Port of Seattle

INTERNAL AUDIT REPORT

INFORMATION TECHNOLOGY AUDIT

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) COMPLIANCE AUDIT

2016

ISSUE DATE: AUGUST 8, 2016
REPORT NO. 2016-13

EXECUTIVE SUMMARY

AUDIT OBJECTIVES AND SCOPE

The purpose of the audit was to ensure the Port is in compliance with the requirements of the Health Insurance Portability and Accountability Act (HIPAA).

Details of our audit's scope and methodology are on page 2.

BACKGROUND

The HIPAA Security Rule includes the potential risks and vulnerabilities to the confidentiality, availability and integrity of all electronic protected health information (ePHI) that an organization creates, receives, maintains or transmits. This includes e-PHI in all forms of electronic media or portable electronic media. Electronic media includes a single workstation as well as complex networks connected between multiple locations.

Thus, an organization's risk analysis should take into account all of its ePHI, regardless of the particular medium in which it is created, received, maintained or transmitted, and regardless of the source or location of the e-PHI.

The HIPAA Privacy Rule extends the administrative, physical and technical safeguards of the HIPAA Security Rule to non-electronic PHI. 42 CFR 164.530(c) requires covered entities to have in place "appropriate administrative, physical and technical safeguards to protect the privacy of protected health information." Additional clarification is provided by the Office for Civil Rights (OCR) in its commentary on the Interim Final Breach Notification Rule in which it notes that "…the term ''unsecured protected health information'' can include information in any form or medium, including electronic, paper, or oral form." (Federal Register, Volume 74, No. 162, Monday, August 24, 2009. "Breach Notification for Unsecured Protected Health Information")

AUDIT RESULT

The Port is not in full compliance with the HIPAA ACT, which is prescriptive in its detailed and lengthy requirements. Opportunities exist to enhance Port practices and document procedures to become compliant.

TABLE OF CONTENTS

TRANSMITTAL LETTER

Audit Committee
Port of Seattle
Seattle, Washington

We have completed an audit of compliance with the HIPAA act.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards and the International Standards for the Professional Practice of Internal Auditing. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis of our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We extend our appreciation to the management and staff of the Human Resource Department, Information & Communications Technology (ICT), and Security & Emergency Preparedness for their assistance and cooperation during the audit.

On behalf of
Joyce Kirangi, CPA, CGMA
Internal Audit, Director

AUDIT TEAM	RESPONSIBLE MANAGEMENT TEAM
Brian Nancekivell, Sr. Auditor APGAR & Associates	Selena Tonti, CISO Claudia Kay, HIPAA Privacy Officer, HR Kim Albert, Asst. ICT Director

BACKGROUND

The HIPAA Security Rule encompasses the potential risks and vulnerabilities to the confidentiality, availability and integrity of all electronic protected health information (ePHI) that an organization creates, receives, maintains or transmits. This includes e-PHI in all forms of electronic media or portable electronic media. Electronic media includes a single workstation as well as complex networks connected between multiple locations.

Thus, an organization's risk analysis should take into account all of its ePHI, regardless of the particular medium in which it is created, received, maintained or transmitted, and regardless of the source or location of the e-PHI. The work related to HIPAA and ePHI is a small portion of the work that Port employee perform and PHI is likewise a small portion of all data that is used at the Port.

The HIPAA Privacy Rule extends the administrative, physical and technical safeguards of the HIPAA Security Rule to non-electronic PHI. 42 CFR 164.530(c) requires covered entities to have in place "appropriate administrative, physical and technical safeguards to protect the privacy of protected health information." Additional clarification is provided by the Office for Civil Rights (OCR) in its commentary on the Interim Final Breach Notification Rule in which it notes that "…the term ''unsecured protected health information'' can include information in any form or medium, including electronic, paper, or oral form." (Federal Register, Volume 74, No. 162, Monday, August 24, 2009. "Breach Notification for Unsecured Protected Health Information")

HIGHLIGHTS AND ACCOMPLISHMENTS

During the course of the audit, we observed the Port is well along the way towards compliance and implementing a robust information security program.

AUDIT SCOPE AND METHODOLOGY

To ensure that the Port is in compliance with the HIPAA requirements, we engaged Apgar & Associates, a firm specializing in HIPAA, to perform a detailed audit and risk assessment of the HIPAA Security and Privacy Rules.

Detailed reports and analysis were provided to management for their consideration.

CONCLUSION

The Port is not in full compliance with the HIPAA act, which is prescriptive in its requirements. Opportunities exist to enhance Port practices and document procedures to become compliant.

The Port of Seattle has made significant improvements to implement a robust information security program. However, several significant risks remain.

REPORTED ISSUES AND RECOMMENDATIONS

1. EXPAND THE SECURITY INCIDENT RESPONSE PLAN

The Port of Seattle has developed a security Incident Response Plan. The Plan does not address security incidents that involve protected health information except by referral to the Benefits Department. There is not a specific Privacy Incident Response Plan. The current policy only addresses incidents that were caused by the Port's employees and vendors.

Breaches are inevitable but the impact of a breach of sensitive information can be minimized if staff are trained and a thorough plan is developed. The cost of a breach can be significant if the team is unable to act quickly in the event of a breach of sensitive data. It is important to plan for breaches caused by employees and vendors. It's also important to plan for breaches that are the result of cybercrime.

Recommendations

We recommend that management expand the existing security incident response plan to address breaches of protected health information and train all team members. Management should also update its policy and plan to address breaches that are the result of cybercrime and/or physical intrusion by unauthorized individuals.

Management response

Management agrees that the Incident Response Plan should be expanded to address breaches (i.e. protected health information, privacy). This expansion, to include awareness and training will be led by the CISO.

2. Access termination policy

The Port has not adopted a termination policy. Defined termination procedures serve to ensure that terminating employees can no longer access Port assets following termination.

Recommendations

We recommend that management develop and adopt a termination policy and procedure and train impacted staff regarding responsibilities and timing for PHI.

Management Response

The Human Resources department appreciates the very thorough and specific approach that the auditors took while performing this audit. We believe it is important to recognize that about ten HR and other department employees have access to PHI and that it is imperative that this information be handled with the utmost care by those who work with it. We acknowledge that our existing employee off boarding practices do not specifically address off boarding employees when the termination is involuntary. To address this, the HR department plans to conduct a comprehensive review of all our HIPAA related practices in 2017. This review will include updating practices and associated

documentation as well as ensuring that training reflects updated practices and that employees needing to be aware of HIPAA requirements and those with access to PHI receive updated training on the updated practices.

3. Mobile device usage

Port employees may be permitted to access Port digital assets such as email using personally owned mobile devices. No tool has been implemented to manage personally owned devices to ensure that devices are encrypted and can be wiped if replaced, lost, or stolen.

Mobile device use in the workplace, especially personally owned devices, represents one of the most significant risks to companies working in the healthcare space today. The lack of a formal and communicated mobile device management policy in the general private and public sectors has and will continue to lead to loss of sensitive health data, harm to businesses and harm to individuals.

Recommendations

We recommend that the Port of Seattle enforce the remote wipe of personally owned mobile devices used to access Port resources that are lost or stolen. We also recommend requiring at a minimum an eight-digit passcode. Finally, we recommend that management adopt a BOYD (Bring Your Own Device) policy.

Management response

The Port currently has a mobile device management (MDM) solution that manages all Port-owned devices, as well as a mobile user agreement that is signed by all Port users issued Port mobile devices. Policy related to the use of Port systems and Port mobile devices is understood. Security controls are also enforced on Port devices, such as remote wipe, a robust passcode length and encryption.

For personally owned devices that receive Port email, the Port has another solution in place that supports a limited enforcement of passcode length and encryption. Management agrees that a formal personal device policy should be adopted and communicated across the Port. This will be an agenda item at the next scheduled IT Governance Board with the recommendation to technically (enforce) prohibit live-feed of Port email to Personal devices.

Port Policy, Code of Conduct-7 (CC-7) Information Systems and Services Acceptable Use Policy, explicitly prohibits the storing of HIPAA information on personal computers and removable media. Reference Section V that discusses Prohibited Item (g): Downloading or storing of Port sensitive information (e.g., Social Security Numbers, HIPAA, CJIS, credit card numbers, etc.) on personal computers, removable media, or portable devices.

CC-7, Section VI (h), also explicitly requires "System Users" to immediately report any lost or stolen systems to the service desk and to file a police report. It doesn't distinguish between personal and work systems.

4. Destruction of media

No mechanism is in place to ensure proper destruction by Benefits Department staff. It also appears a business associate agreement has not been executed between the Port of Seattle and the vendor to destroy media at the end of its useful life. The HIPAA Security Plan states that the disposal of electronic media created by the Benefits Department and other departments, such as HRD, and stored on disks and/or memory sticks is done by members of those departments using standard techniques or the media is transferred to ICT for destruction. "Standard techniques" are not defined. A draft policy was provided that indicates that all portable media at the end of its useful life is transferred to ICT for proper destruction.

Recommendations

We recommend that the Port adopt the policy changes and update the HIPAA Security Plan to reflect the changes.

Management response

Port Policy, Code of Conduct-7 Information Systems and Services Acceptable Use Policy, prohibits the storing of HIPAA information on removable media: Section V(g) Downloading or storing of Port sensitive information (e.g., Social Security Numbers, HIPAA, CJIS, credit card numbers, etc.) on personal computers, removable media, or portable devices;

If HRD and staff follow CC-7 policy, then sensitive data is not at risk from disposal policies as currently written. Nevertheless, Management agrees with the recommendation to finalize and communicate the destruction policy for the Port. The HIPAA Security Plan will be updated to reflect required method/process of destruction.