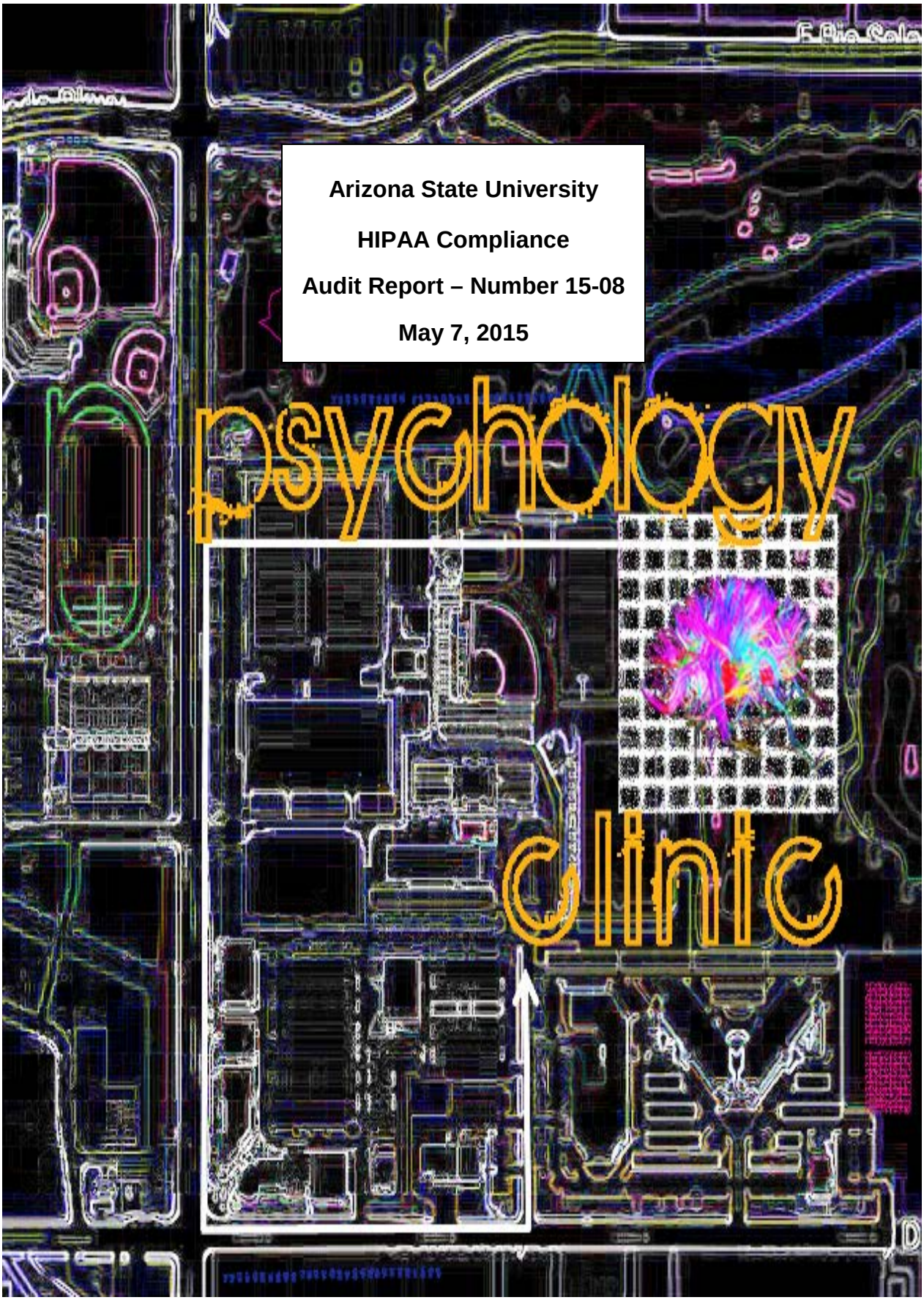
Arizona State University
HIPAA Compliance
Audit Report – Number 15-08
May 7, 2015
psychology
clinic

This page left blank intentionally.

Arizona State University
HIPAA Compliance
Audit Report – Number 15-08
May 7, 2015

Summary

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) audit was included on the Arizona State University (ASU) FY 2015 annual audit plan approved by the Arizona Board of Regents (ABOR) Audit Committee and university senior leadership. This audit was conducted to evaluate the efficiency of the HIPAA process and university adherence to current policies and practices. The audit was requested to review university compliance with new initiatives created by the U.S. Department of Health and Human Services (HHS) and Office for Civil Rights (OCR) to more closely monitor and identify violations.

Background: Arizona State University (ASU) provides health care and performs research activities that are subject to the Federal Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA's purpose is to ensure the confidentiality, integrity and availability of individuals' protected health information.

The OCR enforces three rules related to HIPAA:

1. HIPAA Privacy Rule, which protects the privacy of individually identifiable health information.
2. HIPAA Security Rule, which sets national standards for the security of electronic protected health information (ePHI).
3. HIPAA Breach Notification Rule, which requires covered entities and business associates to provide notification following a breach of unsecured protected health information.

The Standards for Privacy of Individually Identifiable Health Information (Privacy Rule) establishes, for the first time, a set of national standards for the protection of certain health information. The HHS issued the Privacy Rule to implement the requirement of HIPAA. The Privacy Rule standards address the use and disclosure of individuals' health information called Protected Health Information (PHI) by organizations subject to the Privacy Rule called covered entities, as well as standards for individuals' privacy rights to understand and control how their health information is used.

The definition of PHI under HIPAA is broad and includes information maintained by or for the covered entity relating to a person's health, the care received and payment for services. Within the university, the covered entity is comprised of its health care components, clinic components, physicians' offices, self-insured health plans, and student health services. PHI does not include health information in employment records maintained by the university in its role as employer.

Currently there are six designated covered components at ASU:

1. ASU Health Services
2. ASU Counseling Services
3. Speech and Hearing
4. College of Nursing and Healthcare Innovations Health Clinics (CONHI)
5. Center for Health Information and Research (CHiR)
6. University Technology Office

Effective February 18, 2010, in accordance with the Health Information for Economic and Clinical Health Act of 2009 (HITECH), a Business Associate Agreement (BAA) disclosure, handling and use of PHI must comply with HIPAA Security Rule and HIPAA Privacy Rule mandates. Under the HITECH Act, any HIPAA business associate that serves a health care provider or institution is now subject to audits by the OCR within the HHS and can be held accountable for a data breach and penalized for noncompliance.

Non-compliance with HIPAA regulations can lead to both civil and criminal penalties. Violations of HIPAA could result in the following penalties:

	For violations occurring prior to 2/18/2009	For violations occurring on or after 2/18/2009
Penalty Amount	Up to $100 per violation	$100 to $50,000 or more per violation
Calendar Year Cap	$25,000	$1,500,000

The HIPAA Regulations require the university, as a covered entity, to have a BAA whenever a non-university person or entity provides services to the university involving the use or disclosure of the university's protected information. HIPAA requires that agreements with business associates include specific provisions. The university has standard HIPAA BAA's that should be used whenever a business associate agreement is required.

Audit Objectives: The objectives of the audit engagement were to review all six covered entities at ASU subject to HIPAA regulations and assess the level of compliance with applicable policies and procedures and state and federal regulations as it relates to PHI. In addition, perform a review of the controls in place surrounding the HIPAA process to identify gaps and mitigate risks associated with the PHI.

Scope: The scope of this audit encompassed assessing the purpose and relevancy of PHI-related data uses, controls and exposures for ASU. University Audit (Audit) gained an understanding of the process and controls over the designated covered entities through reviewing supporting documentation and holding interviews with applicable staff.

Methodology: Audit performed a review of the current controls surrounding HIPAA regulations as it relates to ASU covered entities. Audit interviewed HIPAA Privacy and Security Officers from the following covered entities: ASU Health Services, ASU Counseling Services, Speech and Hearing, CONHI, and CHiR.

During interviews conducted with Privacy and Security Officers, the following topics were discussed:

- Policies and procedures followed related to the storage and retention of PHI and ePHI.
- Training provided to staff that contact or interact with PHI and ePHI.
- Required forms to be completed by personnel and staff handling PHI and ePHI.
- Measures taken to ensure the security of ePHI on the system network.
- Requirements needed to be met to gain access to PHI and ePHI information.
- Background check requirements before access to PHI and ePHI are granted.
- Personnel and staff's level of satisfaction of the current systems in place related to PHI and ePHI.
- The level of interaction with other covered entities (Privacy and Security Officers in other covered entities).

Walkthroughs were performed to observe the physical security of PHI files and gain an understanding of who has access to PHI files.

Conclusion: Audit test work indicated that covered entities are in compliance with HIPAA regulations but an overall control environment could be strengthened. Recent changes to HIPAA regulations in 2012 increased the risks related to security of PHI and ePHI. A strong control environment is mandated; if a breach was to occur, ASU would have reputational risk as well as monetary fines assessed dependent on the severity of the breach.

The evolution of the changing environment related to PHI and ePHI requires ASU to take proactive approaches to ensure all HIPAA standards and regulations are being not only met but exceeded. ASU is a unique and diverse institution that functions outside most normal facilities that need to meet HIPAA requirements. The constant evolution of the HIPAA process and uses of PHI and ePHI requires continual monitoring to assist in the mitigation of risks.

While many of the requirements stipulated by HIPAA were disseminated across the university, there did not appear to be uniform consistency of knowledge among Privacy and Security Officers interviewed. A need was expressed to have a more active influence from the University Privacy Officer providing direction and guidance to the covered entities.

It was noted during the audit the University HIPAA Privacy Officer has made multiple changes to the HIPAA process. With the continual evolvement of the HIPAA requirements, the university may want to consider providing additional help to the University Privacy Officer, to assist in the monitoring and functionality of the HIPAA process.

In the remainder of this report, Audit has identified exceptions to the process and additional steps that could be taken to mitigate risks associated with HIPAA regulations.

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			
• Business Associate Agreements are utilized for vendors handling PHI	Opportunity for Improvement	4	8
• Properly monitoring access to PHI and ePHI	Opportunity for Improvement	5, 7	9, 11
Effectiveness and Efficiency of Operations			
• Proper channels for distribution of business practices related to PHI	Reasonable to Strong Controls in place	N/A	N/A
• Regular communication is provided to covered entities handling PHI	Opportunity for Improvement	2	6
• HIPAA training is properly monitored and tracked	Reasonable to Strong Controls in place	N/A	N/A
Safeguarding of Assets			
• Proper forms and background checks are being completed	Opportunity for Improvement	6	9
• All personnel privy to PHI and ePHI have completed the HIPAA training	Opportunity for Improvement	3	7
• PHI and ePHI is properly secured	Opportunity for Improvement	1	6
Compliance with Laws and Regulations			
• ASU is following HIPAA regulations	Reasonable to Strong Controls in place	N/A	N/A
• Following ASU policies and procedures	Reasonable to Strong Controls in place	N/A	N/A

We appreciate the assistance of the University HIPAA Privacy and Security Officers and the University Privacy Officer.

Chris Crisci, CPA
Internal Auditor Senior

Tracy Grunig, MPA, CPA, CISA, CFE
Chief Audit Executive

Audit Results, Recommendations and Responses

1. Electronic Personal Health Information was stored on a local drive.

Condition: Nursing staff at the CONHI improperly stored ePHI on a local server instead of the secured network. The information was stored on the local server as it related to the current process for depositing co-pay funds collected from patients at the time services were rendered. The ePHI was being used for financial and patient account reconciliation purposes.

Criteria: Covered entities are required to store ePHI in a secure environment.

Cause: Nursing staff were unaware that the local servers were not considered secure. It was believed that since only they had access, it was considered secure.

Effect: ePHI stored on a local server instead of the secure Citrix server allows for greater access to the information. This increases the risk of a breach and the possibility of causing reputational and monetary damages to the university.

Recommendation: Ensure all ePHI is removed from local servers. Review the current deposit process and modify process to de-identify or not include PHI as it relates to deposit and patient reconciliation purposes.

Management Response: This recommendation has been initiated. The College of Nursing Privacy Officer is removing all ePHI from local servers and is revising the storage process. The university HIPAA Privacy Officer has reinforced university security practices reminding the department of effective security practices. Deadline for completion is December 31, 2015.

2. Increase the communication between HIPAA covered entities.

Condition: Currently, no continuous line of communication exists between the HIPAA Security and Privacy Officers of the covered entities. Group meetings are not being mandated for the Security and Privacy Officers to encourage sharing and learning opportunities to increase the knowledge of the entities. Many of the entities are functioning in a similar manner and exhibiting similar risks and challenges related to HIPAA compliance regulations.

Criteria: Communication of the entities is significant to gain economies of scale and increase the knowledge of each entity. Scheduled meetings may improve the dissemination of new PHI and ePHI requirements as well as provide an open forum to discuss problems or obstacles the entity may be faced with.

Cause: It has not been the practice of the university to have meetings for all covered entities.

Effect: Not having a formal channel of distribution and training for departments is leaving the university in a vulnerable position related to PHI and ePHI requirements regulated by HIPAA.

Recommendation: Conduct regular meetings with the Privacy or Security Officer attending. The regular meeting with personnel and staff from the covered entities could provide training and open forums to discuss obstacles or adversity they may be facing.

Management Response: This recommendation has been implemented. The ASU HIPAA Privacy Officer and HIPAA Security Officer have implemented an annual communication plan including regular meetings (likely quarterly) and regular communications and cross-training opportunities.

3. Contracted janitorial staff cleaning in areas with HIPAA related information are not properly trained or aware of the regulations surrounding HIPAA information.

Condition: Contracted janitorial staff has access to areas in the clinics and offices where PHI is stored. The janitorial staff had not completed the HIPAA training mandated by ASU.

Criteria: Mandating all contracted janitorial staff to perform the HIPAA training course decreases the liability to the university and ensures having proper recourse if PHI is improperly shared or breached.

Cause: Contracted janitorial staff with access to PHI was not required to complete the HIPAA training required by the university.

Effect: Contracted janitorial staff could improperly and unknowingly share PHI, leaving the university in an unfavorable position by not providing proper documentation for legal recourse.

Recommendation: The covered entities should review all personnel who have access or may come in contact with PHI and require them to complete the mandatory HIPAA training course required by the university and have them sign a document agreeing to the completion and understanding of PHI information.

Management Response: This recommendation has been initiated in Covered Entities (CE). A process has been worked out in Health Services that can be mirrored in other CEs. In addition, every CE engages in general privacy and security practices that limit exposure of PHI to janitorial staff.

4. No business associate agreement with Canon Inc. copiers exists.

Condition: A business associate performs functions or activities on behalf of a covered entity that involves access to protected health information or a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of another business associate. Cannon Inc. is responsible for performing maintenance and collection and redistribution of copiers. The copiers contain an internal hard drive allowing for the PHI to be stored on the copiers. This inadvertently gives Cannon Inc. access to university PHI. Business associate agreements are required with all partners that have access to PHI from the university.

Criteria: Canon Inc. is the copy machine provider for the university. Larger copiers have hard drives stored in the machines and Canon Inc. is responsible for the maintenance and recollection and redistribution of the machines.

Cause: Canon Inc. did not have a BAA filed with the university when the audit was conducted.

Effect: BAA's mandate the business handling PHI adhere to HIPAA rules and can be held accountable for a data breach and penalized for noncompliance. Without a signed BAA, the university could have less legal recourse on the company that has improperly stored, disposed, or shared PHI.

Recommendation: Obtain a BAA from Canon Inc. ensuring they are responsible and aware of the requirements for proper handling of copiers used with PHI information.

Management Response: ASU agrees with this recommendation. The process for obtaining a BAA with Canon has been initiated with Sam Wheeler, Executive Director Business and Auxiliary Services.

5. Perform more thorough self-monitoring audit steps on access to PHI at the covered entries.

Condition: Currently clinic staff are randomly selecting patients and reviewing who has accessed the patient's information to see if there has been improper access to a patient's record.

Criteria: The sampling method does provide a level of assurance. However, a more judgmental sampling method should be used when performing self-monitoring audit steps.

Cause: The clinics have always performed the review in this manner and the process has not been reviewed to identify a more efficient way of performing the review prior to this audit.

Effect: By using a random selection of patients, clinic staff is not effectively gaining insight into who is accessing patient's records. Limiting the review to a random sample is not conducive to identify the improper viewing of PHI by someone other than the intended person.

Recommendation: Perform a more thorough review of PHI accessed. For example, obtain a list of physician's known patients, and then review which patient files the physician have accessed outside of their known patients and determine the reason(s) for access to those patients.

Management Response: ASU agrees with this recommendation. All CEs will be asked to provide the University Privacy Officer and Security Officer a more thorough and specific process for reviewing access to PHI. The scheduled deadline for submitting a plan is December 31, 2015 and the scheduled deadline for implementation is June 30, 2016.

6. Confidentiality agreements signed by all personnel using PHI.

Condition: Currently it is not a requirement of the university to have all personnel handling or dealing with PHI sign a confidentiality agreement. Confidentiality

agreements provide legal documentation requiring an employee to sign a consent stating they understand general rules of PHI.

Criteria: Mandating all employees handling PHI and ePHI to complete a confidentiality agreement may decrease the liability to the university and ensure proper legal recourse if PHI is improperly communicated or shared.

Cause: It has not been the practice of the university to have staff and personnel sign confidentiality agreements in previous years.

Effect: Without a signed confidentiality agreement the university could reduce the legal consequences of an employee found who has improperly shared or discussed PHI. With a confidentiality agreement, the university would have legal recourse and reduce the chances of being in an unfavorable position.

Recommendation: Require all staff and personnel to sign a confidentiality agreement coinciding with the HIPAA training that is being mandated. Include this as part of the on-boarding process and annual certifications. Confidentiality agreements could include information such as the following:

- Protected Health Information (PHI) is considered confidential and should not be used for purposes other than its intended use.
- Ethical and legal obligation to protect PHI used or obtained in the course of performing duties and understand that all policies on confidentiality apply equally to data stored on the computer and on paper records as well as information discussed.
- Authorization to disclose PHI is made only by owners of the PHI and only on a need to know basis.
- Unauthorized use of, or access to, PHI may result in discipline up to and including termination. Violation or breach of confidentiality, with regards to PHI, may also create civil or criminal liability.

Management Response: ASU agrees with this recommendation. The HIPAA training module was revised. A “certification statement” will be added to the end of the training that will specifically state the above points in recommendation. Participants in the training are not be able to complete the training without certifying an understanding the general rules of PHI and University practice. This was added and part of the training released in summer 2015.

7. Roles and responsibilities of individuals utilizing and using PHI and ePHI are not documented and communicated to the entire organization.

Condition: A document with the responsibilities (e.g., job description) including information related to the specific roles and responsibilities of individuals utilizing PHI and ePHI should be maintained to reinforce the security standards issued by the HHS.

Criteria: Requesting departments to document the roles and responsibilities of individuals with access to PHI and ePHI will assist the covered entities and the University HIPAA Privacy Officer to clearly identify job duties and needs. In addition, provide a road map of who may be using PHI and ePHI allowing for reviews to be performed ensuring proper access.

Cause: The data needed to provide this information to the University HIPAA Privacy Officer had not been considered or developed prior to this audit.

Effect: Having a formal description of roles and responsibilities reported to the University HIPAA Privacy Officer could decrease the risk of staff and personnel improperly viewing or accessing PHI and ePHI. Roles and responsibilities documented can assist the University HIPAA Privacy Officer in identifying areas of concern within the organization. This could identify people accessing PHI and ePHI without a valid purpose.

Recommendation: Mandate all covered entities create organizational charts including job descriptions, roles, and responsibilities for individuals utilizing PHI and ePHI. The data should be provided to the University HIPAA Privacy Officer and regularly reviewed to determine if the responsibilities of individuals utilizing PHI and ePHI have been clearly defined.

Management Response: ASU agrees with this recommendation. As part of the annual communication plan, all Covered Entities will be asked to send an organization chart with roles and responsibilities related to PHI to the University Privacy Officer and Security Officer. Updates will be requested on an annual basis.

Distribution:

Arizona Board of Regents Audit Committee
Michael M. Crow, President
Morgan R. Olsen, Executive Vice President, Treasurer and Chief Financial Officer
Mark Searle, Deputy Provost, Chief of Staff and Professor
José A. Cárdenas, Senior Vice President and General Counsel
Lisa Loo, Deputy General Counsel
Joanne Wamsley, Vice President for Finance
Gordon Wishon, Chief Information Officer
Tina Thorstenson, Assistant Vice President and Chief Information Security Officer, HIPAA Security Officer
Aaron D. Krasnow, Assistant Vice President and Director, ASU Counseling Services, HIPAA Privacy Officer
Benjamin Mitsuda, Associate General Counsel, General Counsel for HIPAA Compliance