasonable and appropriate measures to establish and implement a Backup plan to be able to create and maintain retrievable exact copies of ePHI, and such plan shall:
      i) Define a backup schedule, to include at a minimum:
         (1) Performing a daily/real time incremental Backup and weekly full Backup of critical systems that create, store, or transmit ePHI.
         (2) Performing Backups of a less critical nature on a daily/weekly basis.

(3) Performing Backups on a 10 day rotation, when reusable Electronic Media such as disks or tapes are used for Backups.
(4) Storing Backups offsite on a daily basis for critical ePHI systems, and on a weekly basis for those with a less critical nature.

ii) Require timely and appropriate training on Backup procedures for workforce members with responsibility for performing ePHI data Backups.

iii) Require Backups, if/when transported, to be in a locked case with access to the key limited to only those responsible for the Backups and/or recovery of data from Backups.

B. Backup plan shall be documented and made available to key workforce members.

C. Backups in storage shall be stored in a fireproof, locked safe away from water sources with access limited to only those individuals responsible for the Backups and/or recovery of data from Backups.

D. Data backup procedures outlined in the Backup plan must be periodically tested to ensure that exact copies of ePHI are retrievable and can be made available when necessary.

E. When ePHI Backups are completed and/or stored by a vendor:
   i) Vendor must have the above stated controls in place, at a minimum.
   ii) A sufficient and signed Business Associate Agreement must be in place with vendor.

2. ***Moving ePHI – Electronic Media***
DHS makes reasonable and practical efforts to control Electronic Media containing ePHI which enters and leaves, and moves within, DHS. Users are responsible for securing devices when on and off the premises, according to DHS's information security policies. Users may not remove Workstations, portable devices, or other Hardware or Electronic Media containing ePHI from the premises, unless properly authorized to do so.

A. Prior to moving Hardware or Electronic Media containing ePHI to a new location:
   i) A retrievable, exact copy of the ePHI is created, when needed, which is then managed as described in the ePHI Data Backup procedures, above.
   ii) The movement is recorded in the Data Management: Moving Media Log. Completed logs are forwarded on a regular basis to and maintained by Security Officer.

B. Backup copies of ePHI created for purposes of moving Hardware or Electronic Media shall be retained for a reasonable and appropriate period of time.

C. Before any disposal of Electronic Media containing ePHI, refer to ePHI Disposal Policy.

3. ***Documentation***. All documentation required by this policy is maintained for six years from the date of creation or the date when it was last in effect, whichever is later.

4. ***Violations and Non-Retaliation***
   A. Violation of any security policy or procedure by Workforce members may result in corrective disciplinary action, up to and including termination of employment. Violation of any security policy and procedures by others, including system users, providers, providers' offices, business associates or partners may result in termination of the relationship and/or associated privileges. Violation may also result in civil and criminal penalties as determined by federal and state laws and regulations.
   B. All Workforce members and other users are required to report suspected violations of the security policies and procedures to the Security Officer. Individuals reporting violations in good faith shall not be subjected to intimidation, threats, coercion, discrimination against, or any other retaliatory action as a consequence.

Resources:

1. BIT Information Technology Security Policy, Data Backup
2. WHITEC Data Management Policy
3. HIPAA COW Data Management and Backup Policy

Applicable Standards/Regulations:

1. 45 CFR § 160.103(a) HIPAA definition of Electronic Media (1/25/13)
2. 45 CFR § 164.308(a)(7)(ii)(A) HIPAA Security Rule Data Backup Plan
3. 45 CFR § 164.310(d)(1) HIPAA Security Rule Device and Media Controls
4. 45 CFR § 164.310(d)(2)(iii) HIPAA Security Rule Accountability
5. 45 CFR § 164.310(d)(2)(iv) HIPAA Security Rule Data Backup and Storage

Auditing Policy

Purpose

To establish auditing guidelines and safeguards to detect, report, and guard against:

- Breaches in confidentiality and security of patient protected health information
- Network vulnerabilities and intrusions
- Viruses, Trojan horses, and worms
- Performance problems and flaws in applications
- Improper alteration or destruction of Electronic Protected Health Information (ePHI) (information integrity)

Responsible for Implementation: Security Officer is responsible for implementing and overseeing this policy, in conjunction with BIT.

Policy

1. This Policy shall work in accordance with the Authentication, Authorization, and Auditing policy of the Information Technology (IT) Security Policy developed by BIT.

2. It is the policy of DHS to audit access to and activity of ePHI applications, systems, and networks and address standards set forth by the HIPAA Security Rule to ensure compliance with requirements to safeguard the privacy and security of ePHI.

3. To implement reasonable hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.

4. To make reasonable and good-faith efforts to safeguard the privacy and security of ePHI through a well-thought-out approach to auditing which is consistent with available resources.

5. To guard against, detect, and report viruses, Trojan horses, and worms.

Scope
This policy has been developed to address the organization-wide approach to information system auditing processes and protection against viruses, Trojan horses, and worms. It applies to organizational information applications, systems,

networks, and computing devices, regardless of ownership (e.g., owned, leased, contracted, and/or stand-alone).

Procedures

1. Security Officer, in conjunction with BIT, is responsible for overseeing the auditing of ePHI information system access and activity, and maintaining documentation related to completed audits and any follow up measures taken.

2. Users are informed that DHS audits their access to all of DHS's workstations, portable devices, servers, systems, and applications and will discuss with them any potential issues found on such audits.

3. Audits and reports of audits are limited to internal use on a minimum necessary, need-to-know basis.
   A. Audit results are intended to be disclosed only to senior leadership, and information which may expose organizational risk may only be shared with extreme caution.
   B. Audit results are not disclosed externally without senior leadership and/or legal counsel approval.
   C. Generic security audit information may be included in organizational reports only after ePHI is removed.

4. DHS makes reasonable and appropriate attempts to obtain and use ePHI systems, applications, and servers capable of generating user audit trail reports, sortable by user and patient and containing the following information: date, time, user name, what accessed, function in system where accessed, action taken, patient name, and medical record number. If audit reports cannot be generated, or contain only limited audit trail information, Security Officer evaluates and documents whether an upgrade is necessary or if a separate application can be utilized.

5. Auditing efforts are focused on areas of greatest risk, organizational resources, and vulnerabilities as identified in previous incidents, the security risk assessment, or other pertinent sources.

6. ***User ePHI Access Audits***
   A. Random user access audits are performed periodically (at least annually) to determine whether actual access to ePHI by workforce members is appropriate for the users' roles and in compliance with established guidelines. Information Services shall conduct such audits and document the following:
      i) Application, system, server, network, workstation, and patient and/or user audited.
      ii) Name of individual performing the audit.

iii) Date and time of audit.
iv) Observations and findings.
v) Corrective actions taken, if any. If it was determined that a breach or other security incident occurred, refer to the Incidents Policy – Security Incident Response.

B. User audits are also conducted in response to:
   i) Suspicion that a user has or may be attempting to inappropriately access ePHI, such as from a patient or employee complaint (refer to the Incidents Policy – Security Incident Response).
      (1) A request for an audit for specific cause must include time frame, frequency, and nature of the request. The request must be reviewed and approved by the Privacy Officer.
      (2) A request for an audit as a result of a patient concern is initiated only by the Privacy Officer. A copy of the audit information is not shared with patients or their guardians/legal representatives. The Privacy Officer communicates details of the audit results to the patient as described in the Incidents Policy – Breach Notification.
   ii) Selected high risk problem-prone events, such as a VIP encounter (e.g. board member, celebrity, governmental or community figure, etc.).

C. Workforce members are not to review audit logs pertaining to their own system activity or have the ability to alter or delete log entries pertaining to their own system activity, if possible. If not possible then management shall ensure that appropriate compensating controls are documented and implemented.

7. ***Log-in Monitoring***

A. Log-in monitoring capabilities are as follows:
   i) ePHI systems, applications, servers, and workstations used to store or transmit ePHI: capture of date and time of each log-on and each log-off attempt, and user name.
   ii) Networks: information on what is operating, penetrations, and vulnerabilities.

B. Log-in attempt reports are reviewed regularly to identify potential hackers.

C. Accounts automatically lock after a specified number of unsuccessful log-in attempts.

D. If a security incident occurred, or is believed to have occurred, refer to the Incidents Policy – Security Incident Response.

E. If log-in monitoring is not possible or DHS decides to not monitor the above mentioned log-in attempts as stated above, the Security Officer shall document the reasons/rationale.

F. Workforce members receive training on procedures for monitoring log-in attempts, including how to effectively use secure log-in processes and how to detect and report log-in discrepancies.

8. ***Protection from Malicious Software.***

A. Users may not open email attachments received from a suspicious sender.
B. Users may not download software without approval from the Security Officer.
C. Portable devices may not be introduced into the network before being scanned for viruses/malware.
D. DHS has anti-virus/malware software, patches, and firewalls in place to guard against, detect, and report viruses, Trojan horses, and worms.
    i) The IS department is responsible for ensuring anti-virus/malware, patches, and firewalls are current, effective, and documented.
    ii) Anti-virus/malware software is on all ePHI servers and workstations.
        (1) Server updates are automated.
        (2) Workstation and portable device (computers, laptops, etc.) updates are automated.
    iii) Patch updates.
        (1) Server, workstation, and portable device updates are automated.
        (2) Patch updates that are done manually are evaluated to ensure the updates do not inadvertently cause other problems.
    iv) Networks and servers are secured with a Firewall.
        (1) Network access is limited to legitimate or established connections.
        (2) Firewall console and other management ports are appropriately secured or disabled.
        (3) Firewall configuration used to protect networks are approved by BIT.
E. Security Officer, in conjunction with BIT, is authorized to select and use auditing tools that are designed to detect network vulnerabilities and intrusions. Such tools are explicitly prohibited by others without the explicit authorization of the Security Officer or BIT. Any contracted external auditors are independent of other organizational operations, have technical expertise in the type of audit conducted, and sign a Business Associate Agreement.

9. ***Documentation.***
A. Application/system audit logs are backed up as part of the application's regular backup procedure and maintained for at least six years, when possible.
B. Reports summarizing audit activities are maintained for six years.

10. ***Violations and Non-Retaliation***
A. Violation of any security policy or procedure by Workforce members may result in corrective disciplinary action, up to and including termination of employment. Violation of any security policy and procedures by others, including system users, providers, providers' offices, business associates or partners may result in termination of the relationship and/or associated privileges. Violation may also result in civil and criminal penalties as determined by federal and state laws and regulations.

B. All Workforce members and other users are required to report suspected violations of the security policies and procedures to the Security Officer. Individuals reporting violations in good faith shall not be subjected to intimidation, threats, coercion, discrimination against, or any other retaliatory action as a consequence.

Resources:

1. BIT Information Technology Security Policy, Authentication, Authorization, and Auditing Policy
2. WHITEC Auditing Policy
3. HIPAA COW Auditing Information System Activity Policy

Applicable Standards/Regulations:

1. 45 CFR § 164.308(a)(1)(ii)(D) HIPAA Security Rule Information System Activity Review
2. 45 CFR § 164.308(a)(5)(ii)(B) HIPAA Security Rule Protection from Malicious Software
3. 45 CFR § 164.308(a)(5)(ii)(C) HIPAA Security Rule Log-in Monitoring
4. 45 CFR § 164.312(b) HIPAA Security Rule Audit Controls

HIPAA Security Oversight Policy

Purpose

DHS is dedicated to maintaining the Confidentiality, Integrity, and Availability of Protected Health Information (PHI) and Electronic Protected Health Information (ePHI) and protecting against any reasonably anticipated threats, hazards, and/or inappropriate access, acquisition, use~~s~~ or disclosure. It is the goal of DHS to make all reasonable and appropriate attempts to maintain the Confidentiality, Integrity, and Availability of PHI and ePHI. This policy establishes overarching security measures used to achieve this goal.

Responsible for Implementation: The Security Officer is responsible for implementing and overseeing this policy and procedure, in conjunction with BIT.

Policy

1. To maintain the Confidentiality, Integrity, and Availability of all ePHI DHS creates, receives, maintains, and/or transmits.

2. To have in place appropriate development, implementation, and oversight of DHS's efforts to comply with the requirements of the HIPAA Security Rule.

3. To continuously monitor security policies, procedures, and existing measures, and update them as needed to better protect ePHI.

Procedures

1. ***Decision Making Process for Security Measures***
   A. Decisions regarding security measures DHS puts in place are based on the size, complexity, technical infrastructure, and capabilities of DHS; the costs of the security measures; and the likelihood of such measures to effectively reduce risk levels.
   B. Addressable Security Rule implementation specifications are assessed as to whether they are reasonable and appropriate safeguards when analyzing the likely contributions to protecting ePHI.
      i) Reasonable and appropriate safeguards are implemented.
      ii) For safeguards deemed not reasonable and appropriate, Security Officer documents rationale and implements equivalent alternative measures if reasonable and appropriate.

2. ***Security Officer Responsibilities***. The Security Officer is responsible for facilitating the development, implementation, and oversight of all activities pertaining to DHS's efforts to comply with the requirements of the HIPAA

Security Rule and maintain the Confidentiality, Integrity, and Availability of ePHI. Such responsibilities include but are not limited to the following:

A. Overseeing the development, implementation, auditing, and enforcement of, and adherence to, DHS's security policies and procedures.
B. Monitoring changes in applicable laws and regulations, new or recently upgraded systems, and identified significant risks; and verifying that security safeguards meet the requirements of the Security Rule while balancing business needs and capabilities to maintain the Confidentiality, Integrity, and Availability of ePHI.
C. Serving as a resource for Workforce regarding the privacy and security of ePHI.
D. Working with Workforce members, vendors, outside consultants, and other third parties to continuously improve security within DHS.
E. Developing, reviewing, updating, and maintaining appropriate written policies and procedures to comply with the Security Rule, and disseminating to workforce members.
F. Facilitating audits to validate Security Rule compliance efforts throughout DHS.
G. Overseeing the documentation of all other security measures, activities, and assessments completed to comply with the Security Rule.
H. Ensuring and documenting that proper security training is provided to Workforce members and ePHI system users, as necessary and appropriate to carry out job functions.
I. Implementing procedures for the authorization and/or supervision of Workforce members who work with ePHI or in locations where ePHI may be accessed.
J. Reporting security efforts and incidents to senior leadership in a timely manner.
K. Assisting in the administration and oversight of Business Associate Agreements.

3. ***Availability of Policies and Procedures***.
   A. DHS's security policies and procedures are available for reference and review by Workforce members with access to ePHI.
   B. Other security documentation is available to those individuals required to follow and implement them, as applicable and appropriate.

4. ***Workforce Security Training***.
   A. Training on DHS's security policies and procedures, as necessary and appropriate to carry out job functions and maintain the Confidentiality, Integrity, and Availability of ePHI, is required for all Workforce members with access to ePHI, and includes the name and contact information of Security Officer and location of security policies and procedures.
   B. Training and updates

i) New Workforce members receive security training as soon as possible but no more than 30 days after date of hire.
ii) Workforce members receive annual security training.
iii) Training updates on material changes to the security policies and procedures are provided within 30 days of the effective date of such material change.

C. Workforce members may not access, use, or disclose ePHI until security training requirements have been met.
D. Workforce members receive security reminders periodically and as needed, such as how to protect workstations and ePHI from unauthorized access, safeguarding passwords, malicious software and virus alerts, etc. Such reminders may be communicated via email, posters, meetings, online postings, newsletter articles, or other methods as appropriate.
E. Workforce members responsible for maintaining workstations, servers, networks, etc., receive additional security training as appropriate to maintain the security of these systems.
F. Training documentation, including the training content provided, date provided, and method provided, is maintained by the Security Officer for six years.

5. ***Violations and Non-Retaliation***
   A. Violation of any security policy or procedure by Workforce members may result in corrective disciplinary action, up to and including termination of employment. Violation of any security policy and procedures by others, including system users, providers, providers' offices, business associates or partners may result in termination of the relationship and/or associated privileges. Violation may also result in civil and criminal penalties as determined by federal and state laws and regulations.
   B. All Workforce members and other users are required to report suspected violations of the security policies and procedures to the Security Officer. Individuals reporting violations in good faith shall not be subjected to intimidation, threats, coercion, discrimination against, or any other retaliatory action as a consequence.

Resources:

1. BIT Information Technology Security Policy, Security Awareness Policy
2. WHITEC HIPAA Security Oversight Policy
3. HIPAA COW HIPAA Security Oversight Policy

Applicable Standards/Regulations:

1. 45 CFR §164.308(a)(2) HIPAA Security Rule Assigned Security Responsibility
2. 45 CFR §164.306(a) HIPAA Security Rule General Requirements
3. 45 CFR §164.306(b) HIPAA Security Rule Flexibility of Approach
4. 45 CFR §164.306(e) HIPAA Security Rule Maintenance
5. 45 CFR §164.308(a)(1)(ii)(c) HIPAA Security Rule Sanction Policy

6. 45 CFR §164.308(a)(3)(ii)(A) HIPAA Security Rule Authorization and/or Supervision
7. 45 CFR §164.308(a)(5)(i) HIPAA Security Rule Security Awareness and Training
8. 45 CFR §164.308(a)(5)(ii)(A) HIPAA Security Rule Security Reminders
9. 45 CFR §164.316(a) HIPAA Security Rule Policies and Procedures
10. 45 CFR §164.306(b)(1) HIPAA Security Rule Documentation
11. 45 CFR §164.306(b)(2)(i) HIPAA Security Rule Time Limit
12. 45 CFR §164.306(b)(2)(ii) HIPAA Security Rule Availability
13. 45 CFR §164.316(b)(2)(iii) HIPAA Security Rule Documentation Updates

Incidents Policy: Security Incident Response, Breach Notifications, and Sanctions

Purpose
The purpose of this policy is to establish consistent guidelines to handle Security Incidents, sanctions, and Breach of Unsecured PHI notifications. An information Security Incident response process is implemented to consistently detect, respond, and report incidents, minimize loss and destruction, mitigate the weaknesses that were exploited, restore information system functionality and business continuity as soon as possible, and provide Breach of Unsecured PHI notifications as required. Consistent sanctions are provided as required by the HIPAA Security Rule and are meant to deter non-compliance with security safeguards in place. When feasible, the handling of Security Incidents under this policy shall conform with the security incident procedures of the Bureau of Information & Telecommunications Cyber Security Incident Response Plan.

Responsible for Implementation:
The Security Officer is responsible for implementing and overseeing this policy and procedure, in conjunction with BIT.

Security Incident Response Team (SIRT) is responsible for responding to Security Incidents. The SIRT includes: The Security Officer, Privacy Officer, and BIT personnel as necessary and appropriate.

Policy
1. This Policy shall work in accordance with the Cyber Security Incidents policies of the Information Technology (IT) Security Policy developed by BIT.

2. It is the policy of DHS to safeguard the confidentiality, integrity, and availability of Electronic Protected Health Information (ePHI) through an established information Security Incident response process.

3. To consistently detect, respond to, and report security issues; minimize loss and destruction as well as mitigate other harmful effects; restore information system functionality and business continuity as soon as possible; and make reasonable efforts to try to prevent incidents from reoccurring.

4. To quickly identify a Breach of Unsecured PHI and provide required notifications within the timeframe required by law.

5. To provide consistent sanctions for non-compliance of the Security Rule and DHS's security policies and procedures.

Procedures

Security Incident Response Procedures

1. ***Identification Phase***:
   A. Security Officer identifies security violations, Security Incidents, and Breaches from:
      i) Workforce members and other system users who are required to report suspected and known security violations, Security Incidents, and Breaches immediately upon observation.
      ii) Individuals or organizations outside of DHS who may report security issues or concerns.
      iii) Proactive monitoring of DHS's network and information system activities.
   B. Upon receipt of a reported Security Incident, Security Officer does the following:
      i) Documents Security Incident and takes steps to investigate, escalate, and remediate, working with others as appropriate.
      ii) Involves members of the Security Incident Response Team (SIRT) as applicable to the type and severity of the issue.
      iii) Follows the Breach of Unsecured PHI notification procedures, if the issue involves a known or suspected Breach of PHI.
      iv) Keeps senior leadership apprised of the issue and progress to resolve it, as appropriate.
      v) If technical assistance is required, moves to the Containment Phase below.
      vi) If technical assistance is not required: completes the investigation, implements preventative measures, resolves the Security Incident, and moves to the Follow-up Phase below.

2. ***Containment Phase (if technical assistance is required):***
   A. The Security Officer, in collaboration with appropriate members of the SIRT, does the following to contain the Security Incident, as applicable:
      i) Verifies that qualified technical security resources are available to assist.
      ii) Employs a combination of technical controls to limit damage as appropriate.
      iii) Secures the physical and network perimeter.
      iv) Backs up the system if appropriate.
      v) Changes the password(s) to the affected system(s).
      vi) Determines whether it is safe to continue operations with the affected system(s).
         (1) If safe, allows the system to continue to function, completes documentation as described below, and moves to Follow-up Phase.
         (2) If not safe, discontinues system(s) operation and moves to Eradication Phase.
   B. SIRT apprises senior leadership of progress made and documents all measures taken.
3. ***Eradication Phase:***

A. The Security Officer, in collaboration with the SIRT, does the following to remove the cause Security Incident and the resulting security exposures on the affected system(s), as applicable:
   i) Determines symptoms and cause related to the affected system(s).
   ii) Strengthens the defenses surrounding the affected system(s), where possible.
   iii) Implements appropriate corrective actions (such as patches, updates, configuration changes, training, etc.) while considering patient care, business continuity, and the need to safeguard the confidentiality, integrity, and availability of ePHI.
   iv) Conducts a risk assessment to verify that all exploitable vulnerabilities have been addressed.
B. SIRT apprises senior leadership of progress made and documents all measures taken.
C. Continue to the Recovery Phase.

4. ***Recovery Phase:***
   A. The Security Officer, in collaboration with the SIRT, does the following:
      i) Determines if affected system(s) has been changed after the security exposures, if any, have been corrected.
      ii) Restores the system(s) to its proper and intended functioning.
      iii) If the system was not changed in any way but was taken offline (i.e., operations had been interrupted), restarts the system and monitors for proper behavior.
   B. SIRT apprises senior leadership of progress made and documents all measures taken.
   C. Continue to Follow-up Phase

5. ***Follow-up Phase:***
   A. Security Incidents are reviewed shortly after resolution to determine where response process could be improved for future incidents.
   B. The Security Officer, in collaboration with the SIRT, does the following:
      i) Evaluates the cost and impact of the Security Incident to DHS.
      ii) Implements any appropriate measures to reduce likelihood of similar reoccurrences.
      iii) Documents any lessons learned during the security incident response process.
      iv) Communicate findings to senior leadership for approval and for implementation of any recommendations.

<u>Breach of PHI Procedures</u>

6. A ***Breach*** is the use or disclosure of unsecured PHI in a manner not permitted by HIPAA, unless a risk assessment demonstrates a low probability that the PHI was compromised. Upon discovery of a potential Breach, Privacy Officer begins an investigation and does the following:

A. Conducts a Breach risk assessment to determine if an impermissible use or Disclosure of PHI constitutes a Breach of Unsecured PHI and whether individuals, media, or the HHS secretary must be notified.
   i) The Breach risk assessment must include the following factors (use the "Breach Risk Assessment Tool" to complete this assessment):
      (1) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
      (2) The unauthorized person who used the PHI or to the Disclosure was made;
      (3) Whether the PHI was actually acquired or viewed; and
      (4) The extent to which the risk to the PHI has been mitigated.
   ii) If a risk assessment is not completed, DHS must presume the impermissible use or Disclosure of PHI rises to the level of a Breach of Unsecured PHI and is required to send notification(s), as outlined below.

B. Documents the Breach risk assessment and investigation, including any outcomes.

7. ***Discovery of Breach:*** A Breach of Unsecured PHI is treated as discovered as of the date DHS or DHS's agent discovers the Breach, or should have discovered the Breach by exercising appropriate diligence.

8. ***Business Associate Responsibilities***:
   A. A Business Associate (BA) of DHS that Accesses, creates, maintains, retains, modifies, records, stores, transmits, destroys, or otherwise holds, uses, or discloses Unsecured PHI shall notify DHS of a Breach without unreasonable delay and in no case later than 60 calendar days after discovery of the Breach.
   B. BA's notice to DHS shall include:
      i) The identification of each individual whose Unsecured PHI was, or is reasonably believed by the BA to have been acquired, Accessed, used, or Disclosed in an unauthorized manner.
      ii) Any other available information that DHS is required to include in notification to the individual at the time of the notification or promptly thereafter as information becomes available (refer below).
   C. DHS will make any required notifications described below, unless otherwise agreed that BA will do so. DHS must document that notifications have been made.

9. ***Breach Notifications***.
   A. *Timeliness.*
      i) Upon determination that a Breach notification is required, the notice shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of the Breach.
      ii) If a Law Enforcement Official informs DHS that a notification, notice, or posting would impede a criminal investigation or cause damage to

national security, notification shall be delayed for the time period specified in writing by the official, or for up to 30 days if time period not specified in writing.

B. *Content of the Notice*: The notice shall be written in plain language and contain the following information:
   i) A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known.
   ii) A description of the types of Unsecured PHI involved in the Breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved).
   iii) Any steps the individual should take to protect themselves from potential harm resulting from the Breach.
   iv) A brief description of what DHS is doing to investigate the Breach, to mitigate harm to individuals, and to protect against further Breaches.
   v) Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, Web site, or postal address.

C. *Methods of Notification*: The method of notification depends on the individuals or entities to be notified, as follows:
   i) Notifications to Individual(s). Utilize the Sample Notification Letter to Patients and provide them in the following form:
      (1) *Written notification* by first-class mail to the individual at his/her last known address or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by secure electronic mail.
         (a) The notification may be provided in one or more mailings as more information becomes available.
         (b) If DHS knows that the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by first-class mail to the next of kin or person representative.
      (2) *Substitute Notice*: When there is insufficient or out-of-date contact information (including an address, phone number, email address, etc.) that prevents direct written or electronic notification, a substitute form of notice reasonably calculated to reach the individual is provided. A substitute notice does not need to be provided when there is insufficient or out-of-date contact information that prevents written notification to the individual and next of kin or personal representative.
         (a) When there is insufficient or out-of-date contact information for fewer than 10 individuals, then the substitute notice may be provided by an alternative form of written notice, telephone, or other means.
         (b) When there is insufficient or out-of-date contact information for 10 or more individuals, then the substitute notice is in the form of

either a conspicuous posting for a period of 90 days on DHS's website home page, or a conspicuous notice in a major print or broadcast media in DHS's geographic areas where the individuals affected by the Breach likely reside. Include a toll-free number in the notice that remains active for at least 90 days where an individual can learn whether his or her PHI may be included in the Breach. This substitute notice must be provided as soon as reasonably possible and in no case later than 60 calendar days from discovery of the breach.

(3) If the notification requires urgency because of possible imminent misuse of Unsecured PHI, notification may be provided by telephone or other means, as appropriate in addition to the methods noted above.

ii) Notifications to the Media:

(1) Notifications must be provided to prominent media outlets serving the state and regional area (of the breached individuals) when the Breach of Unsecured PHI affects more than 500 of the individuals of a State or jurisdiction. What constitutes a prominent media outlet may differ depending upon the State or jurisdiction where the affected individuals reside and must be determined on a case by case basis.

(2) The Notice is provided in the form of a press release to the media by the individual stated in the above Working with the Media procedures, utilizing the Sample Notification Letter to the Media.

(3) Individual identifiers ***are not included*** in these notifications as they are publically available.

iii) Notifications to the Secretary of HHS: Notifications of Breaches must be provided to the Secretary of HHS as follows:

(1) For Breaches involving 500 or more individuals, the Secretary of HHS is notified as instructed at www.hhs.gov at the same time notice is made to the individuals.

(2) For Breaches involving less than 500 individuals, such Breaches are entered in the Breach Notification Log and submitted during the calendar year or no later than 60 days after the end of that calendar year in which the Breaches were discovered (e.g., 2014 Breaches submitted by 3/1/2015). Instructions for submitting the logged Breaches are provided at www.hhs.gov.

(3) Individual identifiers ***are not included*** in these notifications as the information may be made publically available.

Investigation Procedures

10. The Security Officer promptly facilitates a thorough investigation of all reported security violations and incidents, including Breaches, and documents the investigation actions taken.

A. Investigation assistance may be requested from Workforce members and other system users.

B. Workforce members must cooperate with incident response investigations and resolutions and provide factual information.

11. The Security Officer works to prevent recurrence of security violations and incidents whenever possible and feasible. Actions taken may include, but are not limited to, revising security policies and procedures, providing training to workforce members and system users, changing/reducing access levels to PHI, requiring the return or destruction of PHI, and improving technical security controls.

Working with News Media

12. Refer all contact with news media related to any actual or potential security violation and incident, or Breach of ePHI, to the public relations department who serves as the media liaison between DHS and the news media.
13. Releases to news media shall not include any ePHI unless proper written authorization from patient(s) to release such ePHI has been received.
14. Contact legal counsel if unsure if there are legal issues before communicating with news media.

Training

Workforce members and system users are trained:

15. On the privacy and security policies and procedures with respect to PHI and ePHI as necessary and appropriate to carry out their job responsibilities and prevent security violations and incidents from happening.
16. On how to identify and promptly report known and suspected security violations, incidents, and Breaches within DHS, as well as return or destroy PHI, as appropriate for the incident.
17. Workforce members that assist in investigating, documenting, and resolving breaches are trained on how to complete these activities.

Document Retention

18. The Privacy Officer, Security Officer and/or SIRT maintains all documentation, related to the following, in a secure location for a period of six years after the conclusion of the investigation:
    A. Security Incident documentation, including all incident response forms, notes, meeting minutes and other items relevant to the investigation.
    B. All documentation related to Breach of Unsecured PHI investigations, including the risk assessment and notifications made. Note: DHS has the burden of proof for demonstrating that all notifications were made or that an Access, acquisition, use, or Disclosure did not constitute a Breach, as well as evidence demonstrating the necessity of a delay authorized by Law Enforcement (when applicable).
    C. All documentation of security violation investigations, sanctions provided, and actions taken to prevent future occurrences.

Violations, Sanctions and Non-Retaliation

19. Violation of any security policy or procedure by Workforce members may result in corrective disciplinary action, up to and including termination of employment. Violation of any security policy and procedures by others, including system users, providers, providers' offices, business associates or partners may result in termination of the relationship and/or associated privileges. Violation may also result in civil and criminal penalties as determined by federal and state laws and regulations.
20. The security policies and procedures are enforced consistently across DHS, and sanctions imposed as a result of violations of the security policies and procedures are imposed consistently across DHS. Sanctions such as disciplinary actions are determined on a case by case basis, taking into account the specific circumstances and severity of the violation. Sanctions imposed may include verbal or written warnings, required retraining, or termination of employment.
21. All Workforce members and other users are required to report suspected violations of the security policies and procedures to the Security Officer. Individuals reporting violations in good faith shall not be subjected to intimidation, threats, coercion, discrimination against, or any other retaliatory action as a consequence.

Resources:

1. BIT Information Technology Security Policy, Cyber Security Incidents Policy
2. BIT Information Technology Security Policy, Preventing and Responding to Cyber Security Incidents Policy
3. WHITEC Incidents Policy
4. HIPAA COW Security Incident Response Policy
5. HIPAA COW Breach Notification – Protected Health Information For Covered Entities Policy
6. HIPAA COW Security Oversight Policy/Procedure
7. SANS Sample Incident Handling Forms

Applicable Standards/Regulations:

1) Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act (Final Omnibus Rule)
2) FTC Breach Notification Rules - 16 CFR Part 318
3) 45 CFR Parts 160 and 164 – HIPAA Privacy and Security Rules
4) 45 CFR § 164.308(a)(1) HIPAA Security Rule Information System Activity Review
5) 45 CFR § 164.308(a)(1) HIPAA Security Rule Security Management Process
6) 45 CFR § 164.308(a)(6)(i) HIPAA Security Rule Security Incident Procedures
7) 45 CFR § 164.308(a)(6)(i)(ii) HIPAA Security Rule Response and Reporting
8) 45 CFR § 164.308(a)(1)(ii)(C) HIPAA Security Rule – Sanction Policy
9) WI § 134.98 Notice of Unauthorized Acquisition of Personal Information (Note: Not applicable to Covered Entities Under HIPAA)

System Access Policy

Purpose

To establish guidelines to protect Electronic Protected Health Information (ePHI) from unauthorized access, use, disclosure, and modification, as well as safeguards to prevent theft of Workstations and other equipment that stores and/or transmits this information.

Responsible for Implementation: The Security Officer is responsible for implementing and overseeing this policy and procedure, in conjunction with BIT.

Policy

1. This Policy shall work in accordance with the Access Control policy of the Information Technology (IT) Security Policy developed by BIT.

2. To safeguard the confidentiality, integrity, and availability of Electronic Protected Health Information (ePHI) by controlling access to ePHI.

3. To provide only the Minimum Necessary access to ePHI to all users, including Workforce members, volunteers, business associates, contracted providers, consultants, and any other entities.

4. To prevent unauthorized access, use, disclosure, modification, and theft through Workstation and Information System security safeguard controls.

Procedures

Supervision and Clearance

1. DHS takes reasonable and appropriate steps to ensure that workforce members who work with ePHI or in locations where ePHI might be accessed are properly authorized and/or supervised. Such steps may include but are not limited to the following:
   A. Ensuring that Workforce members and other system users follow DHS's security policies and procedures.
   B. Ensuring that user access to ePHI is the Minimum Necessary to perform job responsibilities.
   C. Monitoring Workstations, systems, applications, and facilities for unauthorized use, tampering, and theft of ePHI.
   D. Documenting a process for granting authorization and access to ePHI, including:

i) Procedures for granting different levels of access to ePHI and to areas where ePHI might be accessed.
ii) Documenting authorization of Workforce members' and other users' access to ePHI and to areas where EPHI might be accessed.

E. Not allowing Workforce members to access ePHI or areas where ePHI might be accessed until proper authorization is granted.

2. Before individuals are granted access to DHS's Information Systems, HR Department performs certain background checks as necessary and appropriate, notifies System Administrator(s) of completion, and maintains proper documentation. Such background checks may include:
   i) Office of Inspector General (OIG) Exclusion List (monthly checks recommended)
   ii) Relevant credentialing agencies
   iii) State criminal history record search

Information System Access

3. ***Granting Access***: Appropriate role based access is provided to all Information System users. Such access is granted through adherence to procedures for establishing, documenting, reviewing, and modifying a user's right of access to systems that may contain or transmit ePHI.
   A. Access levels for Information Systems are based on job role classifications.
      i) Only System Administrator may grant access requests and create/assign access to Information Systems.
      ii) Supervisors or designees are responsible for requesting and authorizing access to Information Systems for subordinate users, by submitting written access requests to System Administrator prior to user start date.
      iii) Workforce members are not permitted to authorize their own access to ePHI, create their own access roles, or seek access authorization from another supervisor.
      iv) The level of access granted to Information System users is based on the Minimum Necessary amount of ePHI required to carry out job role responsibilities. Blanket access is not provided for any user.
   B. The System Administrator facilitates the following for all Information Systems, including Workstations, that store or transmit ePHI, or otherwise provide access to ePHI:
      i) Approve access levels/roles as well as requests for changes in access levels/roles.
      ii) Maintain documentation on Information System roles, including type of access provided and list of users assigned to each role.
      iii) Maintain documentation on requests for access, including type of access requested and by whom, date/time access was set up and by whom, and role assigned to user.
   C. Users may only access, use, and disclose the Minimum Necessary of ePHI needed to perform assigned job responsibilities, and only as permitted or required by DHS's policies and applicable laws.

4. ***Modifying Access***: When a user's job role responsibilities change and/or user's access to an Information System is no longer necessary:
   A. User's supervisor or designee submits, prior to commencement of new job responsibilities, a written access modification request to System Administrator specifying the change in user's job role/access level.
   B. System Administrator processes the request and modifies the user's access:
      i) Consistent with the new access needs, and
      ii) Based on existing job classification roles or by creating a new job role/access level if necessary.
   C. System Administrator documents the access modification, including:
      i) Name of the person who made the change request
      ii) Name of the person who changed the access
      iii) The date and time access was changed
      iv) Previous and new job role/access levels assigned to user
   D. System Administrator, in collaboration with the Security Officer, periodically reviews the list of users with ePHI access to ensure consistency with authorized roles and to maintain the Minimum Necessary access, making and documenting changes as necessary and appropriate.

5. ***Terminating Access:*** When a user's access to DHS's Information Systems is no longer required due to termination of the relationship with DHS:
   A. The HR Department immediately completes and submits a written access termination request to System Administrator to deactivate the user's access. In cases requiring immediate deactivation of Information System access, System Administrator may be contacted via telephone to expedite access termination request.
   B. System Administrator processes the request and terminates the user's access.
   C. User access may also be terminated as necessary and appropriate, such as when:
      i) The user has been using access rights inappropriately;
      ii) The user's password has been compromised (a new password may be provided if the user was not responsible for the original password being compromised); or
      iii) An unauthorized individual is utilizing a user's User Login ID and password (a new password may be provided if the user was not responsible for the unauthorized individual obtaining the User Login ID and password).
   D. System Administrator documents the access termination, including:
      i) Name of the person who made the termination request
      ii) Reason for the termination
      iii) Name of the person who terminated the access
      iv) The date and time access was terminated

Workstation Log-Offs

6. Users are required to lock or logoff Workstations, portable devices, and Information Systems when left unattended to ensure that ePHI may not be accessed by unauthorized individuals. Users are to lock their workstation screens or lock down their equipment when leaving their work area.
7. Workstations utilize inactivity time-outs, where applicable, that automatically clear the workstation screen after a defined period of inactivity to prevent unauthorized access to ePHI, requiring user to be authenticated again in order to regain access. This feature is set by the System Administrator and may not be changed by users.
8. Information Systems that store, transmit, or otherwise provide access to ePHI automatically log users off the systems after a defined period of inactivity. Exceptions for systems that do not have this capability are authorized and documented by the Security Officer.
9. User accounts automatically lock after a specified number of invalid login attempts, where applicable, and are reset by System Administrator.

Passwords

10. Workstation access requires a unique User Name and Password (UN & PW) for each individual user, including System Administrators. Exceptions are authorized and documented by the Security Officer.
11. Access to Information Systems that contain or transmit ePHI requires a unique UN & PW for each individual user so that access may be tracked.
12. Users may not:
    A. Share UNs & PWs with anyone, including co-workers, unless properly instructed to do so by an authorized supervisor for a legitimate purpose (such as training or addressing system issues).
    B. Leave UNs & PWs where someone else may see/find them.
    C. Use the UNs & PWs of others, or any Information System logged in under another user's UN & PW.
13. Users are responsible for all inquiries, entries, and changes made to any of DHS's Information Systems using their UNs & PWs.
14. If a user cannot recall their UN & PW, the System Administrator is contacted to provide the user with a temporary, one-time use UN & PW.
15. Information System passwords are masked or suppressed on all online screens, are never printed or included in reports or logs, and are stored in an encrypted format.
16. The following password controls are put in place for all Information Systems and documented by the Security Officer:
    A. Password strength:
        i) Minimum of eight characters, containing a combination of upper and lower case alphabetic characters, numeric characters, and special characters.
        ii) May not include anything personal or easily guessable (family member or pet names, dictionary words, SSN, birth dates, etc.).

B. Users change passwords after first log-in, if a password was provided by the Administrator.
C. Users change passwords every 90 days and compromised passwords are changed immediately.
D. Users may not reuse recently used passwords.
E. For Information Systems that do not have these capabilities, the highest level of password controls available are utilized with password controls being improved as soon as reasonably practical.

Workstation Use and Security

17. All Workstations and equipment purchased by DHS are the property of DHS. Any information accessed or created by user during user's relationship with DHS is the property of DHS and not the user.
18. Users are responsible for taking reasonable precautions to protect the confidentiality, integrity, and availability of ePHI at all times.
    A. Users must monitor Workstations and take measures to prevent unauthorized access and theft.
    B. Users must minimize the Information System or otherwise secure it so ePHI is not viewable when others not authorized to access such ePHI are nearby.
19. Users may not allow unauthorized individuals to use any of DHS's Workstations or Information Systems.
20. Workstations are placed in secure areas away from non-Workforce traffic, and monitors/Workstations are positioned to prevent unauthorized viewing of ePHI.
21. Users may not download ePHI from DHS's Information Systems to store or use on any other system or computer, portable device, or removable storage device unless properly authorized to do so.
22. Users may not:
    A. Download any software to a Workstation without authorization from the Security Officer.
    B. Use tools or techniques to break/exploit security measures.
    C. Connect to unauthorized networks through DHS's systems or devices.
23. Workstations and Information Systems may only be used for authorized business purposes, and may not be used for personal gain or to transmit, retrieve, or store any derogatory, inflammatory, abusive, illegal, unethical, or otherwise inappropriate communications.
24. Laptops and other portable devices may be taken offsite when approved by authorized supervisor and only as needed to perform assigned job responsibilities.
    A. Users are responsible for such devices and shall protect them with security controls equivalent to those for on-site Workstations.
    B. Users must not store ePHI on portable devices unless ePHI is appropriately protected/encrypted.
    C. Locking software for unattended laptops must be activated.
    D. Portable devices must be concealed and/or locked when transported, such as in trunk of car.

Health Care Clearinghouse

25. DHS is not a health care clearinghouse and therefore does not have, and is not required to have, security procedures pertaining to a health care clearinghouse.

Documentation

26. All documentation related to this policy and procedures is maintained for a minimum of six years from the date of creation or date it was last in effect, whichever is later.

Violations and Non-Retaliation

27. Violation of any security policy or procedure by Workforce members may result in corrective disciplinary action, up to and including termination of employment. Violation of any security policy and procedures by others, including system users, providers, providers' offices, business associates or partners may result in termination of the relationship and/or associated privileges. Violation may also result in civil and criminal penalties as determined by federal and state laws and regulations.
28. All Workforce members and other users are required to report suspected violations of the security policies and procedures to the Security Officer. Individuals reporting violations in good faith shall not be subjected to intimidation, threats, coercion, discrimination against, or any other retaliatory action as a consequence.

Resources:

1. BIT Information Technology Security Policy, Access Control Policy
1. BIT Information Technology Security Policy, Password Requirements
2. HIPAA COW System Access Policy
3. WHITEC Auditing Policy

Applicable Standards/Regulations:

1. 45 CFR §164.308a4iiC HIPAA Security Rule Access Establishment and Modification
2. 45 CFR §164.308(a)(3)(i) HIPAA Security Rule Workforce Security
3. 45 CFR §164.308(a)(3)(ii)(A) HIPAA Security Rule Authorization and/or Supervision
4. 45 CFR §164.308(a)(3)(ii)(B) HIPAA Security Rule Workforce Clearance Procedures
5. 45 CFR §164.308(a)(3)(ii)(C) HIPAA Security Rule Termination Procedures
6. 45 CFR §164.308(a)(4)(i) HIPAA Security Rule Information Access Management
7. 45 CFR §164.308(a)(4)(ii)(A) HIPAA Security Rule Isolating Healthcare Clearinghouse Function
8. 45 CFR §164.308(a)(4)(ii)(B) HIPAA Security Rule Access Authorization
9. 45 CFR §164.308(a)(4)(ii)(C) HIPAA Security Rule Access Establishment and Modification
10. 45 CFR §164.308(a)(5)(ii)(D) HIPAA Security Rule Password Management
11. 45 CFR §164.310(b) HIPAA Security Rule Workstation Use
12. 45 CFR §164.310(c) HIPAA Security Rule Workstation Security
13. 45 CFR §164.312(a)(1) HIPAA Security Rule Access Control
14. 45 CFR §164.312(d) HIPAA Security Rule Person or Entity Authentication

15. 45 CFR §164.312(a)(2)(i) HIPAA Security Rule Unique User Identification
16. 45 CFR §164.312(a)(2)(iii) HIPAA Security Rule Automatic Logoff

Business Associate Policy

Purpose

To establish guidelines to identify vendor/business relationships which are Business Associates and Subcontractors, to provide direction in establishing formalized Business Associate Agreements, and to meet the requirements of the relationship between DHS and its Business Associate.

Responsible for Implementation: The Privacy Officer, in conjunction with Contracts and the Security Officer as appropriate, is responsible for implementing and overseeing this policy and procedure.

Policy

1. This Policy shall work in accordance with the Contracts with Third Parties section of the Information Technology (IT) Security Policy developed by BIT.

2. It is the policy of DHS to implement the required Business Associate contract procedures and ensure documentation to establish satisfactory assurance of compliance with the HIPAA Privacy and Security Rules, as well as HITECH.

3. To have Business Associate Agreements in place with Business Associates which establish appropriate safeguards Business Associates must have in place for Protected Health Information (PHI) and Electronic Protected Health Information (ePHI).

4. To protect the confidentiality, integrity, and availability of ePHI by permitting a Business Associate to create, receive, maintain, or transmit ePHI on DHS's behalf only if a written agreement between DHS and the Business Associate is in which provides assurances that Business Associate will appropriately safeguard such ePHI.

Attachments

Attachment 1: Examples of Business Associates and Subcontractors
Attachment 2: Examples of Arrangements that are not Business Associate Relationships

Procedures

1. Before entering into any agreement, contract, or other business relationship with any vendor or contractor, Workforce member contacts the Privacy Officer to assess whether a Business Associate Agreement (BAA) is needed.

2. Privacy Officer assesses whether a BAA is required, based on the HIPAA definition of a Business Associate (BA) and whether the vendor/contractor

creates, receives, maintains, and/or transmits PHI or ePHI on behalf of DHS. If vendor/contractor does so then a BAA is required.

3. Privacy Officer may refer to Attachment 1 (Examples of Business Associates and Subcontractors) and Attachment 2 (Examples of Business Associates and Examples of Arrangements that are not Business Associates Relationships) for guidance in determining if a BA relationship exists and a BAA is required.

4. If a BA relationship exists then Privacy Officer initiates process of obtaining a signed BAA.
   A. If possible DHS's currently approved BAA template is utilized.
   B. If a vendor/contractor relationship requiring a BA is in the process of contract negotiation and development, the provisions of the BAA may be incorporated into the contract between the parties, or provided as a separate document referencing such contract.
   C. The following information is entered into DHS's BAA template, before providing it to the vendor/contractor:
      i) Permitted uses and disclosures of PHI/ePHI by BA, as applicable to the arrangement.
      ii) Limitations on the use and disclosure of PHI/ePHI by BA, as applicable to the arrangement.
      iii) The name and address of the BA, as well as the name of the individual that will sign it.

5. Negotiating and/or signing of a different organization's BAA
   A. In the following situations, the Privacy Officer may be requested to review a BAA from a different organization to ensure that the provisions outlined are consistent with those set forth in this policy and DHS's BAA template, and that such BAA contains all provisions required by the Privacy and Security Rules and HITECH:
      i) DHS may serve as a BA to another organization and may be asked to review and sign that organization's BAA.
      ii) A vendor/contractor may request changes be made to DHS's BAA.
      iii) After several attempts, a vendor/contractor may refuse to sign DHS's BAA and require DHS to sign their BAA.
   B. If the reviewed BAA is not consistent with this policy, DHS's BAA, and/or contains additional provisions or provisions that are inconsistent with the regulations, then Privacy Officer may proceed with the following alternatives:
      i) Agree to the additional or different provisions and have the BAA signed, if the inconsistencies are legal and acceptable.
      ii) Refuse to agree to the provisions and work with the other organization to resolve the issue.
      iii) Refer the BAA to legal counsel to determine appropriateness before signing.

6. If DHS changes the provisions of its in-force BAA's (due to legal or organizational changes), then Privacy Officer facilitates the signing of either new BAA's or BAA addenda by DHS's BA's, as necessary and appropriate.

7. Privacy Officer, in conjunction with the Security Officer as appropriate, shall facilitate the following:
   A. Responding to potential privacy and security violations and breaches when reported by a BA.
      i) Working with the BA to take reasonable steps to cure any potential violation or end the violation.
      ii) Requesting the BA to provide information as to how and why the violation happened, all breach notification elements (as required in the Incidents Policy), measures BA is taking to cure the violation and prevent it from reoccurring, and verification that appropriate disciplinary actions were taken.
      iii) Terminating contract with the BA, if necessary, if the BA violated a material term of the BAA.
      iv) If DHS knows of a pattern of activity or practice of a BA (or Subcontractor) that constituted a material breach or violation of the BA's obligation under the BAA and steps taken to cure the cure the breach or end the violation were unsuccessful, terminating the BAA if feasible. If not feasible, document reasons that termination of the BAA is infeasible.
   B. When a BA is an Agent of DHS, requesting a summary of the privacy and security controls BA has in place. Also consider requesting this of BAs that are not Agents of DHS when the BA stores or assists in transmission and/or security of DHS's PHI and/or ePHI (such as hosted EHR, backup, and record storage vendors).
      i) Reviewing the summary of the privacy and security controls provided by BA.
      ii) Requesting improvements in BA's privacy and security controls, as applicable and appropriate.

8. A BAA shall remain in effect for the duration of the business contract between DHS and BA, unless otherwise terminated in accordance with the applicable provisions of the BAA.

9. Upon termination of a BAA for any reason, BA shall return or destroy all PHI/ePHI received from, or created or received by BA on behalf of, DHS. BA shall retain no copies of such PHI/ePHI.
   A. If BA destroys the PHI/ePHI, DHS may request that BA provide written notification of the timing and method of such destruction.
   B. If return or destruction is not feasible, DHS shall request written notification that BA agrees to limit uses and disclosures of such PHI/ePHI to the purposes that prevent its return or destruction, and shall extend the

protections of BAA to such PHI/ePHI, for so long as BA maintains the PHI/ePHI.

10. ***Documentation***. The Privacy Officer, in conjunction with Contracts, maintains appropriate documentation of all BAA's for a period of six years beyond the date of when the BAA relationship is terminated, and keeps copies of fully executed (signed) BAA's easily accessible by Workforce members, as appropriate.

11. ***Violations and Non-Retaliation***
    A. Violation of any security policy or procedure by Workforce members may result in corrective disciplinary action, up to and including termination of employment. Violation of any security policy and procedures by others, including system users, providers, providers' offices, business associates or partners may result in termination of the relationship and/or associated privileges. Violation may also result in civil and criminal penalties as determined by federal and state laws and regulations.
    B. All Workforce members and other users are required to report suspected violations of the security policies and procedures to the Security Officer. Individuals reporting violations in good faith shall not be subjected to intimidation, threats, coercion, discrimination against, or any other retaliatory action as a consequence.

Resources:
1. BIT Information Technology Security Policy, Contracts with Third Parties
2. HIPAA COW Business Associate Agreements Policy
3. WHITEC Business Associate Policy

Applicable Standards/Regulations:

1. 45 CFR § 164.308(b)(1-3) HIPAA Security Rule Business Associate Contracts and Other Arrangements
2. 45 CFR §164.314(a)(1) HIPAA Security Rule Business Associate Contracts or Other Arrangements
3. 45 CFR § 164.314(a)(2)(i) HIPAA Security Rule Business Associate Contracts
4. 45 CFR § 164.314(a)(2)(ii) HIPAA Security Rule Other Arrangements
5. 45 CFR § 164.502(e)(1) HIPAA Privacy Rule Disclosures to Business Associates
6. 45 CFR §164.504(e) HIPAA Privacy Rule Business Associate Contracts
7. 13401(a) HITECH Application of Security Provisions & Penalties to BAs of CEs
8. 13404 HITECH Application of Privacy Provisions & Penalties to BAs of CEs
9. 13408 HITECH BA Contracts Required for Certain Entities

Attachment 1: Examples of Business Associates and Subcontractors

EXAMPLES OF BUSINESS ARRANGEMENTS INVOLVING PHI THAT REQUIRE BUSINESS ASSOCIATE AGREEMENTS/ADDENDUMS OR CONTRACT PROVISONS	
Accrediting/Licensing Agencies (JCAHO) Accounting Consultants/Vendors Actuarial Consultants/Vendors Administrative Services Agents/Contractors Accessing PHI (Consultants) Application Service Providers (i.e., prescription mgmt.) Attorneys/Legal Counsel Auditors Benchmarking Organizations Benefit Management Organizations Billing Claims Processing or Administration / Clearinghouse Agency Contracts Coding Vendor Contracts Collection Agency Contracts Computer Hardware Contracts Computer Software Contracts Consultants/Consulting Firms Data Aggregation Data Analysis, Processing, or Administration Consultants/Vendors Data Storage Company Data Transmission Services that requires routine access to PHI Data Warehouse Contracts E-prescribing Gateway Emergency Physician Services Contracts Financial Services Health Information Organization (HIO) Hospitalist Contracts Insurance Contracts (Coverage for Risk, Malpractice, etc.) Interpreter Services Contracts IT/IS Vendors Legal Services Contracts Management Medical Staff Credentialing Software Contracts Microfilming Vendor Contracts Optical Disc Conversion Contracts	Pathology Services Contracts Paper Recycling Contracts Patient Safety Activities listed at 42 CFR 3.20 Patient Satisfaction Survey Contracts Payer-Provider Contracts (Provider for Health Plan) Personal Health Record Vendor (provided on behalf of DHS to individuals) Physician Billing Services Physician Contracts Practice Management Consultants/Vendors Professional Services Contracts Quality Assurance Consultants/Vendors Radiology Services Contracts Record Copying Service Vendor Contracts Record Storage Vendors Release of Information Service Vendor Contracts Repair Contractors of Devices Containing PHI Repricing Researcher (performs a function, activity, or service for a CE that falls within the definition of BA) Revenue Enhancement/DRG Optimization Contracts Risk Management Consulting Vendor Contracts Shared Service/Joint Venture Contracts with Other Healthcare Organizations Statement Outsource Vendors Telemedicine Program contracts Third Party Administrators Transcription Vendor Contracts Utilization Review Waste Disposal Contracts (Hauling, Shredding) <u>Health Plan Relationships:</u> Pharmaceutical Benefits Management Contracts Preauthorization Management Contracts Case Management Contracts Third Party Administrator (TPA) Contracts Wellness Promotion Contracts

Attachment 2: Examples of Arrangements that are not Business Associate Relationships

EXAMPLES OF ARRANGEMENTS THAT ARE NOT BUSINESS ASSOCIATE RELATIONSHIPS AND DO NOT REQUIRE BUSINESS ASSOCIATE /ADDENDUMS OR CONTRACT PROVISIONS	
Banks Processing Credit Card Payments Blood Bank/Red Cross (Provider) Clinics (Provider Relationships) Courier Services Delivering Specimens Device Manufacturers Require PHI to Produce Pacemakers, hearing aids, glasses, etc. (Treatment) Cleaning/Janitorial Services DME for Equipment for Treatment Purposes Educational/School Programs (Student Privacy Education Required as Workforce Member) Health Plans Contracting With Network Providers (Covered Entity to Covered Entity) Health Plans for Purposes of Payment Hospitals Housekeeping/Environmental Services (Incidental Exp.) Infusion Provider for Treatment Institutional Review Board Internet Service Providers (ISPs) providing mere data transmission services Law Enforcement Agencies Members of an Affiliated Covered Entity Members of DHS's Organized Health Care Arrangement (OHCA) Pharmacy (Healthcare Provider/Treatment) Providers (Involved in Care & Treatment of Patient)	Members of DHS's Workforce Organ Procurement Organizations Nursing Homes Quality Improvement Organization –Agent of CMS (MetaStar) Rental Employee Agencies (No PHI Shared – Employees Need Privacy Training) Repair Contractors (Maintenance, Copy Machine, Researcher Conducting Research Activities Plumbing, Electricity, etc. – No PHI involved) School Health Nurses Supply Services Support Services Agreements for Supplies/Tx Purposes Tissue Banks Telecommunications company with occasional, random access to PHI U.S. Post Office and Other Couriers Volunteers (Board Members, Ethics Committee Members, IRB Members, etc.) Note: a CE is not required to have a BAA with a BA's Subcontractor (the BA is required to have a BAA with their Subcontractor)

Facility Access Policy

Purpose

To provide guidelines to control access to and within facilities as part of DHS's efforts to safeguard the confidentiality, integrity, and availability of DHS's Electronic Protected Health Information (ePHI).

Responsible for Implementation: Security Officer is responsible for implementing and overseeing this policy and procedure, in conjunction with the Bureau of Information & Telecommunications (BIT) of the State of South Dakota.

Policy

1. This Policy shall work in accordance with the Proximity Card and Hardware Security policies of the Information Technology (IT) Security Policy developed by BIT.

2. To limit physical access to Workstations and information systems that store and/or transmit Electronic Protected Health Information (ePHI) and the facilities where they are housed to only those that need access.

3. To safeguard the facility and the ePHI equipment from unauthorized physical access, tampering, and theft.

4. To control and validate access to facilities.

Procedures

1. ***Identification of Individuals***
   A. All Workforce members who are issued identification badges (ID badges) by DHS must keep them on their person when on the premises.
      i) Security Officer and BIT are responsible for issuing ID badges and access cards to new Workforce members, who must wear a temporary ID badge issued by DHS until permanent ID badge is issued to such member.
      ii) Workforce Members are required to return their ID badge to DHS on their last day of employment or contracted work.
   B. All visitors must sign visitors log upon arrival at DHS, provide proper identification, and state the purpose of their visit.
      i) All visitors must be escorted to and from their destination after signing in at the reception desk, and must sign out when leaving.
      ii) Visitors must maintain on their person visitor ID badges issued by DHS when in Restricted Areas and must return the ID badges before leaving the premises.

2. ***Access to Restricted Areas***
   A. DHS implements procedures to control and validate a person's access to Restricted Areas based on their role or function, including but not limited to:
      i) Properly identifying persons being granted physical access to facility such as by checking government issued identification and employment records.
      ii) Issuing identification badges or cards that include the identification of the person and approved areas of access.
      iii) Monitoring and maintaining a record of all access authorizations issued.
      iv) Updating areas of authorized access when individual's role or responsibility changes.
      v) Revoking access authorization in a timely manner when such access is no longer required.
   B. The following may be permitted access to Restricted Areas, as necessary and appropriate:
      i) Workforce members requiring such access to perform legitimate job duties.
      ii) Vendors/consultants on a long-term contract wearing proper ID badge issued by DHS.
      iii) Others (vendors, auditors, patients, family, friends, etc.) with the escort of a Workforce member into and out of the Restricted Areas.

3. ***Facility Security Controls (Doors)***
   A. Access to DHS's exterior and interior room doors are locked, through the use of keyed locks and/or software based access cards.
   B. Distribution of keys and access cards
      i) Keys and access cards are distributed so that the fewest number of individuals necessary are able to access the facilities and interior locked rooms, based on DHS's needs.
      ii) The Facilities Manager and/or Security Officer distributes keys and access cards and maintains a list of individuals to whom they have been distributed.
      iii) When a Workforce member's job role changes, such member's facility access requirements are reviewed to ensure that issued keys and access cards continue to be appropriate for new role.
      iv) If applicable, key code lock combinations are changed when an individual that knows the code no longer needs the code.
      v) When lock changes are made, the reason for the change and the date the change was made are documented.
   C. Individuals issued with facility keys and access cards:
      i) May not share them with any other individual. Any exceptions must be approved and documented by the Security Officer.
      ii) May not permit access to individuals not authorized to enter the facility or interior rooms.

iii) May only use them to enter DHS's facility and interior rooms to perform legitimate job responsibilities for DHS.
iv) Are required to immediately report when they are lost, stolen, or otherwise compromised to the Security Officer, who may change the lock and/or deactivate access cards, as appropriate.
v) Are required to return them to DHS on last day of employment or contracted work.

D. Exterior doors with locks, and rooms with locks that contain ePHI and ePHI systems, may not be unlocked or propped open and then left unattended.

4. ***Servers and data wiring Safeguards***
   A. Servers that store ePHI are in locked rooms with access limited to those individuals able to maintain and/or restore access to them and any other information system equipment in the rooms. If a computer technician or other individual requests access to server room, the Facilities Manager must be notified prior to such access being granted.
   B. If applicable, data and phone wiring areas are in locked rooms and/or locked cage/rack with access limited to those individuals able to maintain and/or restore access to them and any other information system equipment in the rooms.

5. ***Additional Facility Safeguards***
   A. Workforce members have a duty to approach and/or report unknown individuals in Restricted Areas without a visible ID badge.
      i) May approach and offer assistance, with goal of escorting unauthorized individual out of Restricted Areas.
      ii) Alternatively, may report situation to appropriate personnel to assist individual or have unknown individual questioned/escorted out of Restricted Areas.
   B. Certain DHS facilities may have a security alarm system in place that is activated when the office is closed, as necessary and appropriate.
   C. Certain DHS facilities may have a security camera in place, as necessary and appropriate.

6. All Workforce members are responsible for reporting apparently unauthorized visitors and suspected unauthorized access to DHS's facilities or areas containing Information Systems that store or transmit ePHI.

7. ***Violations and Non-Retaliation***
   A. Violation of any security policy or procedure by Workforce members may result in corrective disciplinary action, up to and including termination of employment. Violation of any security policy and procedures by others, including system users, providers, providers' offices, business associates or partners may result in termination of the relationship and/or associated

privileges. Violation may also result in civil and criminal penalties as determined by federal and state laws and regulations.

B. All Workforce members and other users are required to report suspected violations of the security policies and procedures to the Security Officer. Individuals reporting violations in good faith shall not be subjected to intimidation, threats, coercion, discrimination against, or any other retaliatory action as a consequence.

Resources:

1. BIT Information Technology Security Policy, Hardware Security Policy
2. BIT Information Technology Security Policy, Proximity Cards Policy
3. HIPAA COW Facility Access Policy
4. WHITEC Facility Access Policy

Applicable Standards/Regulations:

1. 45 CFR §164.310(a) HIPAA Security Rule Facility Access Controls
2. 45 CFR §164.310(a)(2)(ii) HIPAA Security Rule Facility Security Plan
3. 45 CFR §164. 310(a)(2)(iii) HIPAA Security Rule Access Control & Validation Procedures

Facility Maintenance Policy

Purpose

To establish guidelines for maintenance, repairs, and modifications to the physical components of DHS's facilities when related to the security of Electronic Protected Health Information (ePHI).

Responsible for Implementation: Facility Services is responsible for implementing and overseeing this policy and procedure.

Policy

1. It is the policy of DHS to document repairs and changes made to buildings when they are related to the security of ePHI.

2. To improve security controls when making repairs and changes to facilities, whenever possible.

Procedures

1. Facility maintenance personnel receive training on Repairs and Changes to allow such Workforce members to take reasonable steps to inform Security Officer of repairs or modifications to DHS's physical facilities that may impact the security of ePHI (such as hardware, walls, doors, and locks).

2. Plans for Repairs and Changes are reviewed and approved by Security Officer before any repairs or modifications that may impact the security of ePHI are made. Security Officer does the following:
   A. Works to ensure that, whenever possible, planned Repairs and Changes will improve measures to safeguard ePHI.
   B. Determines if additional ePHI security controls may feasibly be added to planned Repairs and Changes to enhance the security of ePHI.
   C. Works to ensure that planned Repairs and Changes will not pose a new security risk or reduce current security controls, such as by increasing the potential for unauthorized access to ePHI.

3. Reducing security risks during Repairs and Changes
   A. If a Repair and Change increases the potential for unauthorized access to ePHI, the Security Officer identifies and implements ways to prevent unauthorized access to ePHI through duration of the project, such as by using security guards or cameras, or changing locks and redistributing keys.
   B. The Security Officer monitors the project to make sure ePHI is not compromised during the project.

C. If a Repair and Change will prevent authorized users from being able to access ePHI Workstations and/or Information Systems, the Security Officer notifies such users prior to the Repair and Change and works to put a reasonable alternative plan in place.

4. ***Documentation***.
   A. The Security Officer documents all Repairs and Changes made, including elements such as:
      i) Date and time of repair or modification.
      ii) Reason(s) for repair or modification.
      iii) Individual(s)/entity performing repair or modification.
      iv) Individual approving completed repair or modification.
      v) Cost and outcome of repair or modification.
   B. The Security Officer documents all decisions made and reasons for such decisions, as pertaining to the security of ePHI.
   C. All documentation is maintained by the Security Officer for six years from the date of creation or last date of the Repair and Change, whichever is later.

5. ***Violations and Non-Retaliation***
   A. Violation of any security policy or procedure by Workforce members may result in corrective disciplinary action, up to and including termination of employment. Violation of any security policy and procedures by others, including system users, providers, providers' offices, business associates or partners may result in termination of the relationship and/or associated privileges. Violation may also result in civil and criminal penalties as determined by federal and state laws and regulations.
   B. All Workforce members and other users are required to report suspected violations of the security policies and procedures to the Security Officer. Individuals reporting violations in good faith shall not be subjected to intimidation, threats, coercion, discrimination against, or any other retaliatory action as a consequence.

Resources:
1. HIPAA COW Facility Repairs and Maintenance Policy
2. WHITEC Facility Maintenance Policy

Applicable Standards/Regulations:

1. 45 CFR §164.310(a)(2)(iv) HIPAA Security Rule Maintenance Records

PHI and ePHI Disposal Policy

Purpose

To provide guidelines for the proper disposal of Protected Health Information (PHI) and Electronic Protected Health Information (ePHI), as well as the proper disposal and reuse of Media containing PHI or ePHI.

Responsible for Implementation: The Privacy Officer and Security Officer are responsible for implementing and overseeing this policy and procedure, in conjunction with BIT.

Policy

1. It is the policy of DHS to ensure the privacy and security of PHI and ePHI when it is no longer needed for legitimate use.

2. To take appropriate steps to remove all PHI and ePHI stored on Media prior to reuse of the Media.

3. To destroy/dispose of PHI and ePHI in accordance with Federal Regulations, applicable State laws, and DHS's data retention requirements.

4. To prevent the destruction/disposal of patient records involved in any open investigation, audit, or litigation.

Procedures

1. When no longer needed, DHS takes reasonable and appropriate steps to dispose of PHI and ePHI and/or the Media on which it is stored by using methods to completely and permanently delete and prevent unauthorized access of such PHI and ePHI.

2. All destruction/disposal of PHI and ePHI is done according to DHS's data retention requirements and schedule (and as allowed by law).

3. Participant records are not destroyed/disposed of if they are or may foreseeably be involved in any open investigation, audit or litigation.
   A. Destruction/disposal of such records is suspended until the situation is resolved.
   B. If the records have been requested in the course of a judicial or administrative hearing, a qualified protective order may be obtained to ensure that the records are returned to DHS or properly destroyed/disposed of by the requesting party.

4. Media containing PHI and ePHI scheduled for destruction/disposal are stored securely until the destruction/disposal is complete to prevent unauthorized or inappropriate access.

5. When destruction/disposal services are contracted, a Business Associate Agreement (BAA) is obtained and the following elements are included in the services contract or BAA:
   A. Specific method(s) of destruction/disposal of PHI/ePHI.
   B. Amount of time between acquisition and destruction/disposal of PHI/ePHI.
   C. Business Associate (BA) establishes safeguards against unauthorized disclosures of PHI/ePHI.
   D. BA indemnifies DHS from loss due to unauthorized disclosure.
   E. BA maintains adequate liability insurance coverage at all times that contract is in effect.
   F. BA provides proof of destruction/disposal (e.g. Certificate of Destruction).

6. When contract with BA performing destruction/disposal services terminates, follow the Business Associate Agreement Policy for the proper return or destruction of PHI and ePHI.

7. The Security Officer creates/obtains and maintains documentation of the destruction/disposal of all original (i.e. not copies of) PHI or ePHI that is destroyed/disposed of. Such documentation includes elements such as:
   A. Date of destruction/disposal.
   B. Method of destruction/disposal.
   C. Description of the records destroyed/disposed of.
   D. Inclusive dates covered.
   E. Statement that the records were destroyed/disposed of in the normal course of business.
   F. Signatures of the individuals supervising and witnessing the destruction/disposal.

8. Copies (i.e. not originals) of documents and images that contain PHI or ePHI that do not require retention based on retention policies are destroyed/disposed of by shredding or other acceptable manner as outlined in this policy. Documentation of such disposal is not required, unless done by a contracted organization. PHI must not be discarded in regular trash bins, unsecured recycling containers, or other publicly accessible/unsecure locations.

9. PHI and ePHI are destroyed/disposed of using methods that ensure the PHI/ePHI cannot be recovered or reconstructed. Methods used are as follows:

Medium	Method Used
Audiotapes	• Recycle (tape over), Degauss or pulverize.

Medium	Method Used
Electronic Data/ Hard Disk Drives including drives found in servers, workstations, printers, and copiers	• Destroy data permanently and irreversibly through a DoD wipe, physical destruction (pulverize, shred, disintegrate, incinerate), Degaussing of it, or hard drive erasure software. • Methods of reuse: overwrite data with a series of characters or reformatting the disk to destroy all data on it. (Deleting a file on a disk does not destroy the data, but merely deletes the filename from the directory, preventing easy access of the file and making the sector available on the disk so it may be overwritten.)
Electronic Data/ Removable Media or devices including USB drives, SD cards, CDs, tapes, and cartridges	• Overwrite data with a series of characters or reformat it (destroying everything on it). Total data destruction does not occur until the data has been overwritten. • Magnetic Degaussing that leaves the sectors in random patterns with no preference to orientation, rendering previous data unrecoverable. Magnetic Degaussing will leave the sectors in random patterns with no preference to orientation, rendering previous data unrecoverable. • Shredding or pulverization is done for the final disposition of any removable Media when it is no longer usable.
Handheld devices including cell phones, smart phones, PDAs, tablets and similar devices.	• Activate the Software on these devices that remotely wipes (“bit-wipe”) data from them. • When a handheld device is no longer reusable it is then totally destroyed by recycling or by trash compacting
Optical Media	• Optical disks cannot be altered or reused, making pulverization an appropriate means of destruction/disposal.
Microfilm/ Microfiche and X-rays	• Recycle through a contracted BA or pulverize.
PHI Labeled Devices, Containers, Equipment, Etc.	• Reasonable steps should be taken to destroy or de-identify any PHI information prior to disposal of this medium. Remove labels or incineration of the medium; or • Obliterate the information (make it unreadable) with a heavy permanent marker pen.

Medium	Method Used
	• Ribbons used to print labels may contain PHI and are shredded or incinerated.
Paper Records	• Paper records are destroyed/disposed of in a manner that leaves no possibility for reconstruction of the information. Appropriate methods for destroying/disposing of paper records include: burning, shredding, pulping, and pulverizing. If shredded, use cross cut shredders which produce particles that are 1 x 5 millimeters or smaller in size.
Videotapes	• Recycle (tape over) or pulverize.

10. ***Reuse of ePHI Media***
    A. Before the reuse of any recordable and erasable Media, such as hard drives, workstations, laptops, smart phones, and removable media, the Media is Sanitized to remove all ePHI by:
        i) For reuse within DHS:
            (1) Overwriting the ePHI with pseudorandom data;
            (2) Degaussing the Media; or
            (3) Reformatting the Media so files are not accessible to the new user.
        ii) For reuse outside of DHS:
            (1) Overwriting the ePHI with pseudorandom data multiple times;
            (2) Testing the Media to ensure complete data destruction before transfer for reuse; and
            (3) Removing internal access control tags from Media, if any.
    B. The Security Officer, in conjunction with BIT, documents and/or obtains documentation when this is done, as well as the method used and date/time it was completed.

11. Methods of destruction/ disposal and reuse are periodically reviewed and updated based on current technology, accepted practices, and availability of timely and cost-effective destruction/ disposal and reuse technologies and services.

12. ***Documentation***. All documentation is maintained for a period of six years after the destruction/disposal was completed.

13. ***Violations and Non-Retaliation***
    A. Violation of any security policy or procedure by Workforce members may result in corrective disciplinary action, up to and including termination of employment. Violation of any security policy and procedures by others, including system users, providers, providers' offices, business associates or partners may result in termination of the relationship and/or associated

privileges. Violation may also result in civil and criminal penalties as determined by federal and state laws and regulations.

B. All Workforce members and other users are required to report suspected violations of the security policies and procedures to the Security Officer. Individuals reporting violations in good faith shall not be subjected to intimidation, threats, coercion, discrimination against, or any other retaliatory action as a consequence.

Resources:

1. BIT Information Technology Security Policy, Assurance HIPAA Regulations are Met Policy
2. HIPAA COW Device, Media, and Paper Record Sanitization for Disposal or Reuse Policy
3. WHITEC ePHI and PHI Disposal Policy

Applicable Standards/Regulations:

1. 45 CFR § 160.103(a) HIPAA definition of Electronic Media (1/25/13)
2. 45 CFR §164.310(d)(2)(i) HIPAA Security Rule Device and Media Controls
3. 45 CFR §164.310(d)(2)(ii) HIPAA Security Rule Media Re-use
4. 45 CFR §164.504 (f)(2)(ii)(I) HIPAA Privacy Rule Requirements for Group Health Plans

Technical Access Control Policy: Transmission Security, Encryption, and Integrity

Purpose

To provide guidelines on how to prevent unauthorized access, use, disclosure, and modification of Electronic Protected Health Information (ePHI) during transmissions over electronic communication networks. To provide a method to encrypt ePHI at rest and in transit, whenever possible and deemed appropriate to help protect the confidentiality, integrity, and availability of ePHI. To provide methods to prevent and the ability to verify that ePHI is not improperly altered or destroyed.

Responsible for Implementation: The Security Officer is responsible for implementing and overseeing this policy and procedure, in conjunction with BIT.

Policy

1. This Policy shall work in accordance with the Data Encryption policy of the Information Technology (IT) Security Policy developed by BIT.

2. It is the policy of DHS to implement measures to prevent unauthorized access to Electronic Protected Health Information (ePHI) during transmission over electronic communication networks.

3. To implement mechanisms to securely encrypt and decrypt ePHI at rest and in transit, whenever feasible.

4. To have procedures and technical methods to protect ePHI from improper and/or unauthorized alteration or destruction.

5. To have electronic mechanisms and other security measures in place to ensure and validate that ePHI hasn't been altered or destroyed in an unauthorized manner until properly disposed.

Procedures

<u>Encryption and Other Mechanisms Used to Secure ePHI at Rest and In Transit</u>

1. DHS makes reasonable and appropriate efforts to encrypt ePHI at rest and in transit, to prevent unauthorized access, alteration, and destruction of ePHI.

2. The Security Officer, in conjunction with BIT, completes a risk assessment to determine the need and ability to encrypt ePHI, as well as the type of encryption

to use. Factors considered in the decision making process include but are not limited to the cost, likelihood of loss or theft, likelihood of a breach of confidentiality, potential fines, feasibility of encrypting the ePHI, and loss of reputation. BIT documents all decisions and reasons the decisions were made.

A. If it is determined that the ePHI will be encrypted:
   i) DHS seeks to select encryption products certified to be compliant with FIPS 140-2 Standard (or most current version) to meet criteria specified by Federal law both now and in the foreseeable future; be sufficient to pass audits; and reduce the likelihood of breaches.
   ii) Strong passwords are used when creating encryption passwords (see System Access Policy).
   iii) Users do not share encryption user names or passwords, or leave them where someone else may find/see them (see System Access Policy).
   iv) Encryption Keys are secured and stored so that only the minimum number of individuals with the need and authority to access ePHI servers and backups (to maintain them) may access them.

B. If it is determined that ePHI does not need to be encrypted, BIT documents why it would not be reasonable and appropriate to implement the implementation specification; and implements an equivalent alternative measure if reasonable and appropriate.

3. ***Workstations***
   A. Users may only store ePHI on a Workstation, and any other portable device when:
      i) Authorized to do so by BIT; and
      ii) Such ePHI is encrypted utilizing full disk and/or file encryption.

4. ***Servers and Backups***
   A. Servers that contain ePHI are encrypted with full disk encryption.
   B. Backups that contain ePHI are encrypted with full disk encryption.

5. ***Emailing ePHI***
   A. Standard email is inherently vulnerable to interception by unauthorized individuals and therefore not a secure method of communication.
   B. Users authorized to email ePHI to individuals authorized to receive the ePHI (according to organizational policies) are required to use DHS's specified encryption method(s) when emailing the ePHI.
      i) Do not include any PHI, such as patient identifiers, in email subject line.
      ii) Verify the email is encrypted before sending it.
      iii) Call authorized recipient(s) to provide the encryption password/key.
      iv) To email an encrypted/password protected file containing ePHI:
         (1) Do not include any PHI, such as patient identifiers, in the email subject line.
         (2) Encrypt the ePHI file with a strong password and attach it to the email.
         (3) Call authorized recipient(s) to provide the encryption password/key.

6. ***Texting ePHI***
   A. Standard texting is inherently vulnerable to interception by unauthorized individuals and therefore not a secure method of communication.
   B. As DHS does not have a means to encrypt texts, DHS's PHI may not be texted at any time from any device, whether or not the texting device is owned by DHS.

7. ***Network Transmissions of ePHI***
   A. ePHI may only be transmitted when permitted by this policy and by DHS's release of information policies.
   B. External network transmissions of ePHI must be sent using method(s) set up and monitored by the Security Officer, in conjunction with BIT, who also reviews, approves, and authorizes exceptions. Such methods include:
      i) File Transfer Protocol (FTP) with a protected communication path:
         (1) Secure Shell (SSH) to copy the data from one location to another; this method is generally referred to as Secure File Transfer Protocol (SFTP); and/or
         (2) Secured Socket Layers (SSL) to protect the connection of a standard FTP transmission.
         (3) HTTPS.
      ii) Remote access through :
         (1) The Virtual Private Network (VPN) (private point-to-point network).
         (2) Citrix, through the Citrix Access Gateway product.
         (3) Cisco.
         (4) Juniper.
   C. Only Workstations (including portable devices) authorized by the Security Officer are allowed on DHS's network.

8. ***Wireless Access Points***
   A. WPA2-Enterprise is in place for all non-public wireless access points. A strong password is utilized to access (see System Access Policy for minimum password requirements).
   B. Only Workstations authorized by the Security Officer are allowed on DHS's wireless network.

Integrity DHS utilizes various methods to protect ePHI from improper and/or unauthorized alteration or destruction and validate that this has not happened until properly disposed of according to DHS's PHI and ePHI Disposal Policy. These include, but are not limited to the following:

9. Users may only modify/amend ePHI in Information Systems and on Workstations as described in DHS's Amendment of PHI Policy.

10. Users, during the regular course of their job responsibilities, are required to report any errors or potential errors of ePHI of which they are aware in the Information Systems.

11. The Security Officer, in conjunction with BIT, ensures that Information Systems are tested for accuracy and functionality before using them in the live environment. Data is validated before integrating ePHI from one Information System into another.

12. While completing a risk analysis, DHS considers various risks to the integrity of ePHI and identifies security measures to reduce risks, as described in DHS's Risk Management Policy.

13. Audit trails on ePHI Information Systems and Workstations are in place to identify all changes made to ePHI, as described in DHS's Auditing Policy.

14. Anti-virus/malware is installed and updated, as described in DHS's Auditing Policy.

15. Physical and technical security controls are in place to prevent unauthorized access to Workstations and Information Systems, as described in DHS's System Access, Facility Access, and Facility Maintenance Policies.

16. Encryption and other mechanisms to secure ePHI, as described in this policy, are utilized to prevent transmission errors and unauthorized access to ePHI.

Documentation

17. The Security Officer, in conjunction with BIT, documents all decisions and approvals made related to this policy and its corresponding procedures, and maintains all documentation for six years from the date of creation or date it was last in effect, whichever is later.

Violations and Non-Retaliation

18. Violation of any security policy or procedure by Workforce members may result in corrective disciplinary action, up to and including termination of employment. Violation of any security policy and procedures by others, including system users, providers, providers' offices, business associates or partners may result in termination of the relationship and/or associated privileges. Violation may also result in civil and criminal penalties as determined by federal and state laws and regulations.

19. All Workforce members and other users are required to report suspected violations of the security policies and procedures to the Security Officer.

Individuals reporting violations in good faith shall not be subjected to intimidation, threats, coercion, discrimination against, or any other retaliatory action as a consequence.

Resources:

1. BIT Information Technology Security Policy, Data Encryption Policy
2. HIPAA COW Encryption Whitepaper
3. WHITEC Technical Access Control Policy
4. FIPS 140-2 Standard, 5/25/01 http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

Applicable Standards/Regulations:

1. 45 C.F.R. §164.312(e)(1) HIPAA Security Rule Transmission Security
2. 45 C.F.R. §164.312(a)(2)(iv) HIPAA Security Rule Encryption and Decryption
3. 45 C.F.R. §164.312(e)(2)(ii) HIPAA Security Rule Encryption
4. 45 C.F.R. §164.312(c)(1) HIPAA Security Rule Integrity
5. 45 C.F.R. §164.312(c)(2) HIPAA Security Rule Mechanism to Authenticate Electronic PHI
6. 45 C.F.R. §164.312(e)(2)(i) HIPAA Security Rule Integrity Controls

Group Health Plan Policy

Purpose

To document that DHS does not sponsor a self-funded health plan and therefore is not required to put in place a policy or Plan Documents to comply with the HIPAA Privacy & Security Rules.

The State of South Dakota offers a self-funded plan for State employees. The plan and its documents are managed by the South Dakota Bureau of Human Resources, a State agency separate from DHS.

Responsible for Implementation: The Privacy Officer is responsible for implementing and overseeing this policy and procedure.

1. ***Violations and Non-Retaliation***
   A. Violation of any security policy or procedure by Workforce members may result in corrective disciplinary action, up to and including termination of employment. Violation of any security policy and procedures by others, including system users, providers, providers' offices, business associates or partners may result in termination of the relationship and/or associated privileges. Violation may also result in civil and criminal penalties as determined by federal and state laws and regulations.
   B. All Workforce members and other users are required to report suspected violations of the security policies and procedures to the Security Officer. Individuals reporting violations in good faith shall not be subjected to intimidation, threats, coercion, discrimination against, or any other retaliatory action as a consequence.

Resources:
1. HIPAA COW Plan Documents Policy
2. WHITEC Group Health Plan Policy

Applicable Standards/Regulations:
1. 45 C.F.R. §164.504(f) HIPAA Privacy Rule Requirements for Group Health Plans
2. 45 C.F.R. §164.314(b) HIPAA Security Rule Requirements for Group Health Plans

HIPAA Security Policies & Procedures: Key Definitions

The following definitions apply to all of DHS HIPAA security policies and procedures:

Access: Means the ability or the means necessary to read, write, modify, or communicate data/ information or otherwise use any system resource.

Agent: Organizations are liable for the acts of their BA Agents, in accordance with the Federal common law of agency. The essential factor in determining whether an Agency relationship exists between an organization and its BA is the right or authority of DHS to control the BA's conduct in the course of performing a service on behalf of DHS (i.e. direct the performance of the service provided by the BA). Examples of when a BA is an Agent of DHS: 1) an organization provides interim instructions or directions to a BA; and 2) the terms of a BAA state that the BA must make available PHI to individuals based on the instructions to be provided by or under the direction of a CE. Examples of when a BA is generally not an Agent of an organization: 1) if the only avenue of control is for an organization to amend the terms of the agreement or sue for breach of contract, however, this generally indicates that a BA is not acting as an Agent of DHS; and 2) when DHS is legally or otherwise prevented from performing the service or activity performed by a BA (e.g. accreditation).

Audit: Internal process of reviewing information system access and activity (e.g., log-ins, file accesses, and security incidents). An audit may be done as a periodic event, as a result of a patient complaint, or suspicion of employee wrongdoing, and risk assessment results.

Audit Controls: Technical mechanisms that track and record computer/system activities.

Audit Trail: The records of sequential activities that identify a particular transaction. Used to monitor information operations to determine if a security violation occurred by providing a chronological series of logged computer events (audit logs) that relate to an operating system, an application, or user activities. Audit trails provide:

- Individual accountability for activities such as an unauthorized access of ePHI;
- Reconstruction of an unusual occurrence of events such as an intrusion into the system to alter information; and
- Problem analysis such as an investigation into a slowdown in a system's performance.

*An audit trail identifies **who** (login) did **what** (create, read, modify, delete, add, etc.) to **what** (data) and **when** (date, time).*

Availability: Means the property that data or information is accessible and useable upon demand by an authorized person.

Backup: The process of making an electronic copy of data stored in a computer system. This can either be complete, meaning all data and programs, or incremental, including just that data which changed from the previous Backup.

BIT: The Bureau of Information & Telecommunications (BIT) of the State of South Dakota.

Breach: Means the acquisition, Access, use, or Disclosure of protected health information (PHI) in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI the PHI and is presumed to be a breach unless DHS or BA, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the protected health information or to the Disclosure was made;
3. Whether the protected health information was actually acquired or viewed; and
4. The extent to which the risk to the protected health information has been mitigated.

Breach excludes:

1. Any unintentional acquisition, Access or use of PHI by a workforce member or person acting under the authority of DHS or a Business Associate (BA) 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 under the Privacy Rule.
2. Any inadvertent Disclosure by a person who is authorized to Access PHI at DHS or BA to another person authorized to Access PHI at DHS or BA, or organized health care arrangement in which DHS participates, and the information received as a result of such Disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule.
3. A Disclosure of PHI where DHS or BA 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.

Business Associate (BA): The following are general, overview criteria that define a Business Associate (BA) under HIPAA:

A. The person or business/vendor's staff members are not members of DHS's Workforce and:
   i) Creates, receives, maintains, and/or transmits protected health information (PHI)on behalf of DHS; or a Covered Entity (CE) participating in an organized health care arrangement (OHCA) that performs this function or activity for or on behalf of such OHCA;
   ii) Provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such CE, or to or for an OHCA in which the CE participates, where the provision of the service involves the disclosure PHI from such CE or arrangement, or from another BA of such CE or arrangement, to the person;
   iii) Is a Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such PHI;
   iv) Offers a personal health record to one or more individuals on behalf of a CE; and/or
   v) Are a Subcontractor that creates, receives, maintains, or transmits PHI on behalf of a BA.
B. A CE may be a BA of another CE;

C. BA does not include the following:
   i) Disclosures by a Covered Entity to a health care provider concerning the treatment of the individual;
   ii) Disclosures by a group health plan, health insurance issuer, or HMO with respect to a group health plan to the plan sponsor, to the extent that the requirements of § 164.504(f) Requirements for group health plans apply and are met; or Covered Entity participating in an organized health care arrangement (OHCA) that provides such a service to or for such OHCA by virtue of such activities or services; or
   iii) A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting PHI for such purposes, to the extent such activities are authorized by law.

Business Associate Agreement (BAA): Under the HIPAA Privacy and Security Rules, a legally binding agreement entered into by DHS and a BA (and a BA and a Subcontractor) that establishes permitted and required uses and disclosures of PHI, provides obligations for the BA to safeguard the information and to report any uses or disclosures not provided for in the agreement, and requires the authorization to terminate of the BAA if the BA violates a material term of the BAA. Refer to 45 CFR § 164.502(e)(1) to determine when the standard is not applicable.

Confidentiality: Preventing data or information from being made available or disclosed to unauthorized persons or processes.

Contingency Planning: The process of developing procedures that enable an organization to respond to emergencies so that critical business functions continue with planned levels of interruption or essential change, while continuing to protect ePHI.

Covered Entity: A health plan, health care clearinghouse, or a healthcare provider who transmits any health information in electronic form in connection with a HIPAA transaction.

Data Criticality Level:
1. **Mission Critical**: Any lack of availability of data has a significant and immediate impact on the treatment of patients. Examples include clinical systems like medical transcription, nursing, lab, radiology, or pharmacy
2. **Essential**: Required for normal day-to-day operations, but do not directly affect patient care. Examples include materials management, billing, or accounts payable
3. **Important**: Required for operations, but will not prevent patient care or long term functioning. Examples include messaging systems or management reporting systems.
4. **Low**: Useful but not essential systems, such as marketing, volunteer check-in, or web sites.

Degauss: Using a magnetic field to erase (neutralize) the data bits stored on magnetic Media.

Disaster (Information System): An event that makes the continuation of normal information system functions impossible; an event which would render the information

system unusable or inaccessible for a prolonged period of time (may be departmental or organization-wide).

Disaster Recovery Coordinator (DRC): Individual assigned the authority and responsibility for the implementation and coordination of IS contingency plan/Disaster recovery operations.

Disaster Recovery Plan: Defines the resources, actions, tasks, and data required to manage the business recovery process in the event of a business interruption. The plan is designed to assist in restoring the business process within the stated Disaster recovery goals.

Disaster Recovery Team (DRT): Individuals that assist in efforts to implement the IS contingency plan/Disaster recovery operations. Identify members and determine the scope of its Disaster Team based on organizational need and the type of emergency and/or Disaster source, specific to the recovery of each information system.

Disclosure: Disclosure means the release, transfer, provision of, Access to, or divulging in any manner of information outside the entity holding the information.

Electronic Communication Networks: Email, texting, Internet, private or point-to-point networks, internal transmission, etc.

Electronic Media: Electronic storage material on which ePHI is or may be recorded electronically, such as a computer hard drive and any other removable/transportable digital memory medium (e.g. magnetic tape and disk, optical disk, digital memory card). Electronic Media also includes transmission media used to exchange information already in electronic storage media, such as the Internet, extranet, intranet, leased lines, dial-up lines, private networks, and physical movement of removable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via Electronic Media *if* the information being exchanged did not exist in electronic form *immediately* before the transmission.

Electronic Protected Health Information (ePHI): Any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic media.

Encryption: It is the translation of data into a secret code. Unencrypted data is called plaintext; encrypted data is referred to as cipher text. "…the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key." (Wikipedia, 2009). Strong encryption provides an effective way to achieve data security. To read an encrypted file, you must have access to a secret Encryption Key or password that enables you to decrypt it.

Encryption Key: An encryption key specifies the particular transformation of plaintext into cipher text, or vice versa during decryption.

Event: An Occurrence that does not constitute a serious adverse effect on DHS or its operations, though it may be less than optimal. Examples of Events include but are not limited to:

- A hard drive malfunction that requires replacement
- Systems become unavailable due to power outage that is non-hostile in nature
- Accidental lockout of an account due to incorrectly entering a password multiple times
- Network or system instability

FIPS 140-2: The Federal Information Processing Standards publication 140-2 (FIPS 140-2) "specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information" (NIST, 2002).

Group Health Plan: An employee welfare benefit program, whether insured or self-funded, that provides medical care and payment for 50 or more participants and is administered by an entity other than the employer who established the plan. Defined by the Plan Documents.

Hardware: Any computing device able to create and store ePHI. This includes diagnostic instruments that can store ePHI but may not be physically connected to DHS's network.

HIPAA Security Regulations: The regulations published in the Federal Register by the Department of Health and Human Services on February 20, 2003 as the "Health Insurance Reform: Security Standards; Final Rule," as amended or superseded from time to time, including as modified by the Omnibus Final Rule published in the Federal Register on January 25, 2013.

Hypertext Transfer Protocol Secure (HTTPS): A transmission protocol for secure transmissions over a computer network or Internet. It is the result of layering the Hypertext Transfer Protocol (HTTP) over the SSL/TLS protocol which adds security capabilities of SSL/TLS to standard HTTP communications. It provides authentication of the web site and associated web server that one is communicating with and provides bi-directional encryption of the communications between the client and server (Wikipedia, 12/14/12).

Indication: A sign that an incident may have occurred or may be occurring at the present time. Examples of Indications include:

- A network intrusion detection sensor alerts when a known exploit occurs against an FTP server. Intrusion detection is generally reactive, looking only for footprints of known attacks. It is important to note that many IDS "hits" are also false positives and are neither an Event nor an incident.
- The antivirus software alerts when it detects that a host is infected with a worm.
- The Web server crashes.
- Users complain of slow access to hosts on the Internet.
- The system administrator sees a filename with unusual characteristics.
- The user calls the help desk to report a threatening e-mail message (and it is determined by Information Services that it is a legitimate risk issue).

Information Systems: Software, hardware, servers, backups, Internet sites, Workstations, and portable devices that contain or transmit data.

Integrity: Means the property that data or information have not been altered or destroyed in an unauthorized manner.

Law Enforcement Official: Any officer or employee of an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to investigate or conduct an official inquiry into a potential violation of law; or prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Media: Any record of PHI, regardless of medium (physical form) or characteristic that can be retrieved at any time that are generated and/or received in connection with transacting patient care or business. This includes all original patient records, documents, papers, letters, billing statements, x-rays, films, cards, and photographs. It also includes electronic media which is electronic storage material on which ePHI is or may be recorded electronically, such as a computer hard drive and any other removable/transportable digital memory medium (e.g. magnetic tape and disk, microfilm, optical disk, digital memory card, or sound and video recordings). Media includes transmission media used to exchange information already in electronic storage media, such as the Internet, extranet, intranet, leased lines, dial-up lines, and private networks.

Minimum Necessary: The minimum amount of protected health information necessary to accomplish the intended purpose of an access, acquisition, use, disclosure, or request. The "minimum necessary" standard applies to all protected health information in any form.

Occurrence: An indication that a Security Incident may have occurred, may be occurring at the present time, or may occur in the future that does not constitute a serious adverse effect on DHS or its operations. Examples include:

- **Malicious Code**: A virus, worm, Trojan horse, or other code-based malicious entity that infects a network or host and affects only one or two users
- **Inappropriate Usage:** A person violates acceptable computing use policies, such as installation of unauthorized software
- **Unplanned Downtime:** The network, system, and/or applications, including telephone systems, are not accessible due to any explainable or unexplainable circumstance causing unscheduled downtime for less than one hour (due to system failure, utility failure, power outage, etc.)
- **Network or system instability**
- The network **intrusion detection sensor alerts** when a known exploit occurs against an FTP server. Intrusion detection is generally proactive, looking only for footprints of known attacks.

Off-site: For the purpose of storage of back up Electronic Media, Off-site is defined as any location separate from the building in which the Backup was created. It must be physically separate from the creating site. The environment for Off-site storage must meet storage standards established by the manufacturer of the Backup Electronic Media.

Plan Administration Function: A function that the Plan Sponsor performs on behalf of the Group Health Plan.

Plan Documents: Documents that establish, create, or provide evidence of existence of an ERISA plan. These documents commonly include the plan description and summary plan description (SPD). The SPD is distributed to enrollees and describes benefits, limitations, exclusions, rights and responsibilities of the participants. The "Plan Document" might also consist of several documents that govern the Group Health Plan. Therefore, the Group Health Plan may want to seek legal counsel to determine which documents should be amended.

Plan Sponsor: An employer, organization, or joint relationship between two or more employers that establish or maintain an employee benefit plan.

Precursor: A sign that a security incident may occur in the future. Examples include:

- Suspicious network and host-based IDS Events/attacks.
- Alerts as a result of detecting malicious code at the network and host levels.
- Alerts from file integrity checking software.
- Alerts from third party monitoring services.
- Audit log alerts.

Protected Health Information (PHI): Individually identifiable health information:

- That is created by or received by DHS, including demographic information, that identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:
  - Past, present or future physical or mental health or condition of an individual
  - The provision of health care to an individual
  - The past, present, or future payment for the provision of health care to an individual
- Excluding:
  - Regarding a person who has been deceased for more than 50 years;
  - Employment records held by a covered entity in its role as employer; and
  - Education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g and student records described at 20 U.S.C. 1232g(a)(4)(B)(iv)

Repairs and Changes: For purposes of this policy, any renovating, repairing, remodeling, or purchasing or leasing a new facility, which may in any way may impact the security of ePHI. Examples of changes include, but are not limited to the following:

- Changes to external and internal doors, locks, and controlled access systems
- Remodeling of reception desk areas, nurses' station, etc.
- Moving or changing entryways, walls, and windows
- New security devices (e.g. alarm systems, cameras, etc.)

Restricted Area: Those areas of the building(s) where PHI/ePHI is stored, transmitted, or utilized at any time. These areas include, but are not limited to the following examples:

1. HIM/medical record departments
2. Reception check-in desks/stations
3. Nursing/patient care stations/desks

4. Patient care hallways
5. Patient care rooms or other designated area
6. Employee meeting rooms/kitchens located in patient care areas
7. Mailrooms
8. Offices
9. Cubicles
10. Storage closets and cabinets (including medication storage areas)
11. Information system equipment rooms (server, data wiring, phone wiring, etc.)
12. Business office windows and offices
13. Human resources window and offices
14. Administration offices

Risk: The likelihood that a Threat will exploit a Vulnerability, and the impact of that event on the confidentiality, availability, and integrity of ePHI, organizationally sensitive information, and other information system assets.

Risk Assessment: (Referred to as *Risk Analysis* in the HIPAA Security Rule); the process:

- Identifies the risks to information system security and determines the probability of occurrence and the resulting impact for each Threat/Vulnerability pair identified given the security controls in place
- Prioritizes risks
- Results in recommends possible actions/controls that could reduce or offset the determined risk.

Risk Management: Within this policy, it refers to two major process components: risk assessment and risk mitigation. This differs from the HIPAA Security Rule, which defines it as a risk mitigation process only. The definition used in this policy is consistent with the one used in documents published by the National Institute of Standards and Technology (NIST).

Risk Management Team: Individuals who are knowledgeable about DHS's HIPAA Privacy, Security and HITECH policies, procedures, training program, computer system set up and technical security controls, and who are responsible for the risk management process and procedures in this policy. May be comprised of the Information Security Officer, Physical Plant Security Officer, Systems Analyst(s), Privacy Officer, Risk Manager, Compliance Officer, Chief Information Officer, and Security/Technology subject matter experts.

Risk Mitigation: Referred to as *Risk Management* in the HIPAA Security Rule, and is a process that prioritizes, evaluates, and implements security controls that will reduce or offset the risks determined in the risk assessment process to satisfactory levels within an organization given its mission and available resources.

Role: The category or class of person or persons doing a type of job, defined by a set of similar or identical responsibilities.

Sanitize: Removal or the act of overwriting data to a point of preventing the recovery of the data on the device or Media that is being sanitized. Sanitization is typically done before re-issuing a device or Media, donating equipment that contained sensitive information or returning leased equipment to the lending company.

Security Incident: A violation or imminent threat of violation of information security policies, acceptable use policies, or standard security practices; an adverse event whereby some aspect of computer security could be threatened; an IS Disaster would be considered a Security Incident.

Subcontractor: a person to whom a BA delegates a function, activity, or service, other than in the capacity of a member of the Workforce of such BA.

Threat: the potential for a particular Threat Source to successfully exercise a particular Vulnerability. Threats are commonly categorized as:

- Environmental: external fires, HVAC failure/temperature inadequacy, water pipe burst, power failure/fluctuation, etc.
- Human: hackers, data entry, workforce/ex-workforce members, impersonation, insertion of malicious code, theft, viruses, SPAM, vandalism, etc.
- Natural: fires, floods, electrical storms, tornados, etc.
- Technological: server failure, software failure, ancillary equipment failure, etc. and environmental Threats, such as power outages, hazardous material spills.
- Other: explosions, medical emergencies, misuse or resources, etc.

Threat Action: The method by which an attack might be carried out (e.g., hacking, system intrusion, etc.).

Threat Source: Any circumstance or event with the potential to cause harm (intentional or unintentional) to an IT system. The common Threat sources can be natural, human or environmental which can impact DHS's ability to protect ePHI.

Unsecured Protected Health Information (Unsecured PHI): Protected health information (PHI) that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Pub. L.111-5 on the HHS website.

1. Electronic PHI has been encrypted as specified in the HIPAA Security rule by the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key and such confidential process or key has not been Breached. To avoid a Breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt. The following encryption processes meet this standard.
    A. Valid encryption processes for data at rest (i.e. data that resides in databases, file systems and other structured storage systems) are consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.
    B. Valid encryption processes for data in motion (i.e. data that is moving through a network, including wireless transmission) are those that comply, as appropriate, with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, and may include others which are Federal Information Processing Standards FIPS 140-2 validated.
2. The media on which the PHI is stored or recorded has been destroyed in the

following ways:

A. Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.
B. Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publications 800-88, Guidelines for Media Sanitization, such that the PHI cannot be retrieved.

Vendors: Persons from other organizations marketing or selling products or services, or providing services to DHS. Examples include, but are not limited to the following:

1. Pharmaceutical representatives
2. Equipment repair service personnel
3. Food services
4. Independent Contractors

Virtual Private Network (VPN): The VPN creates a temporary encrypted connection into the host network that exists only for as long as needed. A *Standard VPN* requires a client utility to be installed on the remote Workstation, and creates an encrypted connection, or tunnel, into the company's network; this method uses keys/passwords to authenticate the remote computer, and the IPSEC protocol to create and secure (encrypt) the tunnel; connections are only allowed for computers with the appropriate client utility. An *SSL VPN* is set up as a secure website (similar to how banks provide online banking services); because there is no client to install, this has the advantage of being available to anyone, from anywhere, and not just from a specific computer. A *Lan-to-Lan (or L2L) VPN* creates a permanent encrypted tunnel between two networks (examples include Cisco and Juniper).

Vulnerability: A weakness or flaw in an information system that can be accidentally triggered or intentionally exploited by a Threat and lead to a compromise in the integrity of that system, i.e., resulting in a security breach or violation of policy.

Workforce: Employees, volunteers, trainees, students, contractors, and other persons whose conduct, in the performance of work for DHS or BA, is under the direct control DHS or BA, whether or not they are paid by DHS or BA.

Workstation: An electronic computing device, such as a laptop or desktop computer, notebook, iPad, or any other device that performs similar functions, used to create, receive, maintain, or transmit ePHI. Workstation devices may include, but are not limited to: laptop or desktop computers, personal digital assistants (PDAs), smart phones, USB/flash drives, tablet PCs, and other handheld devices. For the purposes of this policy, “Workstation” also includes the combination of hardware (i.e. Ethernet ports, hard drive, etc.), operating system, application software, and network connection (including remote and wireless).