

17-211 Patient Privacy System (FairWarning)

We have completed our audit of the Patient Privacy System (FairWarning). This audit was performed at the request of the UTHealth Audit Committee and was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing*.

BACKGROUND

FairWarning (FW) is a security application that provides data protection and governance for electronic health records. FW detects inappropriate access to electronic health records and alerts on patient privacy violations. At UTHealth, IT Security administers the FW application and has configured alerting for Allscripts, axiUm, GE Centricity Business (GECB), Sunrise Clinical Manager (SCM), and the School of Biomedical Informatics (SBMI) Chronic Disease Registry.

OBJECTIVES

The objective of this audit was to determine whether controls around patient privacy and the FairWarning application are adequate and functioning as intended.

SCOPE PERIOD

The scope period was September 1, 2017 to December 31, 2017.

METHODOLOGY

The following procedures were performed:

- Selected a sample of applications monitored by FW, verified policies and procedures were in place around the investigation/resolution process, and assessed adequacy of controls. For each sampled application, selected a sample of FW alerts, assessed adequacy of resolutions, and verified final resolutions were documented in FW.
- For a sample of applications, verified end user alerting preferences agreed to the alert configuration in FW.
- Selected a sample of FW alerts outstanding for more than 30 days and verified reminders were sent to end users by IT Security.
- Verified policies and procedures are in place for the administration of access to FW. Obtained the current user access listing, selected a sample of users, and verified access was properly reviewed and approved. Using the current user access listing, verified user access was appropriate based on job titles/responsibilities. Additionally, verified a regular access review was conducted by the system owner or their designee.

AUDIT RESULTS

A&AS identified the following areas for improvement:

- There are no IT Security policies and procedures around the FW application.
- A regular review of FW access is not conducted by the system owner or their designee.

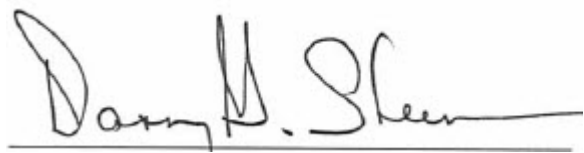
17-211 Patient Privacy System (FairWarning)

- Approval of access to FW is not formally documented.
- Resolution of alerts is not consistently documented in FW.
- Applicable parties are not consistently notified of possible abuses of employee access to medical records.

NUMBER OF PRIORITY & HIGH FINDINGS REPORTED TO UT SYSTEM

None

We would like to thank the staff and management within the IT Security, UT Physicians Clinical Information Technology, and Harris County Psychiatric Center (HCPC) who assisted us during our review.



Daniel G. Sherman, MBA, CPA, CIA
Assistant Vice President

MAPPING TO FY 2017 RISK ASSESSMENT

Risk (Rating)	R.16 Medical records are inappropriately accessed by employees.
----------------------	---

DATA ANALYTICS UTILIZED

Data Analytic #1	N/A
-------------------------	-----

AUDITING & ADVISORY SERVICES ENGAGEMENT TEAM

Assistant Vice President	Daniel G. Sherman, MBA, CPA, CIA
Audit Manager	Brook Syers, CPA, CIA, CFE, CISA
Auditor Assigned	Lieu Tran, CISA
End of Fieldwork Date	March 21, 2018
Issue Date	May 21, 2018

Copies to:

Audit Committee
Eric Fernette
Dr. James Griffiths
William Lemaistre
Rick Miller

17-211 Patient Privacy System (FairWarning)

Amar Yousif
Melissa Pifko
Christina Solis

17-211 Patient Privacy System (FairWarning)

<p>Issue #1</p>	<p>Section 164.308(a)(1)(i) Administrative Safeguards of the HIPAA Security Rule requires the implementation of policies and procedures to prevent, detect, contain, and correct security violations.</p> <p>Section 6.2.6 of the ITPOL-004 Access Control Policy states: “Owners or their designees must review access lists regularly to ensure access privileges are appropriate. Timeframe for access list review should be established based on documented risk management decisions.”</p> <p>POLICIES & PROCEDURES</p> <p>A&AS noted no IT Security policies and procedures around the FW application, including the processes governing access administration and documentation of alert resolutions.</p> <p>ACCESS REVIEWS</p> <p>Additionally, we noted a regular access review of FW is not conducted by the system owner or their designee.</p> <p>ACCESS APPROVALS</p> <p>A&AS obtained the FW user access listing and selected a random sample of 5 users to verify access was appropriate and properly approved. For 5 of 5 (100%) users in our sample, we noted no formal approval of access.</p> <p>ALERT RESOLUTION</p> <p>A&AS selected a sample of 18 FW alerts from the Allscripts application and obtained evidence of resolution. For 15 of 18 (83%) alerts, the final resolution was not recorded in FW. Five of the alerts were determined to be erroneous (“false positives”) by the Medical Records staff. IT Security informed us false positives should be documented as such in FW so alert criteria can be further refined.</p>
<p>Recommendation #1</p>	<p>We recommend IT Security management perform the following:</p> <ul style="list-style-type: none"> • Develop and implement policies and procedures around the FW application, including processes governing access administration and documentation of alert resolution. • Develop and implement a process to ensure a regular access review of FW is conducted by the system owner or their designee.
<p>Rating</p>	<p>Medium</p>
<p>Management Response</p>	<p>IT Security agrees with the recommendation and will:</p> <ul style="list-style-type: none"> • Explore augmenting existing IT Security policies/processes/procedures with updated information as it pertains to FW.

17-211 Patient Privacy System (FairWarning)

	<p>If needed, we will develop and implement internal procedures around the FW application governing access, administration, and a feedback mechanism from our FW users regarding issues affecting alert resolutions.</p> <ul style="list-style-type: none">• Ensure a regular access review of FW is conducted by the system owner or their designee.
Responsible Party	Amar Yousif, CISO
Implementation Date	October 31, 2018

17-211 Patient Privacy System (FairWarning)

<p>Issue #2</p>	<p>UT Physician’s <i>Auditing Employee Access to EMR</i> procedure states:</p> <p>“The FairWarning application runs and creates reports of possible employee access violations. Each possible violation creates an alert and notifies the Medical Records Department for further investigation.”</p> <p>The Medical Records staff is required to email a <i>Notice of Possible Abuse of Employee Access to Medical Records</i> letter (Notification Letter) to Human Resources and the employee’s administrator with a brief narrative describing the auditor’s findings if the areas accessed are not within the scope of the employee’s role. The Medical Records staff will update their internal Access Violation Log of the resolution.</p> <p>Additionally, the Senior Legal and Privacy Officer informed us they should also be notified of such cases.</p> <p>A&AS selected a sample of 18 FW alerts from the Allscripts application and verified a Notification Letter was sent to the applicable parties. Of the 18 FW alerts in our sample, we noted the following issue:</p> <ul style="list-style-type: none"> • For 10 of 18 (56%) alerts, Notification Letters were not sent to the applicable parties (Human Resources, employee’s administrator, and/or Senior Legal and Privacy Officer).
<p>Recommendation #2</p>	<p>We recommend management review the current policy and procedure related to potential access violations/Notification Letters and update each accordingly.</p>
<p>Rating</p>	<p>Medium</p>
<p>Management Response</p>	<p>We will review the current policy and procedure related to potential access violations/Notification Letters and update each based on the results of the review.</p>
<p>Responsible Party</p>	<p>Christina Solis, Senior Legal and Privacy Officer</p>
<p>Implementation Date</p>	<p>November 1, 2018</p>