Office of Internal Audit

UT Southwestern
Medical Center

The University of Texas Southwestern Medical Center
HIPAA Privacy Program Audit

Internal Audit Report 15:20

July 6, 2015

Table of Contents

Executive Summary

Background

The Health Insurance Portability and Accountability Act (HIPAA) was created in 1996 to safeguard protected health information (PHI). PHI is individually identifiable health information; which includes individual demographic information, the individual's past, present, or future physical or mental health conditions, or the provision of healthcare. The Office for Civil Rights (OCR) enforces the following rules issued by the U.S. Department of Health and Human Services (HHS):

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

The University of Texas Southwestern Medical Center (UT Southwestern) maintains and transmits PHI throughout various locations such as hospitals, clinics, pharmacies, research departments, and billing departments. The Privacy Office together with the Information Security Office are responsible for ensuring compliance with all regulatory requirements in regards to the handling of PHI and ePHI within UT Southwestern. The Executive Compliance Committee provides governance over these functions.

The Privacy Office, within the Office of Compliance, addresses issues related to privacy practices, patient privacy rights, privacy concerns, and complaints. Specifically, the Privacy Office will:

- Designate a privacy officer.
- Develop and implement institutional privacy policies and procedures.
- Establish, update and monitor required HIPAA training programs.
- Serve as a resource for employees, faculty, and students on privacy matters.
- Conduct internal monitoring and assessments for compliance with established privacy rules and practices.
- Respond to privacy rights requests and detected offenses, and develop corrective actions.
- Enforce disciplinary standards through well publicized guidelines.

The Information Security Office handles the provisions related to the HIPAA Security Rule. The Privacy Office coordinates with the Security Office on any technology related privacy matters.

Scope and Objectives

The UT Southwestern Office of Internal Audit has completed its HIPAA Privacy Program Audit. This was a compliance risk based audit and part of the fiscal year 2015 Audit Plan. The audit scope included processes related to the activities of the Privacy Office from January 1, 2014 to March 31, 2015. Audit procedures included interviews with stakeholders, review of policies and procedures and other documentation, data analytics and substantive testing.

Executive Summary

The primary objectives of the audit were to evaluate the adequacy and effectiveness of the UT Southwestern Privacy Office's program to ensure compliance with HIPAA rules and regulations. Internal Audit evaluated the following:

- Performance of a risk assessment and development of an annual HIPAA Privacy Office work plan, ensuring adequate coverage of high risk areas and key rules and regulations.
- Progression and completion of the annual work plan.
- Monitoring of new regulation requirements and timely implementation of updates to privacy policies and procedures.
- Completion and effectiveness of the regular monitoring procedures and compliance assessment program.
- Effective maintenance and monitoring of required HIPAA employee training.
- Timely investigation and reporting of potential violations and corrective actions.

We conducted our examination according to guidelines set forth by the Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing.

Conclusion

The table below summarizes the observations and the respective disposition of these observations within the UT Southwestern internal audit risk definition and classification process. See Appendix A for Risk Rating Classifications and Definitions.

High (0)	Medium/High (1)	Medium (2)	Low (3)	Total (6)

Specific strengths identified during the audit include:

- Institutional Privacy Compliance Policies and Procedures are complete and updated timely for regulatory changes.
- Valid Risk Assessment process is in place, work plans are approved, and work plan performance is on track.
- On-site monitoring is being performed regularly in clinical and hospital areas and follow up on identified issues is performed timely.
- Online HIPAA training is appropriate and updated for regulatory changes in a timely manner.
- Procedures are in place to investigate complaints and other potential privacy violations in a timely manner and reporting on validated breaches is performed as required.
- The content of the Notice of Privacy Practices Acknowledgement is appropriate and procedures are in place to obtain the acknowledgement from all patients with limited exceptions.

Key improvement opportunities risk-ranked as medium/high and medium are summarized below:

- **HIPAA Privacy Training** – The Privacy Office monitors and reports statistics on the completion rates of required HIPAA privacy online training by employees. However, similar statistics are not currently gathered for POIs (temporary workers, interns, other non- employees) and CWRs (contingent workers). In addition, training is monitored only for new hires; but there is not a process in place to identify and follow up on existing employees who have never completed the required HIPAA privacy training.

Executive Summary

- **Research and Billing Departments** - A comprehensive monitoring program for the proper handling of PHI in research and billing offices has not been in place.

- **Identity Theft** - Procedures are not currently in place to perform automated monitoring for potential instances of medical identity theft.

Management has plans to address the issues identified in the report. These responses, along with additional details for the key improvement opportunities listed above and other lower risk observations are listed in the Detailed Observations and Action Plans Matrix (Matrix) section of this report.

We would like to thank the departments and individuals included in this audit for the courtesies extended to us and for their cooperation during our review.

Sincerely,

Valla J. Wilson

Valla Wilson, Assistant Vice President for Internal Audit

Audit Team:

Yasemin Polat, Auditor II
Kelly Iske, Manager of Internal Audit
Valla Wilson, Assistant Vice President for Internal Audit

Cc: Arnim Dontes, Executive Vice President, Business Affairs
Sharon Parsley, Assistant Vice President, Office of Compliance
Joshua Spencer, Assistant Vice President, Information Security
Pamela Bennett, Interim Privacy Officer, Office of Compliance

Detailed Observations and Action Plans Matrix

Observation	Recommendation	Management Response
Risk Rating: Medium/High ● 1. **Improve HIPAA Privacy Training Monitoring** Monitoring of required online HIPAA privacy training for all workforce members may not be adequate. Specifically: • The Privacy Office does not perform monitoring or report on the completion rates for training taken by POIs (temporary workers, interns, other non- employees) or CWRs (contingent workers). • The Privacy Office currently monitors and reports to the ECC statistics on the training completion rates by new hire employees every quarter. However, there is not a process to identify and follow up on existing employees who do not eventually complete the required training. The U.S. Department of Health and Human Services (HHS) requires covered entities to "train all workforce members on its privacy policies and procedures as necessary and appropriate for them to carry out their functions." Workforce members are defined as "employees, volunteers, trainees, and may also include other persons whose conduct is under the direct control of the entity (whether or not they are paid by the entity)." Without proper monitoring, reporting, and follow up on HIPAA privacy training for all workforce members, UT Southwestern may be out of compliance with regulations and face fines from the Office of Civil Rights.	1. Evaluate the cost benefit of system or process improvements that would allow for the determination of whether a POI or CWR meets the definition of a workforce member. 2. Implement monitoring procedures deemed necessary to evaluate compliance with workforce POIs and CWRs' HIPAA privacy training requirements. 3. Work with management and the ECC to determine the acceptable risk tolerance for HIPAA training not completed by workforce members, and the necessary level of ongoing follow up. 4. Implement additional necessary controls that are determined warranted as a result of the aforementioned risk assessment to improve HIPAA training compliance.	**Management Action Plans:** 1. Privacy Office management will collaborate with the appropriate stakeholder departments to fully implement the recommendation. 2. Privacy Office management will collaborate with stakeholder departments to implement the monitoring deemed necessary, after conclusion of the cost benefit analysis outlined in step 1. 3. Privacy Office management will collaborate with the stakeholder departments to implement the necessary follow up at the direction of the ECC and management, and report expectations to the ECC. 4. Privacy Office management will collaborate with the stakeholder departments to implement the controls determined to be appropriate as result of the preceding steps of this action plan. **Action Plan Owners:** Assistant Vice President, Office of Compliance Assistant Vice President, Information Security (to consult on technical considerations) **Target Completion Dates:** 1. October 1, 2015 2. November 1, 2015 3. January 1, 2015 4. November 1, 2015

Detailed Observations and Action Plans Matrix

Observation	Recommendation	Management Response
Risk Rating: Medium 2. **Establish Monitoring Procedures for Research and Billing Departments** A comprehensive monitoring program for the proper handling of PHI in Research and Billing offices is not in place. The Research Compliance area includes testing for appropriate HIPAA Privacy acknowledgements within their sample compliance reviews; but a comprehensive review for proper handling of PHI within Human Research studies is not yet fully designed. No monitoring of PHI handling procedures is performed for Billing offices. Without effective oversight, improper handling of PHI within Research or Billing functions may not be identified and lead to privacy breaches.	1. Implement a monitoring program for PHI used in billing departments and the physical security of PHI. Utilize self-assessment tools in order to focus on the greatest risk areas. 2. Implement a monitoring program for HIPAA Research documentation and physical security of documents. Utilize a risk stratification methodology and self-assessment tools in order to focus on the greatest risk areas.	**Management Action Plans:** 1. Privacy Office management agrees with and will fully implement the recommendation. 2. Privacy Office management agrees with and will fully implement the recommendation. **Action Plan Owners:** Interim Privacy Officer, Office of Compliance **Target Completion Dates:** 1. October 1, 2015 2. December 1, 2015

Detailed Observations and Action Plans Matrix

Observation	Recommendation	Management Response
Risk Rating: Medium 3. **Establish Monitoring for Medical Identity Theft** Procedures are not currently in place to perform automated monitoring for potential instances of medical identity theft. Potential automated reports were assessed within the last two years; but insufficient data elements were available to correlate activities which could indicate identify theft. A re-assessment of alternative monitoring reports is under consideration with the implementation of new reporting features recently introduced by the upgrade to EPIC 2014. Additionally, while clinical orientation includes instructions on the process to report suspected identify theft, there is not training specific to prevention and identification of medical identity theft. Medical identity theft can cause reputational damage for the Medical Center as well as lost revenues.	1. Evaluate and select an appropriate automated method or develop internal reporting that will help to detect potential medical identity theft encounters. 2. Expand the current level of instruction on identity theft reporting during clinical orientation to also include medical identity theft prevention and identification.	**Management Action Plans:** 1. The Privacy Office and Information Security will work with Information Resources to re-evaluate the creation of system reporting that can be used to detect potential instances of medical identify theft. 2. Privacy Office management agrees with the recommendation and will work with appropriate hospital and ambulatory services leadership to expand clinical orientation materials to include medical identity theft prevention and identification. **Action Plan Owners:** 1. Assistant Vice President, Office of Compliance Assistant Vice President, Information Security 2. Interim Privacy Officer, Officer of Compliance Assistant Vice President, Information Security **Target Completion Dates:** 1. December 1, 2015 2. December 1, 2015

Detailed Observations and Action Plans Matrix

Observation	Recommendation	Management Response
Risk Rating: Low ● 4. **Improve Monitoring of Notice of Privacy Practices Acknowledgements** The method of monitoring Privacy Practices Acknowledgement forms can be improved. Internal Audit performed data analytics on 100% of all patient visits (hospitals and clinics) in a 3 month period to confirm that the Notice of Privacy Practices (NPP) Acknowledgement form was on file as required: • Of the 70,848 completed hospital and clinic visits from January 1, 2015 to March 31, 2015, 556 (<1%) did not contain NPP acknowledgement forms on file in Epic. • A random sample of exceptions (22 of the 556) was tested to determine if the Consent to Treatment Acknowledgement form was on file instead of the NPP. Sixteen of the 22 sample items did not have evidence of the Consent to Treatment form or NPP acknowledgement form. The Privacy Office monitors compliance with Notice of Privacy Practices (NPP) and/or Consent to Treatment acknowledgements by performing sample testing during periodic on-site reviews at clinic and hospital locations. As an alternative, performing analytics similar to that performed by Internal Audit above may identify problems with privacy acknowledgement compliance in a more timely and complete manner.	1. Utilize data analytics quarterly to determine whether all departments are in compliance with the requirement to have patients sign the NPP acknowledgement form or the Consent to Treatment form.	**Management Action Plans:** 1. Privacy Office management agrees with and will fully implement the recommendation. **Action Plan Owners:** Interim Privacy Officer, Office of Compliance **Target Completion Dates:** 1. December 1, 2015

Detailed Observations and Action Plans Matrix

Observation	Recommendation	Management Response
Risk Rating: Low ● 5. **Conduct Surprise On-Site Reviews** The Privacy Office does not conduct surprise reviews as part of their regular on-site monitoring of clinical and hospital areas. On-site reviews by the Privacy Office consist of physical and technical safeguard observations, interviews with staff on policies and procedures, audits of the department's online HIPAA training completion, and audits of the department's NPP forms. These reviews are performed regularly and follow up on identified issues is performed timely. However, areas are given a one week notice by the Privacy Office prior to the on-site review, which may not provide an objective observation of the area's consistent compliance with privacy requirements. Departments may prepare for the Privacy Office visit and return to their original habits after the review is over. The Office of Civil Rights performs surprise audits to check for compliance with the HIPAA Privacy, Security, and Breach notification rules, so internal monitoring on a surprise basis would therefore be most appropriate.	1. Incorporate unannounced monitoring reviews into the on-site monitoring program.	**Management Action Plans:** 1. The Privacy Office will develop guidelines for on-site reviews that include the use of unannounced monitoring. These guidelines will be documented with the Privacy Office SOPs. **Action Plan Owners:** Interim Privacy Officer, Office of Compliance **Target Completion Dates:** 1. December 1, 2015

Detailed Observations and Action Plans Matrix

Observation	Recommendation	Management Response
Risk Rating: Low ● 6. **Develop Standard Operating Procedures** Standard operating procedures (SOPs) for the Privacy Office are not documented. Without finalized SOPs, procedures may not be consistent with management's understanding and expectations.	1. Develop standard operating policies and procedures, and finalize draft policies with management approval.	**Management Action Plans:** 1. Privacy Office management agrees with and will fully implement the recommendation. **Action Plan Owners:** Interim Privacy Officer, Office of Compliance **Target Completion Dates:** 1. December 1, 2015

As you review each observation within the Detailed Observations and Action Plans Matrix of this report, please note that we have included a color-coded depiction as to the perceived degree of risk represented by each of the observations identified during our review. The following chart is intended to provide information with respect to the applicable definitions and terms utilized as part of our risk ranking process:

	Degree of Risk and Priority of Action	
Risk Definition - The degree of risk that exists based upon the identified deficiency combined with the subsequent priority of action to be undertaken by management.	**High**	The degree of risk is unacceptable and either does or could pose a significant level of exposure to the organization. As such, immediate action is required by management in order to address the noted concern and reduce risks to the organization.
	Medium/High	The degree of risk is substantially undesirable and either does or could pose a moderate to significant level of exposure to the organization. As such, prompt action by management is essential in order to address the noted concern and reduce risks to the organization.
	Medium	The degree of risk is undesirable and either does or could pose a moderate level of exposure to the organization. As such, action is needed by management in order to address the noted concern and reduce risks to a more desirable level.
	Low	The degree of risk appears reasonable; however, opportunities exist to further reduce risks through improvement of existing policies, procedures, and/or operations. As such, action should be taken by management to address the noted concern and reduce risks to the organization.

It is important to note that considerable professional judgment is required in determining the overall ratings presented on the subsequent pages of this report. Accordingly, others could evaluate the results differently and draw different conclusions.

It is also important to note that this report provides management with information about the condition of risks and internal controls at one point in time. Future changes in environmental factors and actions by personnel may significantly and adversely impact these risks and controls in ways that this report did not and cannot anticipate.