The University of Texas at Austin
Institutional Audit Committee

Mr. William O’Hara, External Member, Chair
Dr. Gregory Fenves, President
Dr. Judith Langlois, Executive Vice President and Provost, ad interim
Dr. Patricia Clubb, Vice President for University Operations
Ms. Patricia Ohlendorf, Vice President for Legal Affairs
Dr. Daniel Jaffe, Vice President for Research
Dr. Gage Paine, Vice President for Student Affairs
Mr. Darrell Bazzell, Senior Vice President and Chief Financial Officer
Ms. Mary Knight, CPA, Associate Vice President for Finance
Mr. Paul Liebman, Chief Compliance Officer, University Compliance Services
Mr. Cameron Beasley, University Information Security Officer
Ms. Christine A. Plonsky, Women’s Athletics Director and Executive Senior Associate Athletics Director for External Services
Mr. Tom Carter, External Member
Ms. Lynn Utter, External Member
Ms. Susan Whittaker, External Member
Mr. Michael Vandervort, Chief Audit Executive, Office of Internal Audits
Mr. J. Michael Peppers, Chief Audit Executive, University of Texas System Audit Office

The University of Texas at Austin
Office of Internal Audits

Chief Audit Executive: Michael Vandervort, CPA
Associate Director: Jeff Treichel, CPA
Assistant Directors: Angela McCarter, CIA, CRMA
*Chris Taylor, CIA, CISA
Audit Manager: *Brandon Morales, CISA, CGAP
Auditor III: Michael Hammond, CIA, CISA, CFE
Cynthia Martin-Hajmasy, CPA
Ashley Oheim, CPA
Auditor II: Bobby Castillo
Stephanie Grayson
Kerri Jordan
Miranda Pruett, CFE
Auditor I: Jason Boone
IT Auditor: Tiffany Yanagawa
Mike McIntosh
* denotes project members

This report has been distributed to Internal Audit Committee members, the Legislative Budget Board, the State Auditor’s Office, the Sunset Advisory Commission, the Governor’s Office of Budget and Planning, and The University of Texas System Audit Office for distribution to the Audit, Compliance, and Management Review Committee of the Board of Regents.

Health Insurance Portability and Accountability Act, Security Rule – Athletics Sports Medicine
Project Number: 15.311
June 8, 2016

President Gregory L. Fenves  
The University of Texas at Austin  
Office of the President  
P.O. Box T  
Austin, Texas  78713

Dear President Fenves,

We have completed our audit for compliance with the Health Insurance Portability and Accountability Act (HIPAA), Security Rule at Athletics Sports Medicine (ASM). Our scope included applicable IT controls within ASM.

Based on the audit procedures performed, we conclude that ASM is generally in compliance with HIPAA guidelines. Our audit report provides detailed observations for each area under review. Suggestions are offered throughout the report for improvement in the existing control structure.

We appreciate the cooperation and assistance of ASM throughout the audit and hope that the information presented herein is beneficial.

Sincerely,

Michael W. Vandervort, CPA  
Chief Audit Executive

cc:  Institutional Audit Committee Members  
Mr. Allen Hardin, Senior Associate Athletics Director, Intercollegiate Athletics  
Ms. Patricia Ohlendorf, Vice President for Legal Affairs  
Mr. Jeff Treichel, Associate Director, Office of Internal Audits
# Table of Contents

Executive Summary ................................................................. 1

Background .............................................................................. 2

Scope, Objectives, and Procedures .......................................... 2

Audit Results ........................................................................... 3

Conclusion ............................................................................... 5

Appendix ................................................................................. 6
EXECUTIVE SUMMARY

Conclusion
Based on the audit procedures performed, it appears that Athletics Sports Medicine (ASM) is generally in compliance with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule guidelines. Two recommendations were made regarding contingency planning and review of information system activity logs. Management agreed with the recommendations and is taking corrective actions.

Summary of Recommendations
Internal Audits identified two notable issues which led to the following recommendations:

- Management should ensure that a comprehensive contingency plan is documented and tested regularly. (Audit Issue Ranking: High)
- Management should implement procedures to regularly review records of information system activity related to HIPAA data. (Audit Issue Ranking: High)

No additional recommendations were necessary.

Audit Scope and Objective
The scope of this audit included applicable information technology controls within ASM. The specific audit objective was to determine whether ASM is in compliance with HIPAA Security Rule guidelines.

Background Summary
Title II of HIPAA defines policies, procedures, and guidelines for maintaining the privacy and security of individually identifiable health information. The Department of Health and Human Services’ Administrative Simplification of HIPAA’s Security Rule specifically relates to electronic protected health information and requires appropriate security standards to ensure the confidentiality, integrity, and security of electronic protected health information.

ASM is responsible for ensuring the health and safety of every student-athlete in The University of Texas at Austin’s 20 intercollegiate sports programs. Trainers, physical therapists, and sports medicine physicians use state-of-the-art technology to aid in injury and illness prevention and diagnostic, therapeutic, and rehabilitative services. As part of its operations, ASM works with electronic protected health information.

This audit was conducted as part of the Fiscal Year 2015 Audit Plan, based on risk identified in the annual risk assessment.


**BACKGROUND**

Title II of the Health Insurance Portability and Accountability Act (HIPAA) defines policies, procedures, and guidelines for maintaining the privacy and security of individually identifiable health information. The Department of Health and Human Services provides an Administrative Simplification of Title II and divides its requirements into the following areas:

- **The Privacy Rule** – requires appropriate safeguards to protect the privacy of personal health information and regulates the use and disclosure of this information;
- **The Security Rule** – establishes standards to protect individuals’ electronic personal health information that is created, received, used, or maintained by covered entities;
- **The Breach Notification Rule** – requires notifications following a breach of unsecured protected health information;
- **The Transactions and Code Sets Standards** – standardizes health care transactions;
- **Identifier Standards for Employers and Providers** – require the use of standardized identification numbers; and
- **The Enforcement Rule** – relates to compliance and investigations and sets civil monetary penalties for HIPAA violations.

The focus of this audit is the Administrative Simplification of the Security Rule. The Security Rule specifically relates to electronic protected health information and requires appropriate administrative, physical, and technical safeguards, as well as organizational requirements, policies and procedures, and documentation to ensure the confidentiality, integrity, and security of electronic protected health information.

Athletics Sports Medicine (ASM) is responsible for ensuring the health and safety of every student-athlete in The University of Texas at Austin’s 20 intercollegiate sports programs. Trainers, physical therapists, and sports medicine physicians use state-of-the-art technology to aid in injury and illness prevention and diagnostic, therapeutic, and rehabilitative services. As part of its operations, ASM works with electronic protected health information.

**SCOPE, OBJECTIVES, AND PROCEDURES**

The scope of this audit included applicable IT controls within ASM. The specific audit objective was to determine whether ASM is in compliance with the HIPAA Security Rule guidelines.

To achieve this objective, we:

- Gained an understanding of ASM’s IT environment and the IT controls in place for accessing and storing electronic protected health information;
• Reviewed current documented policies and procedures at ASM related to HIPAA Security Rule guidelines;
• Reviewed the results of network vulnerability scans; and
• Tested a sample of computers within ASM.

This audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* and with *Government Auditing Standards*.

**AUDIT RESULTS**

The HIPAA Security Rule consists of required and addressable implementation specifications in the following areas:
- Administrative Safeguards,
- Physical Safeguards,
- Technical Safeguards,
- Organizational Requirements, and
- Policies and Procedures and Documentation Requirements.

ASM does not house electronic HIPAA data, instead opting to use the third party - Workflow to store and access their HIPAA data.

The following two recommendations were made in the area of Administrative Safeguards. Each issue has been ranked according to the University of Texas System Administration (UT System) Audit Issue Ranking guidelines. Please see the Appendix for ranking definitions.

**Administrative Safeguards – Contingency Plan**

**Audit Issue Ranking: High**

The Intercollegiate Athletics contingency plan is not routinely tested and does not include instructions pointing to the Workflow Disaster Recovery Plan (DRP) which covers Athletics Sports Medicine HIPAA data. Without a documented and tested contingency plan in place that includes the program housing Athletics Sports Medicine electronic HIPAA data, operators, technicians, and management may not be able to adequately recover and continue operations of critical systems and data in the event of a disaster.

*HIPAA Administrative Simplification Regulation Text*\(^1\) part 164.308 a.7 states:
- Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

---

\(^1\) HIPAA Administrative Simplification Regulation Text -
- Implement procedures for periodic testing and revision of contingency plans.

**Recommendation 1:** Management should ensure that a comprehensive contingency plan is in place including information pointing to the Workflow DRP which covers Athletics Sports Medicine electronic HIPAA data. This contingency plan should be documented within The University of Texas at Austin’s UT Ready Continuity Planning tool and should be tested at least annually.

**Management’s Response and Corrective Action Plan:** Emergency Access Procedure: Sports Medicine Policy & Procedure Manual serves as Contingency Plan. These procedures will be acknowledged in the Disaster Preparedness Plan and will be documented within UT Ready Continuity Planning tool. The procedures will be tested annually.

Responsible Person: Phillip Jaeger, Athletics IT Services

Planned Implementation Date: July 1, 2016

**Post Audit Review:** Internal Audits will perform follow-up activities in the first quarter of fiscal year 2017.

---

**Administrative Safeguards – Information System Activity Records Review**

**Audit Issue Ranking:** High

Athletics Sports Medicine has the capability to log information system activity and run reports but there is no routine schedule for reviewing the logs or reports. Without regularly reviewing records of information system activity, there is an increased risk of loss or misuse of HIPAA data.

*HIPAA Administrative Simplification Regulation Text*\(^2\) part 164.308 a.1.ii.D states, Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

**Recommendation 2:** Management should implement procedures to regularly review records of information system activity related to HIPAA data. This review should be documented.

**Management’s Response and Corrective Action Plan:** Procedure will be established to review User Authentication Successes and User Authentication Failures and document review of such. Reports are viewable but not exportable.

---

\(^2\) HIPAA Administrative Simplification Regulation Text -
Athletics will request from vendor that creation of exportable reports be established.

**Responsible Person:** LaQuinta Pollard, Athletics Sports Medicine

**Planned Implementation Date:** July 1, 2016

**Post Audit Review:** Internal Audits will perform follow-up activities in the first quarter of fiscal year 2017.

---

**CONCLUSION**

Based on the audit procedures performed, it appears that ASM is generally in compliance with the HIPAA Security Rule guidelines. Two recommendations were made regarding contingency planning and the review of information system activity logs. Management agreed with the recommendations and is taking corrective actions.

In accordance with directives from The University of Texas System Board of Regents, the Office of Internal Audits will perform follow-up procedures to confirm that audit recommendations have been implemented.
Audit issues are ranked according to the following definitions, consistent with UT System Audit Office guidance. These determinations are based on overall risk to UT System, UT Austin, and/or the individual college/school/unit if the issues are left uncorrected. These audit issues and rankings are reported to UT System directly.

- **Priority** – A Priority Issue is an issue that, if not addressed immediately, has a high probability to directly impact achievement of a strategic or important operational objective of UT Austin or the UT System as a whole.
- **High** – An issue that is considered to have a medium to high probability of adverse effects to UT Austin either as a whole or to a significant college/school/unit level.
- **Medium** – An issue that is considered to have a low to medium probability of adverse effects to UT Austin either as a whole or to a college/school/unit level.
- **Low** – An issue that is considered to have minimal probability of adverse effects to UT Austin either as a whole or to a college/school/unit level. Issues with a ranking of “Low” are reported verbally to the unit and are not included in the final report.