INTERNAL AUDIT
UT HEALTH SCIENCE CENTER®
SAN ANTONIO

AUDIT REPORT

TO: Gail Madison-Brown, Chief Compliance Officer, Office of Regulatory Affairs and Compliance

FROM: Angela D'Anna, Chief Audit Executive, Internal Audit and Consulting Services

DATE: August 31, 2016

SUBJECT: HIPAA Privacy Rule (16-23)

EXECUTIVE SUMMARY

Internal Audit and Consulting Services has reviewed compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule at The University of Texas Health Science Center at San Antonio (Health Science Center). The scope included the period of September 1, 2015 through June 30, 2016. The primary objective of this review was to evaluate the Health Science Center's alignment with the HIPAA Privacy Rule.

We noted that controls surrounding HIPAA training and patient acknowledgement of the Notice of Privacy Practices (NPP) needed to be strengthened. An additional opportunity for improvement was noted related to ensuring that the most current NPP was available at all patient care locations. These issues require immediate attention.

The audit issues were ranked according to the University of Texas System Administration audit ranking guidelines. This audit identified no issues considered priority to the institution. Please see the Appendix for ranking definitions. Attached is the detailed report.

DETAILED AUDIT REPORT

Internal Audit and Consulting Services has reviewed compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule at The University of Texas Health Science Center at San Antonio (Health Science Center). The Health Science Center serves patients in clinics and health care facilities across San Antonio, Laredo and the Rio Grande Valley. This includes the clinical practices of UT Medicine, UT Dentistry and the School of Nursing Employee Health and Wellness Clinic.

PURPOSE AND SCOPE

The purpose of this review was to evaluate the Health Science Center's alignment with the HIPAA Privacy Rule.

The primary objectives of the audit were as follows:

- Determine whether HIPAA Privacy policies and procedures were in place and communicated to employees.
- Ascertain whether employees were provided appropriate HIPAA training and whether the training was documented.
- Determine whether the Notice of Privacy Practices (NPP) was posted at clinical practices and acknowledged by new patients.
- Evaluate whether employees who interact with patients took appropriate actions to safeguard protected health information (PHI).
- Evaluate the process in place for documenting the release of PHI to certain agencies/parties so that an accounting of disclosures can be prepared upon request.
- Evaluate whether Business Associate Agreements included elements required by the HIPAA Privacy Rules and Health Science Center policy.
- Assess the process in place for patients to access and amend their records.

The scope included the period of September 1, 2015 through June 30, 2016. We conducted walkthroughs at the following Health Science Center facilities:

- Medical Arts and Research Center
- Cancer Therapy and Research Center
- UT Medicine Medical Drive Primary Care
- University Plaza
- UT Medicine Westover Hills Primary Care
- UT Medicine One Oak Hills Place
- Texas Diabetes Institute
- UT Dentistry clinical practices
- Employee Health and Wellness Clinic

BACKGROUND

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule set national standards for the protection of health information for convered entities and became effective on April 14, 2003. The Department of Health and Human Services Office for Civil Rights enforces the HIPAA Privacy Rule and completes both desk reviews and onsite audits as part of enforcement.

The Health Science Center Office of Regulatory Affairs and Compliance (Compliance) is responsible for the compliance program including HIPAA Privacy. This includes providing education, training, and guidance to all faculty and staff in order to prevent accidental or intentional non-compliance with the HIPAA Privacy Rule. The Health Science Center Handbook of Operating Procedures (HOP) includes patient privacy policies that cover oversight, uses and disclosures of PHI, patients' rights, and training. Compliance is responsible for monitoring activities to detect any violations of policy and procedure, including discipline for any faculty or staff involved in non-compliant behavior. In addition, Compliance

investigates patient complaints and breaches of health information including providing notifications to patients.

RESULTS

Compliance with the HIPAA Privacy Rule needs to be strengthened. Specifically, the opportunities for improvement related to procedures to ensure HIPAA training is completed by all required individuals, that clinical practices consistently obtain the acknowledgement of the NPP from the patients and that the most current NPP is available in all patient care locations. These issues require immediate attention.

Attached are the audit recommendations, management action plans, responsible parties, and anticipated completion dates. These matters are offered for management's consideration in the spirit of continuously improving processes and reducing risks in the organization.

* * * * * *

This audit was performed by Cynthia Scheick, Senior Internal Auditor with the assistance of other members of the Internal Audit and Consulting Services Department. The audit was conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing* as promulgated by the Institute of Internal Auditors.

cc: Michael E. Black, Senior Executive Vice President and Chief Operating Officer
Eileen T. Breslin, Ph.D., Dean, School of Nursing
William W. Dodge, D.D.S., Dean, School of Dentistry
Kristie Foster, Director, Practice Operations, UT Medicine CTRC
Francisco González-Scarano, M.D., Dean, School of Medicine and Executive Vice President for Medical Affairs
Gary F. Guest, D.D.S., Associate Dean for Patient Care, School of Dentistry
William L. Henrich, M.D., President
Jeanette J. Hernandez, Director, Practice Operations, UT Medicine
Charles Hoag, Clinic Manager, School of Nursing
Andrea Marks, Vice President and Chief Financial Officer
Tim Marlow, Director, Practice Operations, UT Medicine
Casey Peterson, Senior Director, Practice Operations, UT Medicine
Carlos Rosende, M.D., Clinical Affairs and Executive Director, UT Medicine

HIPAA Training

Opportunity for Improvement:

Issue Ranking - High

During our review, we noted the following:

- The report used to produce the HIPAA mandatory training list did not capture all new employees due to an error. We selected 831 active employees hired between September 1, 2015 and June 30, 2016 and determined that 69 (8%) were not listed in the report used by Compliance and thus were not assigned HIPAA training.

- The monitoring performed by Compliance to identify individuals who had not taken the initial or recurring training entailed using a report (called the expired training report) that did not list residents. As a result, 89 residents had not taken the mandatory training. The report also showed that 20 employees and 21 students had not completed the training.

The HIPAA Privacy Rule §164.530(b) requires that training be provided within a reasonable period of time after an individual joins the entity and that training documentation be maintained by the entity. The Handbook of Operating Procedures (HOP) Policy 11.4.1, *Education and Training on Patient Privacy*, requires all new employees, faculty, students, or residents to take training within 30 days of hire and every two years thereafter.

Untrained staff may inadvertently disclose PHI inappropriately putting the institution at risk for a breach of patient confidentiality.

Recommendation:

Compliance should request that the report used to produce the HIPAA mandatory training list be corrected to include all new hires. Furthermore, Compliance should collaborate with the Knowledge Center to automate the assignment of HIPAA training to employees. Also, the report used by Compliance to monitor HIPAA training should include the residents.

Management's Action Plan:

Responsible Party(s): Gail Madison-Brown

Estimated Completion Date(s): September 1, 2016

Compliance has worked with Human Resources to identify and ensure that all employees required to take HIPAA training are captured and assigned the training. Beginning September 1, 2016, all residents will be assigned and required to take HIPAA training, as required by HOP policy. We will continue to work with the Knowledge Center regarding automation potentials; however, recent attempts were not able to provide an automated solution.

School of Medicine – UT Medicine

Opportunity for Improvement:

Issue Ranking - High

Established procedures were not always followed to ensure the Notice of Privacy Practices (NPP) acknowledgement was signed by new patients at all UT Medicine Clinics. We reviewed 60 new patient records and determined that 11 (18%) did not contain the NPP acknowledgement. Specifically the following clinics did not consistently obtain the acknowledgement:

- UHC Ophthalmology - 3 of 4 (75%) new patients.
- Health Science Center Psychiatry - 4 of 8 (50%) new patients.

In addition, certain clinics did not have the most current NPP posted to be available if requested by patients. Specifically, we visited 14 clinical practices and noted:

- Eight (57%) practices did not have the NPP posted at the clinic location.
- Two (14%) practices did have the most current NPP available for patients.

HIPAA Privacy Rule §164.520(c) (2), *Provisions of Notice - Certain Covered Health Care Providers*, and Handbook of Operating Procedures (HOP) Policy 11.3.4 *Notice of Privacy Practices* requires the NPP to be provided no later than the first date of service and that staff make a good faith effort to obtain a written acknowledgement from the patient. The rule and HOP policy also requires the NPP to be posted in a clear and prominent location and be available for patients.

Recommendation:

UT Medicine should follow-up with the specific clinics to train staff in the registration procedures that ensure the NPP acknowledgement is obtained from patients. Staff should also obtain the NPP acknowledgement for the patient exceptions noted in this review upon their next visit.

Management's Action Plan:

Responsible Party(s): Casey Peterson
Tim Marlow
Jeanette J. Hernandez
Kristie Foster
Gail Madison-Brown

Estimated Completion Date: September 30, 2016

Clinic managers will ensure staff receive training and follow the procedures for patient registration including the acknowledgement of the NPP. Staff will ensure the NPP acknowledgement is obtained from patients noted as exceptions if possible. UT Medicine will coordinate with Compliance to ensure practices have posted and available the most current notice of privacy practices.

School of Nursing – Employee Wellness Clinic

Opportunity for Improvement:

Issue Ranking - High

Established procedures were not always followed to ensure the Notice of Privacy Practices (NPP) acknowledgement was signed by new patients at the Employee Health and Wellness Clinic. We selected 10 new patients and determined that five (50%) did not have the NPP acknowledgement on file. Furthermore, the most current NPP was not posted at the clinic to be available if requested by patients.

HIPAA Privacy Rule §164.520(c) (2), *Provisions of Notice - Certain Covered Health Care Providers*, and Handbook of Operating Procedures (HOP) Policy 11.3.4 *Notice of Privacy Practices* requires the NPP to be provided no later than the first date of service and that staff make a good faith effort to obtain a written acknowledgement from the patient. The rule and HOP policy also requires the NPP to be posted in a clear and prominent location and be available for patients.

In addition, staff at the clinic had not received additional HIPAA training specific to clinic operations as required by Health Science Center policy. HOP policy 11.4.1 *Education and Training on Patient Privacy*, states departments and clinics are responsible for providing additional one-on-one training to staff who interact with patients.

Untrained staff may inadvertently disclose PHI inappropriately putting the institution at risk for a breach of patient confidentiality.

Recommendation:

The Clinic Manager for the Employee Wellness Clinic should provide specific HIPAA training to staff including the registration procedures that ensure the NPP acknowledgement is obtained from patients. In addition, the clinic staff should ensure the NPP acknowledgement is included in the file for all patients by verifying this at each patient visit. Staff should also obtain the NPP acknowledgement for the patient exceptions noted is this review upon their next visit.

Management's Action Plan:

Responsible Party: Charles Hoag

Estimated Completion Date: September 1, 2016

HIPPA Training for Employee Health and Wellness Clinic staff was provided by the Office of Regulatory Affairs and Compliance on August 29th, 2016. Staff will validate the NPP acknowledgement is on file for each patient during the registration process. Copies of the current NPP in trifold format were placed in the lobby area of the clinic and are available upon request.

School of Dentistry – UT Dentistry

Opportunity for Improvement:

Issue Ranking - Low

Certain clinical practices did not have the most current Notice of Privacy Practices (NPP). Of the eight UT Dentistry practices visited, four (50%) did not have the most current NPP available to provide to patients upon request.

HIPAA Privacy Rule §164.520(c)(2), Provisions of Notice - Certain Covered Health Care Providers, and the Health Science Center Handbook of Operating Procedures (HOP) Policy 11.3.4 *Notice of Privacy Practices*, requires the NPP be available for patients to request a copy.

Also, staff at UT Dentistry had not received additional HIPAA training specific to clinic operations as required by Health Science Center policy. HOP policy 11.4.1 *Education and Training on Patient Privacy*, states departments and clinics are responsible for providing additional one-on-one training with staff who interact with patients.

Recommendation:

UT Dentistry should provide specific HIPAA training to clinic staff. Additionally, UT Dentistry should ensure all clinical practices have the most current NPP available for patients.

Management's Action Plan:

Responsible Party: Dr. Gary Guest

Estimated Completion Date: January 1, 2017

UT Dentistry practices were all provided with the current NPP and any old versions of the NPP were removed effective August 31, 2016. The Office of Regulatory Affairs and Compliance (Compliance) will ensure any updates to the NPP are distributed to the appropriate leadership including, Administrators, Directors, and Clinic Managers as appropriate. We are also working with UT Medicine and Compliance to develop content for additional HIPAA training specific to clinic operations.

Appendix - Audit Issue Ranking Definitions

The audit issues were ranked according to the following University of Texas System Administration issue ranking guidelines:

- ***Priority*** – A priority finding is defined as an issue identified by internal audit that, if not addressed immediately, has a high probability to directly impact achievement of a strategic or important operational objective of the Health Science Center or the UT System as a whole.

- ***High*** – A finding identified by internal audit that is considered to have a medium to high probability of adverse effects to the Health Science Center either as a whole or to a significant college/school/unit level.

- ***Medium*** – A finding identified by internal audit that is considered to have a low to medium probability of adverse effects to the Health Science Center either as a whole or to a college/ school/unit level.

- ***Low*** – A finding identified by internal audit that is considered to have minimal probability of adverse effects to the Health Science Center either as a whole or to a college/ school/unit level.