INTERNAL AUDIT REPORT

Information Technology Audit

Health Insurance Portability and Accountability Act (HIPAA) Privacy & Breach Compliance Audit

January 2016 – July 2019

Issue Date: September 13, 2019
Report No. 2019-14 A

Prepared by Apgar & Associates, LLC in partnership with the Port of Seattle's Internal Audit Department

Port of Seattle | INTERNAL AUDIT

Table Of Contents

Executive Summary

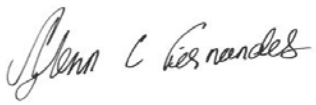
Internal Audit (IA) in partnership with Apgar & Associates, LLC completed an audit of HIPAA Privacy and Breach compliance for the period January 2016 through July 2019. HIPAA Security compliance, which has security sensitive elements, will be addressed in a separate audit report. The audit was performed to assess the privacy practices at the Port of Seattle involving the use, maintenance, transmission and disclosure of protected health information (PHI) and personally identifiable information (PII) in connection with the Port's employee benefit plans. Existing processes and controls in place to protect PHI were assessed against the HIPAA Privacy and Breach Rules using the federal Office for Civil Rights (OCR) Audit Protocol to determine the level of compliance and identify areas for improvement.

Self-funded group health plans, and other employer welfare plans providing medical benefits that share information with employers, must comply with the privacy, security and breach notification rules under HIPAA. Employer-maintained self-funded medical plans, such as a major medical plan, a medical Flexible Spending Account, a Health Reimbursement Arrangement (HRA), or a self-funded dental plan, are "covered entities" under HIPAA. These covered entities are required to evaluate risks and necessary protections for plan information and to document the evaluation and the policies and procedures the employer adopts for the plan to protect all plan information. While the audit noted that the Port maintains certain employee PHI such as enrollment and eligibility data, the Port does not maintain employee medical records.

Our audit noted that the Port is not in compliance with several requirements of HIPAA Privacy & Breach Notification Rules, and we identified the following issues.

1. (High) – The Port had not designated itself as a hybrid entity for the purposes of the HIPAA Rule. The Port had not defined what units within the Port were part of the designated health care component.
2. (Medium) – The Port's understanding of what systems and applications create, receive, use, maintain or transmit PHI and EPHI was incomplete. Combined with the hybrid entity issue, this could result in team members having more access to sensitive information than allowed by law and regulation.
3. (Medium) – The Port did not consistently enter into and manage business associate agreements with vendors that use, disclose, maintain or transmit the Port's PHI and EPHI to perform a business function for the Port.
4. (Medium) – HIPAA Privacy and Breach Training were not being provided to Port employees within a reasonable timeframe.
5. (Medium) – The Port did not provide any four-factor risk assessment required under federal law to document how the organization made the determination that there was a low risk of compromise to PHI from the acquisition, access, use, or disclosure of protected health information in a manner not permitted under the Privacy Rule.

These issues are discussed in more detail beginning on page five of this report.



Glenn Fernandes, CPA
Director, Internal Audit

Responsible Management Team
Katie Gerard, Sr. Director Human Resources
Matt Breed, Chief Information Officer
Brad Jenson, Interim Director of Information Security
Sandra Spellmeyer, Total Rewards Mgr. Human Resources (Privacy Official)
Tammy Woodard, Director HR-Total Rewards

Background

The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) enforces the following HIPAA Privacy, Security and Breach Notification Rules:

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.

HIPAA established important national standards for the privacy and security of protected health information and the Health Information Technology for Economic and Clinical Health Act (HITECH) established breach notification requirements to provide greater transparency for individuals whose information may be at risk. HITECH required the OCR to conduct periodic audits of covered entity and business associate compliance with the HIPAA Privacy, Security, and Breach Notification Rules. A pilot program in 2011 and 2012 assessed the controls and processes implemented by 115 covered entities to comply with HIPAA's requirements. OCR implemented phase two of the program in 2016, auditing both covered entities and business associates. As part of this program, OCR developed enhanced protocols to assess compliance in each of the regulatory areas. The OCR uses the protocols to assess organizational compliance in case of complaint or breach investigation.

HIPAA is applicable to the Port's medical and dental programs. The objective of this audit was to evaluate the effectiveness of management controls to assure the proper protection of individually identifiable health information in compliance with the HIPAA Privacy and Breach requirements while following the OCR Audit Protocol.

HIPAA Security is addressed in audit report number 2019-14B.

Audit Scope and Methodology

We conducted the engagement in accordance with GAGAS and the International Standards for the Professional Practice of Internal Auditing. Those standards require that we plan and conduct an engagement to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our engagement objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our engagement objectives.

The period audited was January 2016 through July 2019 and included the following procedures:

- Onsite assessment of the physical safeguards in place to assure the privacy of PHI and PII at the Port of Seattle occurred at Port offices.
- Structured interviews with Port management charged with HIPAA compliance activities.
- Review of policies and procedures related to HIPAA compliance.
- Obtained evidence as defined in the OCR audit protocol.
- Reviewed vendor contracts and related agreements.
- Tested relevant controls to assess their operating effectiveness.
- Performed an assessment of the HIPAA training process.

Schedule of Findings and Recommendations

1) Rating: High

The Port had not designated itself as a hybrid entity for the purposes of the HIPAA Rule. The Port had not defined what units within the Port were part of the designated health care component.

The Port offers, administers and self-insures various group health plans and is a covered entity for purposes of the HIPAA Privacy & Breach Notification Rules. Absent the hybrid entity designation, all Port operations and personnel are subject to HIPAA Privacy & Breach Notification Rules. This was a repeat finding from the Port's HIPAA Compliance Audit performed in 2016 by Apgar & Associates, LLC.

Recommendations:

We recommend that the Port's Privacy Official should:

1. Take the action necessary to designate the Port as a hybrid entity.
2. Designate the positions and function that fall within the designated health care component of the Port.

Management Response/Action Plan:

After consulting with legal counsel; Human Resources, Information/Communication Technology, and Information Security, have determined the Port, as a whole, is not a covered entity under HIPAA. We do agree that specific health plans sponsored by the Port are covered by HIPAA and we should work through the process of designating the benefit plans as a hybrid entity. We appreciate the Auditor helping us to understand that the steps we previously took did not fully accomplish this goal. The Port's Human Resources, Information/Communication Technology, Information Security and internal legal staff are consulting with outside counsel to complete the steps necessary to fully designate the group health plans sponsored by the Port as the health care component of a Hybrid Entity.

DUE DATE: 11/30/2019

2) Rating: Medium

The Port's understanding of what systems and applications create, receive, use, maintain or transmit PHI and EPHI was incomplete. Combined with the hybrid entity issue, this could result in team members having more access to sensitive information than allowed by law and regulation.

Staff members throughout Total Rewards and ICT had access to protected health information and electronic protected health information (PHI and EPHI) through their access to Port-hosted and vendor-hosted tools to implement and manage benefit plans. Since the Port had not defined what units within the Port were part of the designated health care component, access to PHI may not be appropriately designed. We additionally noted that carrier portal access by Port staff was not routinely monitored or reviewed.

Recommendations:

We recommend that the Port's Privacy Official should:

1. Conduct a thorough review of all Port-hosted tools and applications that create, receive, maintain, use or disclose PHI or EPHI.
2. Review employee access to the tools and applications discovered in step one.
3. Restrict access as appropriate to employees who are part of the designated health care component and need the access to perform their job duties.
4. Conduct the same review with vendor-hosted tools and applications that create, receive, maintain, use or disclose PHI or EPHI.
5. Review employee access to the tools and applications discovered in step four.
6. Restrict access as appropriate to employees who are part of the designated health care component and need the access to perform their job duties.
7. Train the relevant employees.
8. Develop a process to routinely review carrier portal access by Port employees. This should include definition of who can authorize such access; written records of approval and steps to be taken at employee termination from employment in the designated health care component.

Management Response/Action Plan:

The Port's perspective is points 1-3 are applicable to Port hosted tools to manage benefit plans. The Port's Human Resources, Information/Communication Technology, and Information Security teams are working with legal counsel to confirm which Port hosted tools or application contain PHI and EPHI.

Information/Communications Technology has a documented list of individuals with access of the different Port-hosted tools and applications and reviews and maintains this access by the list on a quarterly basis. Once the tools and applications that contain PHI/EPHI are confirmed, Human Resources will work with Information/Communications Technology to update their current list to specify the tools containing PHI/EPHI on the list. When access to the tools containing PHI/EPHI is updated Information/Communications Technology can notify Human Resources of the individuals with access to these so Human Resources can ensure HIPAA training has been provided.

The Port's perspective is points 4-6 & 8 are applicable to Vendor hosted tools to manage benefit plan data. Human Resources is aware of the vendor hosted tools and applications contain PHI/EPHI and is taking steps to confirm that Information/Communications Technology also maintains a list documenting Port employee with access of Vendor-hosted tools and applications, and that this list is reviewed and updated quarterly with changes to employees having access. Once the vendor tools and applications access list is confirmed, Human Resources, Information Security and Information/Communications Technology will confirm which vendor tools contain PHI/EPHI so this can be noted on the list.

Information/Communications Technology can then notify Human Resources of the individuals with access to the vendor tools containing PHI/EPHI so that Human Resources can ensure HIPAA training has been provided to employees who require it.

The Port agrees training employees on HIPAA is important, please see our response to number 4.

DUE DATE: 11/30/2019

3) Rating: Medium

The Port did not consistently enter into and manage business associate agreements with vendors that use, disclose, maintain or transmit the Port's PHI and EPHI to perform a business function for the Port.

No Business Associate Agreement was provided for SharePoint (Microsoft). The Port stores PHI and EPHI in SharePoint. A business associate agreement is required. Business Associate Agreements are missing pages. In at least one instance, the Business Associate Agreement does not explicitly address the business associate's regulatory responsibility to ensure compliance with the HIPAA Security Rule. A business associate agreement was provided with an original effective date of July 26, 2019. The Service Agreement between the Port and the vendor was fully executed in September 2016. No single group appears to have been tasked with business associate contract management. This was a repeat finding from the Port's HIPAA Compliance Audit performed in 2016 by Apgar & Associates, LLC.

Recommendations:

We recommend that the Port's Privacy Official should:

1. Execute a business associate agreement with SharePoint at the earliest possible date.
2. Clarify the process by which vendors are determined to be business associates.
3. Designate a work unit as lead in the business associate contracting process.
4. Review all existing business associate agreements to make sure that they are fully compliant with the requirements of the HIPAA Privacy and Security Rule.

Management Response/Action Plan:

The Port is working with legal counsel to determine which vendors are Business Associates and require Business Associate Agreements. If vendors are determined to be Business Associates and the Port's contract with that vendor does not include a Business Associate Agreement work will begin to add a Business Associate Agreement to the contract.

The Port agrees that having a defined process for determining which vendors are Business Associates and therefore require a Business Associate Agreement is beneficial and will bring relevant groups together to establish this process.

The Port agrees that designating a work unit lead to ensure Business Associate Agreement are appropriately in place will be beneficial and will bring relevant groups together to identify these work unit leads.

All current Business Associate Agreement have been reviewed and one Business Associate Agreement was identified, which needs updated language. Work is underway with the vendor to get an updated Business Associate Agreement in place.

DUE DATE: 12/31/2019

4) Rating: Medium

HIPAA Privacy and Breach Training were not being provided to Port employees within a reasonable timeframe.

According to the Privacy Rule, HIPAA training is required for "each new member of the workforce within a reasonable period of time after the person joins the Covered Entity´s workforce" and also when "functions are affected by a material change in policies or procedures" – again within a reasonable period of time. According to the Privacy Rule, HIPAA training is required initially and for all new hires, while best practice is to periodically repeat the training.

The external consultant noted that the HIPAA Privacy and Breach Training at the Port most recently occurred in October 2017 and that the training videos were produced in December 2017.

Recommendations:

We recommend that the Port's Privacy Official should:

1. Train all the existing employees in the designated health care component no later than December 31, 2019.
2. Train all new hires in the designated health care component within 30 days from their date of hire.
3. Institute regular refresher training for staff in the designated health care component no less frequently than annually.
4. Review and update as necessary any existing training videos.

Management Response/Action Plan:

Information Security has set up HIPAA Compliance training as a required learning module in the Learning Management System for certain departments and job roles that may have access to HIPAA information. Those training records are available upon request. This training is not required of all employees, only those in designated areas.

Human Resources has not had automated HIPAA training available through the Learning Management System. New hires have been manually notified of required HIPAA training and received this training via video or paper materials when Human Resources was made aware of a new hire with access to PHI and EPHI in conjunction with the Port sponsored health plans.

Human Resources is in the process of automating HIPAA training through the Learning Management System. This training will be assigned to all employees identified as potentially having access to HIPAA related information associated with the Port sponsored health plans. Training will be assigned to all applicable new hires to be completed within 30 days from their date of hire. In addition, annual HIPAA refresher training is being implemented.

DUE DATE: 10/31/2019

5) Rating: Medium

The Port did not provide any four-factor risk assessment required under federal law to document how the organization made the determination that there was a low risk of compromise to PHI from the acquisition, access, use, or disclosure of protected health information in a manner not permitted under the Privacy Rule.

The Rule requires that any acquisition, access, use, or disclosure of protected health information in a manner not permitted in the Privacy Rule is presumed to be a breach unless the entity demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment. While the Port stated that no breaches have occurred, there was at least one situation where the Port investigated to determine whether a security weakness had led to a breach but did not document the use of a four-factor risk assessment.

Recommendations:

We recommend that the Port's Privacy Official should:

1. Review all privacy and security incidents that involved plan member PHI and EPHI that was acquired, accessed, used or disclosed in a manner not permitted by the Privacy Rule during the audit period.
2. Determine if regulatory requirements were followed – i.e., documentation of a breach exception and completion of a four-factor risk assessment.
3. For any 2019 incidents in which regulatory requirements weren't followed, execute and document the required regulatory steps.
4. Consult with the Legal Department to determine treatment of 2018 incidents in which regulatory requirements weren't followed.

Management Response/Action Plan:

Human Resources and Information Security will create a log to document all the incidents involving PHI and EPHI that are brought to the Port's attention. These departments will bring together appropriate individuals to conduct an appropriate risk assessment on each identified incident. Human Resources, Information/Communication Technology, and Information Security will also bring together appropriate individuals to discuss any 2018-2019 incidents to ensure appropriate assessments have been completed. Any 2018-2019 incidents and assessments will be added to the Port's incident log.

DUE DATE: 10/31/2019

Appendix A: Risk Ratings

Findings identified during the audit are assigned a risk rating, as outlined in the table below. Only one of the criteria needs to be met for a finding to be rated High, Medium, or Low. Findings rated Low will be evaluated and may or may not be reflected in the final report.

Rating	Financial Stewardship	Internal Controls	Compliance	Public	Commission/ Management
High	Significant	Missing or not followed	Non-compliance with Laws, Port Policies, Contracts	High probability for external audit issues and / or negative public perception	Requires immediate attention
Medium	Moderate	Partial controls Not functioning effectively	Partial compliance with Laws, Port Policies Contracts	Potential for external audit issues and / or negative public perception	Requires attention
Low	Minimal	Functioning as intended but could be enhanced to improve efficiency	Mostly complies with Laws, Port Policies, Contracts	Low probability for external audit issues and/or negative public perception	Does not require immediate attention