State of Wisconsin
Department of Employee Trust Funds
Robert J. Conlin
SECRETARY

801 W Badger Road
PO Box 7931
Madison WI 53707-7931

1-877-533-5020 (toll free)
Fax 608-267-4549
etf.wi.gov

Correspondence Memorandum

Date: March 6, 2018

To: Audit Committee

From: Yikchau Sze, Director
Office of Internal Audit (OIA)

Subject: HIPAA Privacy and Breach Notification Compliance Audit

This report is for Committee review and discussion. No action is required.

Attached is the audit report of a HIPAA privacy and breach notification compliance audit. The results of this audit have been submitted and discussed with the Office of the Secretary, Department of Employee Trust Funds (ETF).

This audit was conducted in accordance with the biennial Audit Plan for Fiscal Year 2018-2019.

The results of this audit indicate that ETF complied with the material provisions of the HIPAA Privacy and Breach Notification Rules. However, OIA identified two findings that represent higher risk for the organization and offered three observations to improve the administration of HIPAA compliance activities at ETF.

This audit was conducted by Rick Onasch, who will be available at the Committee meeting to discuss the audit and answer any questions.

Attachment: HIPAA Privacy and Breach Notification Compliance Audit Report

Reviewed and approved by Robert J. Conlin, Secretary

Electronically Signed 3/13/18

Board	Mtg Date	Item #
AUD	3.29.18	5

Office of Internal Audit

HIPAA Privacy and Breach Notification Compliance Audit

March 1, 2018

Prepared for Audit Committee meeting of the Employee Trust Funds Board, March 29, 2018

Objective:

The audit objective was to assess Employee Trust Fund's (ETF) compliance with the Privacy Rule and the Breach Notification Rule of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The audit was also conducted to evaluate data sharing agreements with vendors for adequate protection of personally identifiable information (PII) and protected health information (PHI) of Wisconsin Retirement System (WRS) members and their dependents.

Scope:

The audit scope focused on ETF's compliance with the Privacy Rule and Breach Notification Rule as of January 19, 2018, and the potential HIPAA incident reporting during January through September 2017. Also in scope are the business associate[1] agreements effective in 2017, specifically, the contract language regarding PII and PHI protection.

Background:

The Regulation

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) included Administrative Simplification provisions that required the US Department of Health and Human Services (HHS) to adopt national standards for electronic health care transactions and code sets, unique health identifiers, and security. Recognizing that the advance in electronic technology could erode the privacy of health information, Congress also incorporated into HIPAA provisions that mandated the adoption of Federal privacy protections for PHI. Subsequently, HHS published the Privacy Rule, Security Rule, Breach Notification Rule, and Enforcement Rule.

The Privacy Rule sets national standards for the protection of PHI by three types of covered entities: health plans, health care clearinghouses, and health care providers who conduct standard health care transactions electronically. Compliance with the Privacy Rule was required as of April 14, 2003, for most such entities.

The Security Rule specifies safeguards that covered entities and their business associates must implement to protect the confidentiality, integrity, and availability of electronic protected health information. Compliance with the Security Rule was required as of April 20, 2005 (not within scope of this audit).
The Breach Notification Rule was promulgated by HHS in 2009 following the enactment of the HITECH Act[2] to strengthen the privacy and security protections for PHI under HIPAA. Under

[1] Business Associate – A "Business Associate" is a person or entity, other than a member of the workforce of a covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to protected health information.
[2] HITECH – The Health Information Technology for Economic and Clinical Health Act, was enacted under Title XIII of the American Recovery and Reinvestment Act of 2009.

certain circumstances, it requires a covered entity to notify affected individuals, the Secretary of HHS, and, for some cases, regional media, of a breach[3] of unsecured PHI. In addition, a business associate must notify covered entities and follow the same notification standards as a covered entity if a breach occurs at or by the business associate.

The Enforcement Rule provides standards for the enforcement of all the Administrative Simplification Rules. It contains provisions relating to compliance and investigations, the imposition of civil money penalties for violations (from $100 per violation, per day, per year up to a maximum cumulative penalty of $1.5 million per year), and procedures for hearings.

ETF's Administration of HIPAA Compliance

ETF administers a self-insured prescription drug benefit plan and a self-insured dental coverage for the employees of state and local participating employers, annuitants, and eligible dependents. Because ETF creates, stores and transmits PHI of the individuals covered by the self-insured plans, ETF is subject to HIPAA.

In 2003, when the HIPAA Privacy Rule became effective, ETF appointed a HIPAA Compliance Manager to establish the compliance program at ETF. This person was also designated the HIPAA Privacy Officer as mandated by the Rule. The Privacy Officer was also responsible for the HIPAA Security Rule when it became effective in 2005. In 2008, ETF created the Office of Policy, Privacy, and Compliance (OPPC) to ensure ETF's compliance with various federal and state rules and regulations.

The Privacy Officer oversees the development, implementation, maintenance of, and adherence to privacy policies and procedures regarding the safe use and handling of PHI in compliance with HIPAA regulations. The Privacy Officer also maintains the day to day duties relevant to HIPAA compliance based on the activities or privacy issues that occur with PHI at ETF. The Security Officer, as required by the HIPAA Security Rule, is responsible for developing and implementing security policies and procedures for ETF. Historically, the Security Officer's responsibilities have been shared between the Privacy Officer and the Information Security Officer of the Division of Management Services. In May of 2017, ETF hired a Chief Information Security Officer to further develop ETF's information security. This employee is now the sole designated person responsible for compliance with the Security Rule.

Testing:

The Office of Internal Audit (OIA) conducted this audit by:

[3] Breach – as defined by HIPAA is: "an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information (PHI)."

- Researching relevant laws and regulations
- Obtaining an understanding of ETF's compliance program, including conducting interviews of the Privacy Officer, and reviewing policies and procedures developed by the OPPC
- Mapping relevant HIPAA requirements to ETF's current policies, procedures and practices
- Vouching a sample of supporting documents to ensure policies and procedures were appropriately followed when applicable
- Examining contractual terms and conditions of selected vendor contracts for appropriate inclusion of HIPAA compliance requirements and appropriate protection of PII and PHI
- Testing of HIPAA privacy incident reporting for timeliness and appropriate reporting

Mapping Relevant HIPAA Requirements to ETF's Current Policies, Procedures and Practices

OIA adopted the HIPAA self-assessment questionnaires from AuditNet[4]. The self-assessment tool was developed by AuditNet based on the Office for Civil Rights HIPAA audit program. There is a total of 152 questions relating to material provisions of the Privacy Rule and the Breach Notification Rule that were examined by OIA. By interviewing responsible staff and reviewing relevant documentation, OIA was able to map all the questions of the adopted questionnaires to ETF's current policies, procedures and practices. Of the 152 questions, ETF fully addressed 150. In the Finding section of the report, we recommended actions that ETF could consider to fully address the remaining two questions.

Vouching Supporting Documents to Verify Adherence to Policies and Procedures

OIA reviewed HIPAA policies and procedures created by OPPC and mapped them to relevant provisions of the HIPAA regulations. To verify that policies were implemented and procedures were followed, OIA requested supporting documents for our testing. For example, we selected samples from a list of forms ET-7414, *Authorization to Disclose Medical Information*, to verify that ETF properly disclosed PHI to the requested party. We also selected samples from a list of forms ET-2421, *Request to Copy or Inspect Medical Information*, to verify that ETF distributes the medical information based on the proper request. Although no exceptions were noted during our audit, there was also no evidence of review of such forms being conducted by OPPC to monitor compliance.

Testing Privacy Incident Reporting

Privacy incidents were either reported to the Privacy Officer by ETF staff for internal reportable incidents or the Privacy Officer was notified by business associates in compliance with the Privacy Breach Notification clause of vendor contracts. The Privacy Officer enters and tracks the reported incidents on an Excel spreadsheet.

[4] AuditNet – serves the global internal audit community as an online digital network where auditors share resources, tools, and experiences including audit work programs and other audit documentation. OIA obtained access to AuditNet's repository online audit programs through the TeamMate audit management software license.

From January through September of 2017, the Privacy Officer received 44 incident reports, of which 12 were internal and 32 were external. Our review of the 12 internal privacy incidents did not indicate potential HIPAA breaches. Since OIA had conducted an audit on the internal incident reporting in 2014 without exceptions, we focused our testing on external reported privacy incidents. The majority of the privacy incidents reported by third parties were not based on requirements under HIPAA, but based on contractual requirements with ETF or the Group Insurance Board. Those third parties are considered covered entities in their own right and not business associates of ETF or the Group Insurance Board.

We tested attributes outlined in the HIPAA regulation for breach notification. Of the eight incidents randomly selected for testing, we were able to verify that incidents were reported appropriately. We reviewed the incident reports from the third parties and communications from the third parties that are stored in a shared OPPC folder. We also reviewed a tracking spreadsheet maintained by the Privacy Officer. The information recorded on the tracking spreadsheet is not adequate to understand the incidents being reported and does not contain the incident reports or communications from third parties but merely tracks the incidents.

Contract Review

A business associate who as a person or organization, interacts with PHI from ETF must follow the HIPAA privacy and security rules and must protect the PHI and administer it consistently with the obligations of ETF. All business associates are required by HIPAA to sign a business associate agreement, a legal contract that describes how the business associate adheres to HIPAA along with the responsibilities and risks they take on.

We reviewed the terms and conditions of the following three vendor contracts that are in effect in 2017: Navitus contract (Pharmacy Benefit Manager), Truven contract (Data Warehouse and Visual Business Intelligence Solution), and the Stay Well contract (Wellness Program for WRS). In particular, we focused our review on Section 22 “Confidential Information and HIPAA Business Associate Agreement” and Section 28 “Data Security and Privacy Agreement” to ensure that contract language satisfies HIPAA business associate agreement provisions and PII confidentiality protection. We also noted that all three contracts carry the term “Privacy Breach Notification” that requires that the vendor must notify ETF within 24 hours of any incident that occurs if discovered that PHI or PII may have been breached or has been breached.

We did not identify any exceptions during our contract review and conclude that the terms and conditions, especially Section 22 and 28 address the data use and data sharing requirements and is adequate in protecting PHI and PII of WRS’s members and their dependents.

Results:

Findings:

1. Changes to published Notice of Privacy Practices (NPP) were updated timely but were not published on the ETF website prior to the effective date of the changes; revisions to privacy policies were not always published in a timely manner.

To meet HIPAA administrative requirements, material changes to the NPP need to be updated in a prompt manner. During our testing, we noticed that although ETF changed certain health insurance plans for 2018 by removing some self-insured plans and adding the Uniform Dental Benefits, the changes were not reflected in the NPP that was published on ETF's internet site as of January 1, 2018. The version displayed online was updated on January 23, 2018, instead of January 1, 2018, which was the effective date of the changes. The delay in updating the changes in the NPP could cause confusion to a WRS member as to which health insurance plan the NPP applies to.

In addition, although ETF updated 18 privacy policies and published the revised policies on ETF's intranet as of April 2017, two policies, policy 14 – No Retaliation Against Persons Exercising Privacy Right, and policy 16 – Actions in Response to Unauthorized Uses or Disclosures, were still dated as of April 2005, on ETF's intranet.

Please note, publication updates were made to the above-mentioned notice and policies once we communicated our findings to OPPC at the end of our testing.

Recommendation:

We recommend that ETF develop a process to track what needs to be updated and ensure that updates are published in a timely manner.

Management Response: Updates to the NPP are determined by the Privacy Officer each year during the "It's Your Choice" annual process. Please note that this was a matter of changing names of health plans in the NPP, and that there were no material changes to the provisions that affect privacy rights. We provided the final updates of plan name changes to the Office of Communications (OC) in mid-December, but OC did not complete the updates until OPPC contacted OC again in January. Going forward, OPPC will ensure that updates are made and published by January 1 of any year, as necessary, and promptly following a material change.

The policies referenced by this finding were indeed updated timely by the OPPC. However, in the publishing process, the OC hyperlinked to the old policies for two of the policies, rather than to the updated documents. In any event, OPPC will ensure that updates to the HIPAA privacy policies are made as necessary and will follow through to ensure that the updates are properly and timely published.

Responsible Staff: Steve Hurley and Mary Alice McGreevy
Completion Date: August 31, 2018

2. The written policy and procedures for notifying the media of potential large breaches of over 500 individuals have not been formally adopted by the agency.

The requirements of HIPAA regulations calling for notification to individuals in the event of a large breach of over 500 individuals are very specific. There are timeframes involved, mitigation efforts, determination of what PHI was compromised or involved and the need for documentation of all actions taken. The process is quite detailed and lengthy based on the actual HIPAA regulations. Although OPPC has developed the policy and procedure for privacy incident response, without formal approval and adoption of the policy and procedure, ETF's proper handling of a large breach that addresses all HIPAA requirements could be at risk.

Recommendation:

We recommend that ETF formalize the written policy and procedure for notifying the media of potential large breaches to ensure a timely and orderly response that is in compliance with HIPAA.

Management Response: OPPC agrees with the recommendation. OPPC has written a policy and procedure for privacy incident responses. However, it has not been formally adopted by the agency and is being reviewed in conjunction with the CISO's development of a new security breach incident plan. OPPC has had an internal (to OPPC) written privacy incident policy and procedure for many years.

Responsible Staff: Steve Hurley and Mary Alice McGreevy
Completion Date: August 31, 2018

Observations:

1. Review to ensure that adequate and correct information were obtained on forms that were used by individuals who requested copies of their own PHI record or authorized another person or entity to get those records is not consistently performed.

Individuals who request a copy of their own PHI records or authorize another person or entity to get those records must fill out HIPAA-related forms. OIA was able to verify, through our sample testing, that those forms were used correctly and contained required information. However, we noticed that OPPC did not perform monitoring review of those forms to verify that existing policies and procedures were adhered to.

Recommendation:

We recommend that OPPC perform periodic and random review of HIPAA information access forms to verify compliance with policies and procedures. The results of these random reviews should be recorded and maintained.

Management Response: OPPC agrees with the recommendation to perform periodic review of submitted HIPAA authorization forms. OPPC currently reviews these forms on an ad hoc basis. For several years after the HIPAA Privacy Rule implementation date, OPPC did in fact review all such HIPAA-related forms as they came into the agency for HIPAA compliance. However, as ETF staff matured in their understanding of HIPAA and these forms, we made the decision to have ETF's Member Services process these forms, and contact OPPC whenever there was a question. Over the years, ETF staff have requested that OPPC review many of the forms. This arrangement has improved efficiency and customer service, while allowing OPPC to weigh in on more complex situations. However, we feel that the periodic review that has been suggested would augment our documentation efforts. We propose that such review be conducted annually.

Responsible Staff: Steve Hurley and Mary Alice McGreevy
Completion Date: Review conducted and recorded by July 1 each year.

2. The Incident Report tracking spreadsheet that is used by OPPC to log reported incidents does not contain all the relevant information regarding each incident to allow an efficient review and follow-up. The related information and documentation is contained in separate files.

The Privacy Officer at OPPC logs reported privacy incidents in an Excel spreadsheet. The spreadsheet is used as a management tool by OPPC to coordinate and address privacy matters. Although all the information regarding the privacy incident could be found on the individual Incident Report, including additional information on the tracking spreadsheet, such as the determination of whether it was PII or PHI, when the matter was resolved, would make review and follow-up on the privacy matter more efficient.

Recommendation:

To improve operational efficiency, we recommend that OPPC include the following information on the Incident Report tracking Excel spreadsheet: a more detailed explanation of what occurred, comments from OPPC, if correspondence was sent, when the matter is resolved or closed and a final status and date. In addition, we recommend that the initial actual Privacy Incident Reports, other supporting documents, such as written correspondence that assisted in the determination, be hyperlinked or cross referenced to the spreadsheets to allow for a more efficient future reference and review.

Management Response: OPPC agrees that adding certain information and hyperlinks into the tracking spreadsheet could improve efficiency when reviewing privacy incident history. However, in our view, the tracking spreadsheet has adequately performed its function, which is to record basic information to allow the Privacy Officer and others in OPPC to coordinate the status of privacy matters. As noted, more detail can be found in the corresponding Privacy Incident Reports.

Responsible Staff: Steve Hurley and Mary Alice McGreevy
Completion Date: July 1, 2018

3. Cross training to handle compliance of HIPAA Privacy and Breach notification rules is lacking.

The Privacy Officer at OPPC is the only individual who handles this critical compliance function. Although a backup to the Privacy Officer was identified, no staff are currently specifically cross-trained. As such, the risk of non-compliance increases should the Privacy Officer be unavailable.

Recommendation:

Consider cross-training additional ETF staff to handle HIPAA Privacy Officer duties.

Management Response: OPPC's Office Director was formerly the HIPAA Privacy Officer and is familiar with the duties of the role and fulfills the duties of the role when the Privacy Officer is away from ETF. Specific cross-training of all staff in OPPC will be conducted before July 1, 2018.

Responsible Staff: Steve Hurley and Mary Alice McGreevy
Completion Date: July 1, 2018

Conclusion:

The results of our audit indicate that ETF complied with the material provisions of HIPAA Privacy and Breach Notification Rules. We identified two findings during the audit that represent higher risk for the organization and offered three observations to OPPC to improve the future performance of this compliance function.