Arizona State University
HIPAA Security Rule
Audit Report
August 7, 2017

This page left blank intentionally.

Arizona State University
HIPAA Security Rule Audit
August 7, 2017

Summary: The HIPAA Compliance audit was included in the Arizona State University (ASU) FY2017 audit plan approved by the Arizona Board of Regents (ABOR) Audit Committee and ASU senior leadership. The audit focused on compliance to the defined requirements of the HIPAA Security Rule. This audit is in support of ASU's mission of preserving the availability, confidentiality, and integrity of its information resources.

Background: The Health Insurance Portability and Accountability Act (HIPAA) is legislation that provides data privacy and security provisions for safeguarding medical information. The Act includes a Privacy Rule and a Security Rule. The Privacy Rule established standards to protect individuals' medical records and other personal health information (PHI). The Security Rule provides additional standards related to PHI that is held or transferred in electronic form (ePHI). The Security Rule covers the following four general areas:

- Ensure the confidentiality, integrity, and availability of ePHI created, received, maintained or transmitted
- Identify and protect against reasonably anticipated threats to the security or integrity of information
- Protect against reasonably anticipated impermissible uses or disclosures, and
- Ensure compliance by the workforce.

HIPAA applies to health plans, health care providers and health care clearinghouses, which are referred to as Covered Entities. For ASU, HIPAA applies to departments that have been identified as a Covered Entity, departments that handle PHI and ASU employees who provide management, administrative, financial, legal or operational support to a Covered Entity.

Compliance with HIPAA is mandatory. The U.S. Department of Health and Human Services Office for Civil Rights (OCR) is responsible for enforcing HIPAA's Privacy and Security Rules. OCR enforces the rules by investigating complaints and conducting compliance reviews to determine if covered entities are in compliance. HIPAA violations can be quite costly to an institution. There are HIPAA Breach Notification rules that require specific notification to the patient following a data breach. In addition to the notification costs, institutions can incur fines as well as face criminal penalties stemming from violations of the HIPAA Privacy and Security rules. Fees can range from $100 to $50,000 per violation.

Audit Objective: The objective of this engagement was to assess compliance with the HIPAA Security Rule. Specifically, areas assessed included the following:

- 164.306 – Security Standard General Rules
- 164.308 – Administrative Safeguards
- 164.310 – Physical Safeguards
- 164.312 – Technical Safeguards

Scope: The scope of the audit was limited to the segmented HIPAA environment located at the IO datacenter (a third-party datacenter utilized by ASU). The HIPAA environment is comprised of applications and data from multiple areas across the University that have been identified as being required to comply with HIPAA.

The physical security and overall infrastructure is managed by the University Technology Office (UTO) while management of the specific applications is the responsibility of the specific University functions and data stewards. The scope of this audit was limited to the UTO-managed functions and does not provide coverage of the specific applications residing in the environment.

In addition, this audit did not cover the overall Risk Assessment provisions of the HIPAA Security Rule due to the focus being limited to the defined HIPAA environment.

Methodology: Our audit consisted of tests of procedures and policies necessary to provide a reasonable basis for expressing our opinion. Specifically, audit work consisted of interviews with ASU staff, observation of work processes, review of documented policies and substantive tests including the following areas:

- Verifying a policy exists addressing responsibility for the protection, security and integrity of university data including relevant sanctions for noncompliance.
- Verifying ASU has a designated HIPAA Privacy Officer and HIPAA Security Officer.
- Assessing logical access to the HIPAA environment through the following:
    - Confirming access is restricted to appropriate individuals.
    - Verifying logical access to the HIPAA environment is approved by the data steward or their delegate by tracing a sample of 15 new hires to the documented request and validating required approvals were obtained.
    - Verifying access to the HIPAA environment is removed timely by validating access is removed within 2 days for a sample of 15 terminated employees.
- Assessing physical access to the IO data center through the following:
    - Confirming access is restricted to appropriate individuals.
    - Verifying the required fingerprinting/background check was performed for a sample of 12 individuals.
    - Verifying physical access was approved by ASU datacenter operations by

  - tracing a sample of 12 individuals to the documented request and validating appropriate approvals were obtained.
  - Reviewing the annual review of IO datacenter access to ensure it was completed and necessary actions performed.
  - Reviewing the IO Datacenter SOC 2 security report.
- Assessing that appropriate Security Awareness is in place through the following:
  - Validating new employees complete the mandatory Information Security/HIPAA Training within 30 days of hire by validating completion dates for a sample of 65 new hires.
  - Validating individuals with access to the HIPAA environment complete the mandatory HIPAA and Information Security training on an annual basis by validating that all users have completed testing within the last year.
- Assessing monitoring and security incident processes of the HIPAA environment through the following:
  - Verifying the environment is part of the defined monitoring procedures performed by the Security Operational Control team through reviewing SPLUNK activity logs.
  - Verifying the environment is part of the defined vulnerability scanning and remediation processes.
  - Verifying session logging functionality for Citrix.
  - Confirming an Incident Management Program exists by reviewing the program documentation and confirming with management that the program applies to the HIPAA environment.
- Verifying the HIPAA environment has antivirus protection through reviewing SCCM status reports.
- Verifying password configuration for the HIPAA environment meets the defined password policy through reviewing configuration screenshots for the environment.
- Verifying automated backups of HIPAA data are occurring by reviewing automated schedule configuration and related backup logs to ensure retention period is appropriate.
- Confirming a disaster recovery exercise occurred within the past 12 months and provided appropriate coverage of key disaster recovery components.
- Verifying the HIPAA environment is encrypted by reviewing the Citrix Admin configuration settings.
- Verifying the HIPAA environment has appropriate automated logoff settings by reviewing the Citrix Admin configuration settings.

Conclusion: Overall, ASU has developed a robust HIPAA awareness program that addresses the key components included in the HIPAA Security Rule; however, improvement is needed to ensure compliance with defined guidance. Specifically, controls were found operating effectively in the HIPAA environment related to physical security, antivirus, security monitoring, backups, disaster recovery and encryption. In addition, ASU has a formal policy addressing responsibility for the protection, security, and integrity of university data including relevant sanctions for noncompliance. There are also designated individuals responsible for HIPAA Privacy and Security. Defined policies and standards exist in the areas of logical access, security awareness, vulnerability management, password configuration and automated logoff; however, testing indicated that the HIPAA environment is not in compliance with these standards.

Logical access to the HIPAA environment is not appropriately restricted. While processes governing granting logical access are effective to ensure only authorized individuals are granted access, controls do not ensure that required security awareness training is completed before access is granted. Additionally, there are no periodic access reviews performed of the environment. As a result, we identified 19 individuals with inappropriate access. Testing also indicated that access is not removed in a timely manner for terminated employees.

Security awareness is a key aspect of the HIPAA Security Rule. All new employees are required to complete Information Security training within 30 days of new hire and annually thereafter. Employees who have access to HIPAA data are also required to take HIPAA training at the time access is granted and annually thereafter. While the Security Awareness program is appropriate, there is an overall lack of compliance with the required training. Testing indicated that 51% of the new hires tested did not complete the Information Security Training within 30 days of new hire. In addition, 45% of the individuals with access to the HIPAA environment have not taken the Information Security Awareness or HIPAA training (or both) over the past 12 months.

The HIPAA Security Rule also requires various safeguards to be in place to protect the overall security of the environment. UTO has effectively implemented encryption, antivirus protection and data backups for the HIPAA environment to ensure the integrity and availability of data; however, improvement is needed to ensure data is protected against reasonably anticipated threats to security. Specifically, there is currently no session logging capability with the existing version of Citrix used to access the environment. Management is in the process of updating the version of Citrix to a version that supports logging; however, this was not in place at the time of the audit. In addition, although semi-annual vulnerability scans are performed over the HIPAA environment, processes to review, analyze and remediate identified vulnerabilities require improvement. Testing also indicated that the local password configuration and the configuration for automatic logoff do not meet defined Information Security Policies or guidance.

The control standards we considered during this audit and the status of the related control environment are provided in the following table.

General Control Standard (The bulleted items are internal control objectives that apply to the general control standards, and will differ for each audit.)	**Control Environment**	**Finding No.**	**Page No.**
Reliability and Integrity of Financial and Operational Information	N/A	N/A	N/A
Effectiveness and Efficiency of Operations			
• Automated backups of the HIPAA environment are performed and retained.	Reasonable to Strong Controls in Place.	N/A	N/A
• Disaster Recovery exercises are performed annually to ensure effective recovery strategy and capabilities.	Reasonable to Strong Controls in Place.	N/A	N/A
Safeguarding of Assets			
• Logical access to the HIPAA environment is appropriately restricted.	Significant Opportunity for Improvement.	1	8
• Logical access is removed within two days of termination date.	Opportunity for Improvement.	4	11
• Password requirements and complexity configuration meet the defined Information Security Policy.	Opportunity for Improvement.	6	13
• Physical access to the data center is appropriately restricted.	Reasonable to Strong Controls in Place.	N/A	N/A
• Automated logoff settings are implemented to terminate sessions after a reasonable time of inactivity.	Opportunity for Improvement.	5	12
• Antivirus protection is implemented to protect against malware.	Reasonable to Strong Controls in Place.	N/A	N/A
• Encryption is implemented to meet the defined data encryption requirement.	Reasonable to Strong Controls in Place.	N/A	N/A
• Vulnerability management is implemented including review, analysis and remediation.	Opportunity for Improvement.	3	10
• Security event monitoring is implemented to monitor the HIPAA environment.	Reasonable to Strong Controls in Place.	N/A	N/A
• Detailed session logging is implemented to ensure audit logs are available for review.	Opportunity for Improvement.	7	14
Compliance with Laws and Regulations		N/A	N/A

• Information Security Policy exists addressing responsibility for the protection, security and integrity of university data.	Reasonable to Strong Controls in Place.	N/A	N/A
• There is a designated HIPAA Privacy Officer and HIPAA Security Officer.	Reasonable to Strong Controls in Place.	N/A	N/A
• Information Security and HIPAA awareness programs ensure employees are adequately trained.	Significant Opportunity for Improvement.	2	9

We appreciate the assistance of University Technology Office staff during the audit.

David Jones

David Jones, CEH
IT Auditor

Lisa Grace

Lisa Grace, CPA, CIA, CISA, CISSP
Executive Director

Audit Results, Recommendations, and Responses

1. Logical access to the HIPAA environment is not appropriately restricted.

Condition: Access to the HIPAA environment is not appropriately restricted. Specifically, 19 (4%) of the 425 user accounts were related to terminated employees or employees that had transferred roles and no longer needed access.

Criteria: HIPAA Security Rule 164.308 requires that procedures be in place to ensure access to ePHI is appropriate.

Cause: Although UTO is responsible for granting/removing access to the HIPAA environment, they are dependent on the various departments to notify them when to remove access. Consistent notification processes are not in place, and as a result UTO is not consistently notified when employees are terminated or change positions, nor is this being detected through periodic access reviews.

Effect: Access to the HIPAA environment is not appropriately restricted which may result in inappropriate or unauthorized access or changes to HIPAA data. In two instances, it was noted that a user id was accessed after termination date.

Recommendation: A comprehensive access review of the HIPAA environment should be performed. The exceptions noted in this issue were the result of high-level audit procedures and do not constitute a full access review. In addition, ongoing periodic access reviews should be implemented.

Follow up should also be performed with the appropriate departments to ensure that appropriate visibility exists for terminated and transferred employees.

Management Response: UTO concurs with this recommendation and has taken the following steps to confirm that all access is appropriate:

1. A comprehensive review was completed and all current users have been validated.

2. Each Covered Entity's HIPAA Security Officer, or designee, will be provided with ability to provision and de-provision their covered entities personnel access to the HIPAA environment via the WINEDS system. This will provide better visibility and accountability for ongoing access review. Target completion date: October 1, 2017.

3. Beginning this fiscal year HIPAA Privacy and Security Officers will require

Security Officers, representing each covered entity, to provide reporting bi-annually, validating WINEDS access for individuals in each Covered Entity.

2. Information Security and HIPAA awareness training is not enforced resulting in low compliance.

Condition: All ASU employees are required to take the Information Security training within 30 days of hire and then annually thereafter. In addition, employees with access to HIPAA data are required to take the HIPAA training before they are granted access and then annually thereafter. Although training is required, it is not enforced resulting in low compliance.

Criteria: HIPAA Security Rule 164.308 (5) requires that a security awareness and training program be implemented. ASU Information Security has developed a program which requires initial and annual training.

Cause: Currently, there are no enforcement controls in place to ensure individuals complete the required training. Some monitoring controls are in place; however, without enforcement controls, the monitoring is ineffective.

Effect: Overall, there is a low compliance rate for the required training. Testing indicated the following:

- 51% (33 of 65) of new hires tested that have access to the HIPAA environment did not complete Information Security training within 30 days of hire; 18% (12 of 65) have never completed Information Security training.
- 26% (17 of 65) of new hires tested that have access to the HIPAA environment have not completed HIPAA training. HIPAA training is required before access is granted.
- 35% (149 of 425) of employees tested with access to the HIPAA environment have not completed the required annual Information Security training.
- 23% (98 of 425) of employees tested with access to the HIPAA environment have not completed the required annual HIPAA training.

Recommendation: Existing dashboards should be enhanced to provide better transparency into overall compliance rates/trends. In addition, further controls are required to ensure compliance with required training. It is recommended that Information Security collaborate with the data stewards of the areas that have access to the HIPAA environment to develop escalation procedures for non-compliance. Procedures that should be considered include enhanced reminders, reporting to management/data stewards as well as suspending access to the HIPAA environment until required training is complete.

Management Response: UTO concurs with this recommendation and has taken the following steps to confirm that all access is appropriate:

1. Dashboards will be expanded to provide visibility to HIPAA training compliance for all Covered Entities and processes will be enhanced to manage escalation as appropriate to ensure compliance. Target completion date: October 1, 2017.

2. Collaboration will occur with each covered entities HIPAA Security Officer to implement procedures to maintain compliance, such that, new users will not be added to the system until training is completed and existing users will be suspended from access to the HIPAA environment if training is not completed.

3. Vulnerability management processes for the HIPAA environment require improvement.

Condition: Management conducts semi-annual vulnerability scans of the HIPAA environment as part of the overall data center scans. Results are reviewed with RiskSense, the third party utilized for scanning. Critical vulnerabilities are assessed and are remediated as necessary; however, management currently does not utilize the RiskSense tool to track the status of remediation efforts and approved exceptions.

Criteria: HIPAA Security Rule 164.308 (6) requires that processes be put into place to identify and respond to security incidents.

Vulnerability management is the process of identifying, assessing, prioritizing and remediating IT security vulnerabilities to ensure the environment is protected from external and internal security treats.

Cause: Data center management has not fully implemented the RiskSense tool to facilitate the vulnerability management program. As a result of the tool not being utilized as designed, current scans are not an accurate representation of the environment as reporting is based on previously identified vulnerabilities that have not been actioned as well as new vulnerabilities. In addition, there is no tracking of completed remediation or risk acceptance where remediation is not performed.

Effect: Without effective vulnerability management processes in place, UTO and the departments utilizing the HIPAA environment do not have adequate visibility to the security risks in the environment, increasing the overall risk of a potential breach of ePHI.

Recommendation: Fully implement the RiskSense tool which includes capturing the analysis of results, remediation actions performed and risk acceptance of vulnerabilities not remediated. As part of the implementation efforts, existing reporting should be enhanced to provide effective reports for end users to utilize in their analysis.

Formal tracking and reporting should also be implemented to provide better transparency to management of the scan results as well as the status of necessary analysis and remediation efforts.

Management Response: UTO concurs with this recommendation and will take the following steps to improve the vulnerability management process:

1. UTO will fully implement RiskSense across all HIPAA systems. Target completion date: October 1, 2017.

2. Additional RiskSense training will be completed for staff that support the HIPAA environment. Target completion date: October 1, 2017.

3. In conjunction with training, UTO will work with RiskSense to further segment HIPAA systems to simplify report review, remediation activity, and tracking. Target completion date: October 1, 2017

4. Logical access to the HIPAA environment is not removed timely for terminated employees.

Condition: Access to the HIPAA environment is not removed timely for terminated employees. Specifically, for 47% of users tested (7 of 15), access was not removed until three or more days after the termination date.

Criteria: HIPAA Security Rule 164.308 requires that procedures be in place to ensure access to ePHI is removed timely when an employee is terminated or transferred.

Cause: Exiting processes do not ensure that UTO is notified in a timely manner when an employee terminates or transfers to a new position

Effect: Access to the HIPAA environment is not appropriately restricted which may result in inappropriate or unauthorized access or changes to HIPAA data. In two instances, it was noted that the user id was accessed after terminated date.

Recommendation: Formalize policy with data stewards to ensure timely notification of terminations or transfers.

Management Response: UTO concurs with this recommendation and will implement the following process to ensure that all access is removed timely when each employee is terminated.

1. Each Covered Entity's HIPAA Security Officer, or designee, will be provided with ability to provision and de-provision their covered entities personnel access to the WINEDS system. This will provide better visibility and accountability for ongoing access review. Target completion date: October 1, 2017.

2. Document procedure identifying responsibilities of each covered entities security officers role for administering access according to employment and training compliances. Target completion date: October 1, 2017.

5. Configuration of the auto-lockout for the HIPAA environment does not meet the recommended setting defined in the HIPAA guidance.

Condition: The Citrix session logoff is configured for 6 hours which does not meet the defined Information Security HIPAA guidance.

Criteria: HIPAA Security Rule 164.312 (a) requires that procedures be implemented that terminated electronic sessions after a predetermined time of activity. ASU's HIPAA guidance defines the lockout setting to be set at a maximum of 10 minutes.

Cause: The existing configuration was set to meet business needs of those groups utilizing the HIPAA environment; however, these business needs have not been visited in many years nor was there a formalized risk acceptance process followed to ensure appropriate transparency into the increased risk.

Effect: The existing configuration does not meet the defined guidance of 10 minutes, increasing the overall risk of unauthorized access to the HIPAA environment. This issue is somewhat mitigated by the various end-point configuration settings; however, in all cases but one the configuration of the end points also did not meet the required 10 minute requirement.

Recommendation: The HIPAA Privacy Officer should review the various business needs and determine if the existing HIPAA guidance is appropriate to ensure adequate protection of the HIPAA environment while meeting business needs and update accordingly. In addition, a formal exception process should be implemented for needed exceptions to ensure management has appropriate visibility to the increased risk.

Management Response: UTO concurs with this recommendation and has taken the following steps to ensure session logoff.

1. A review was completed and the default session logoff will be set to 15 minutes. Target completion date: August 31, 2017.

2. Moving forward all exception requests for the default session logoff will be reviewed by the HIPAA Privacy and Security Officers for appropriate action.

6. Password configuration for the HIPAA environment does not comply with the defined Information Security Password Standard.

Condition: The existing group policy configuration for local privileged accounts does not meet the defined Password Standard. Current group policy configuration for privileged accounts is seven characters and does not meet the complexity requirements.

Criteria: HIPAA Security Rule 164.308 (5) requires that defined processes be put into place for governing password requirements. ASU's password standard requires the following items:

- 10 character minimum
- 180 day reset and
- The use of 3 of the 4 following attributes (Upper, Lower, Digits and Special)

Cause: Configuration was not set to meet minimum requirements.

Effect: Passwords can be set for local privileged accounts that do not meet the defined password standard resulting in increased risk of compromised credentials.

Recommendation: Update the existing configuration to meet the defined standard.

Management Response: UTO concurs with this recommendation and will update the group policy configuration to be compliant with the Information Security password standard. This requires a software upgrade. Target completion date: January 31, 2018.

7. Session logging is not in place for Citrix.

Condition: Detail session logging is not possible in the current version of Citrix.

Criteria: HIPAA Security Rule 164.308 (1) requires that defined processes be put into place to regularly review records such as audit logs to detect potential security violations. ASU's HIPAA guidance recommends centralized logging and monitoring.

Cause: The version of Citrix that ASU is utilizing does not have reliable session logging.

Effect: Audit logs are not created to capture Citrix activity which may impact ASU's ability to effectively triage a data breach.

Recommendation: Update the existing version of Citrix to a version that supports session logging.

Management Response: UTO concurs with this recommendation and will update the environment to fulfill the recommendation to support detail session logging. This requires a software upgrade. Target completion date: January 31, 2018.

Distribution:

Arizona Board of Regents Audit Committee
Michael M. Crow, President
Morgan R. Olsen, Executive Vice President, Treasurer and Chief Financial Officer
Mark S. Searle, Executive Vice President, University Provost
James Rund, Senior Vice President, Educational Outreach & Student Services
Gordon Wishon, Chief Information Officer
Aaron Krasnow, Associate Vice President/Director Counseling and Health Services, ASU HIPAA Privacy Officer
Tina Thorstenson, Associate Vice President, Chief Information Security Officer, ASU HIPAA Security Officer
Jay Steed, Assistant Vice President Operations
Jack Hsu, Senior Director Operations Systems and Security
Shawn Bryan, Senior Director Operations
Dave McKee, Senior Director Operations Netcom
Internal Audit Review Board