UNIVERSITY OF CALIFORNIA, SAN FRANCISCO
AUDIT AND ADVISORY SERVICES

OCR Readiness Review – Phase II
Project #15-024

January 2015

University of California
San Francisco

UCSF

Audit and Advisory Services

January 26, 2015

Deborah Yano Fong
Chief Privacy Officer
Privacy Office

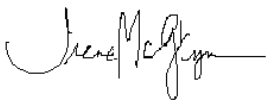
SUBJECT: OCR Readiness Review – Phase II

As a planned internal audit for Fiscal Year 2015, Audit and Advisory Services ("AAS") conducted a review of OCR Readiness. Our services were performed in accordance with the applicable International Standards for the Professional Practice of Internal Auditing as prescribed by the Institute of Internal Auditors (the "IIA Standards").

Our preliminary draft report was provided to department management and the Privacy Office in December 2014. Management provided us with their final comments and responses to our observations in January 2015. The observations and corrective actions have been discussed and agreed upon with department management and it is management's responsibility to implement the corrective actions stated in the report. In accordance with the University of California audit policy, AAS will periodically follow up to confirm that the agreed upon management corrective actions are completed within the dates specified in the final report.

This report is intended solely for the information and internal use of UCSF management and the Ethics, Compliance and Audit Board, and is not intended to be and should not be used by any other person or entity.

Sincerely,



Irene McGlynn
Director
UCSF Audit and Advisory Service

OCR Readiness Review – Phase II
Audit Services Project #15-024

MANAGEMENT SUMMARY

As a planned audit for Fiscal Year 2015, Audit and Advisory Services conducted a review of UCSF's compliance with the Health Insurance Portability and Accountability Act of 1996 Privacy Rule. The purpose of this review was to evaluate and assess the adequacy of the procedures and processes for safeguarding protected health information. The review was focused on the following areas: Breach Notifications, Self-Pay Restrictions, and Accounting of Disclosures. The audit protocol released by the Office of Civil Rights was used in determining compliance with HIPAA Privacy regulations.

Procedures performed as part of the review included interviews with departmental management and personnel; review of relevant policies and procedures; assessment of processes; and sample testing of transactions and activities.

The scope of the review covered transactions and activities for the 12 month period ending September 2014 at UCSF Medical Center, School of Medicine, School of Dentistry, Langley Porter Psychiatric Hospital and Clinics, and the Proctor Foundation.

Based on work performed, all locations reviewed generally comply with breach notifications and self-pay restrictions. The incident handling process within the Privacy Office is thorough, ensuring that appropriate investigations are conducted in response to incidents and that patients and external agencies are notified in a timely manner when necessary. The processes for restricting disclosures for self-pay patients at all locations are sufficient for ensuring that self-pay restrictions are handled correctly.

Opportunities for improvement exist in the areas of updating policies for accountings of disclosures and self-pay restrictions and methods for documenting and reporting disclosures to assure that they are fully captured and accounted for.

Additional information regarding the observations is detailed in the body of the report.

OCR Readiness Review – Phase II
Audit Services Project #15-024

TABLE OF CONTENTS

I. BACKGROUND

As a planned audit for Fiscal Year 2015, Audit and Advisory Services (AAS) conducted a Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule review to assess the adequacy of the procedures and processes for safeguarding protected health information (PHI) and meeting HIPAA regulations.

HIPAA required the creation of The Privacy Rule for identifiable health information. The resultant Privacy Rule took effect on April 14, 2003, and was updated in the Final Omnibus Rule as part of the American Recovery and Reinvestment Act (ARRA) of 2009. The update incorporated provisions from the Health Information Technology for Economic and Clinical Health (HITECH) Act and the Genetic Information Nondiscrimination Act (GINA) and became effective in March 2013. Organizations needed to be in compliance by September 24, 2013. The Privacy Rule and Final Omnibus Rule imposed a number of obligations on covered entities regarding the manner in which they use and disclose PHI and provided certain rights to patients related to uses and disclosures of their PHI.

OCR commenced Phase 1 audits of covered entities and Business Associates (BAs) in 2012 to evaluate compliance with regulations, identify best practices, uncover risk areas, and evaluate the audit protocol developed to test compliance with the Final Omnibus Rule. Phase 2 audits were expected to be conducted in 2014 - 2015; however, OCR has since announced a delay.

Risks of non-compliance with HIPAA can result in civil penalties, including fines[1] or the need to comply with a resolution agreement[2] and a corresponding payment amount. Additionally, there is reputational risk for the University if PHI is not used appropriately and adequately protected.

UCSF is a health care component of the University of California (UC). A variety of departments at UCSF and associated locations are involved in disclosure documentation and self-pay restriction processes. The custodian of medical records for UCSF is Health Information Management Services (HIMS), who receives requests for and provides the AODs. All locations reviewed go through HIMS for AODs except LPPI, who process their own AOD requests. Primary policies for AODs, breach notification, and self-pay restrictions for each location are:

- UCSF Medical Center – 5.02.01 Confidentiality, Access, Use, and Disclosure of Protected Health Information and Patient Privacy, HIMS Accounting of Disclosures Request Procedures
- School of Dentistry – Laboratory and Clinics Policies and Procedures Manual
- School of Medicine – 200-30 Privacy Investigation Policy
- LPPI – 324 Accounting for Disclosures of Protected Health Information
- Proctor Foundation - Health Information Management and Disclosure Procedures

[1] The maximum penalty for HIPAA violations is $50,000 per violation, with an annual maximum of $1.5 million for all violations of an identical provision.

[2] A resolution agreement is a contract signed by HHS and a covered entity in which the covered entity agrees to perform certain obligations (e.g., staff training) and make reports to HHS, generally for a period of three years. During this period, HHS monitors the covered entity's compliance with its obligations.

Oversight for HIPAA Compliance at UCSF resides with the Privacy Compliance Steering Committee, comprised of senior leaders from across UCSF. It functions as an approving body and a communication link to the respective areas, schools, and departments at UCSF. It also supports the mandated responsibility to keep UCSF's senior leaders informed of the organization's compliance progress and status related to these regulations.

II. AUDIT PURPOSE AND SCOPE

The purpose of this review was to evaluate UCSF policies, procedures, and processes established both centrally and at department level against selected program modules of the OCR audit protocol to ensure compliance with the new HIPAA Privacy requirements.

AAS conducted a Phase I of this review in Fiscal Year 2014[3], covering 33 categories within the Uses and Disclosures section of the OCR Audit Protocol and four categories within the Notice of Privacy Practices section. The HIPAA Privacy regulations selected to be in-scope for this review were Incident Handling and Breach Notification, Self-Pay Restriction, and Accounting of Disclosures (AOD).These were identified for review in consultation with the UCSF Chief Privacy Officer and also identified in prior AAS reviews[4] as potential areas of risks.

The scope of the review covered transactions and activities for the 12 month period ending September 2014 at UCSF Medical Center (UCSFMC), School of Medicine (SOM), School of Dentistry (SOD), Langley Porter Psychiatric Hospital and Clinics (LPPI), and the Proctor Foundation (Proctor).

To conduct our review the following procedures were performed for the areas in scope:

- Reviewed relevant HIPAA Regulations to gain an understanding of the regulatory requirements;
- Reviewed policies and procedures pertaining to protection of accounts with self-pay restriction requests, provisions of AODs, and investigation of potential breaches at UCSFMC, SOM, SOD, LPPI, and Proctor, all of which are areas with clinical services who report compliance to the UCSF Privacy Office;
- Interviewed relevant management and staff personnel to obtain an understanding of existing practices and processes;
- Reviewed samples of incidents reported for appropriateness and compliance with HIPAA regulations in terms of investigation conducted and notifications made to patients and to third-parties, where applicable;
- Assessed the process for recording self-pay restriction requests and protecting those restricted accounts;
- Reviewed a sample of self-pay restriction requests for documentation of the restriction and appropriate handling of billing;
- Reviewed the process for requesting and providing AODs;
- Reviewed a sample of AODs provided to validate that they contained the required information and were provided within the required timeframe;

[3] Audit Project 14-039, report issues September 2014
[4] Audit Project 12-020, report issued January 2012

- Reviewed the Management Corrective Action (MCA) from a prior audit review to validate that the processes developed had been implemented and were functioning as intended;
- Validated the retention of AODs, self-pay restriction requests, and investigation documentation.

Work performed was limited to the specific activities and procedures described above. As such, this report is not intended to, nor can it be relied upon to provide an assessment of compliance beyond those areas specifically reviewed. Fieldwork was completed in October 2014.

III. CONCLUSION

Based on work performed, locations reviewed generally comply with self-pay restrictions and breach notifications. All locations reviewed had procedures in place for notifying the UCSF Privacy Office of incidents and the majority had procedures for documenting self-pay restriction requests. All breaches tested that were handled by the UCSF Privacy Office were in compliance with HIPAA requirements, and the UCSF Privacy Office has thorough procedures and guidelines in place to ensure effective incident investigation and breach notification. All registration and billing systems in use at the locations reviewed have sufficient controls for restrictions for self-pay patients.

Opportunities for improvement exist in the areas of documenting disclosures and information contained in AODs and updating or creating policies and procedures related to AODs, self-pay restrictions, and breach notifications. The method for documenting disclosures in APeX was not understood by all groups responsible for disclosures. For AODs provided, information was not always complete or sufficient, and the requirements for AODs were not documented and retained. Additionally, information from eDisclose was not used in preparing the AODs; therefore disclosures by the Cancer Registry and Clinical Labs may not have been included on AODs provided to patients.

.IV. OBSERVATIONS AND MANAGEMENT CORRECTIVE ACTIONS

A. Accounting of Disclosures

1. The process for documenting disclosures is not well understood by all groups at UCSF resulting in inconsistencies and/or non-capturing of disclosures.

Four of the eight departments who disclose PHI to outside entities were not following the procedures for documenting disclosures in APeX using the Quick Disclose section or eDisclose[5]. These four departments included Clinical Laboratories, Emergency Department, Patient Relations, and Social Work. Additionally, research using identified data was not being documented.

Guidelines for when disclosures need to be documented and where to document in APeX or eDisclose were developed as part of the corrective

[5] eDisclose is an online reporting system used by Clinical Laboratories and the Cancer Registry to track disclosures of PHI.

action plan from a prior HIPAA Privacy Internal Audit review, which found that accounting of disclosures was limited to disclosures entered by HIMS, Cancer Registry, and public health disclosures from Clinical Laboratory as the Medical Center had limited procedures or mechanisms in place to capture and account for all required disclosures under HIPAA. However, due to transition of staff, the above departments were not aware of the guidelines for documenting disclosures under APeX's Quick Disclose and not all staff had been trained in the use of Quick Disclose or eDisclose, which are the main sources of disclosure information HIMS uses to provide AODs.

If the sources for documenting disclosures are not complete, the AOD provided to the patient will be incomplete and may be non-compliant with HIPAA requirements.

Under HIPAA §164.530 Administrative requirements, covered entities must maintain a written or electronic record of actions, activities, or designations that are required to be documented and maintain this documentation for six years to sufficiently meet its burden of proof.

Management Corrective Actions

1. The owners of accounting of disclosures will ensure their workforce is trained on using APeX's Quick Disclose module to appropriately document disclosures. The owners will send a training report to the Privacy Office by February 28, 2015 and will retain backup documentation of the training for six years.

2. Effective March 31, 2015, the Privacy Office will conduct a random annual audit to validate this training for three years, and then assess the necessity for continued audits.

2. Disclosure documentation in eDisclose is not being used for accounting of disclosures by HIMS.

HIMS policy states that they will use the Quick Disclose section in APeX and the eDisclose report in order to account for all disclosures made.

HIMS has only been using the information in the Quick Disclose section of APeX as a source of information for the AODs, and not eDisclose. While most departments should be using the Quick Disclose section of APeX, eDisclose is the system used by Clinical Labs and the Cancer Registry for documenting their disclosures. The Cancer Registry uses eDisclose to report what disclosures have occurred on a monthly basis. Clinical Labs uses eDisclose to document potential inappropriate disclosures as they are detected rather than the disclosures to outside health agencies.

If all relevant sources are not used to provide the accounting, the accounting provided to the patient may be incomplete and non-compliant with HIPAA requirements, resulting in potential fines and resolution agreements.

Management Corrective Actions

1. By February 28, 2015, HIMS will check eDisclose for AODs requested in the past six years to determine if any disclosures have been made for those patients. If any such cases are identified, HIMS will send the cases to Privacy for review and determination on whether an amended AOD will be required.

2. By June 30, 2015, Privacy Office will work with IT to implement a method by which bulk disclosures can be imported into APeX for Cancer Registry and Clinical Labs.

3. By March 31, 2015, Human Research Protection Program in coordination with Privacy Office and Clinical Data Research Consultation Services (CDRCS) will communicate to Investigators that identifiable data to be used for research should be obtained through CDRCS.

4. By March 31, 2015 HIMS will update its Accounting of Disclosures Request Procedure to include contacting CDRCS for potential research uses or disclosures.

3. Policies and Procedures relating to AODs for some areas are absent or have not been updated.

Review of policies and procedures for the locations in scope identified the following:

- LPPI Policy 324 Accounting for Disclosures of Protected Health Information has not been updated to reflect current practices and requirements;
- The SOD's Laboratory and Clinics Policies and Procedures Manual does not currently have a definition of AODs or a process for the provision of AODs, but is currently in the process of being updated;
- The Department of Oral and Maxillofacial Surgery (OMFS) does not have current written procedures for creating and providing AODs;
- Proctor does not have current written procedures for creating AODs;

Under HIPAA §164.30 Administrative requirements, covered entities must implement policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements and change its policies and procedures as necessary and appropriate.

Complete and updated documented policies and procedures provide guidance for employees to ensure awareness of and compliance with current HIPAA regulations and also serve to reduce inconsistencies in how processes are carried out.

Management Corrective Action

By February 28, 2015, the following locations will update their policy and provide a copy to the UCSF Privacy Office:

1. LPPI – Policy 324 Accounting for Disclosures of Protected Health Information will include current AOD requirements.

2. UCSF SOD – Laboratory and Clinics Policies and Procedures Manual will include a process for the provision of AOD.

3. Proctor– Health Information Management and Disclosure Procedures will include AOD procedures.

4. OMFS – Administrative policies for AODs will be created to comply with OCR requirements and training will be provided to staff.

4. Not all AODs provided by the Medical Center over the past six years had complete documentation.

Review of 17 AODs provided by UCSFMC over the past six years found one case that did not have sufficient description of the PHI disclosed in the AOD and another case that did not have documentation of what had been included. The AOD without a sufficient description of the PHI disclosed was from 2013, and the description of the PHI disclosed was "pertinent data," which is insufficient. The AOD without documentation of what had been included was from 2010, and only had the request for the accounting, not what information was provided; however, this case occurred prior to the creation of the current policy that states that the information provided will be maintained by HIMS. Also it was noted that the historic documentation of the information required to be included in an accounting for AODs is not maintained.

Under HIPAA § 164.528 Accounting of disclosures of protected health information, a covered entity must provide the patient with an accounting that includes disclosures of PHI that occurred during the six years (or such shorter time period at the request of the patient) prior to the date of the request for an accounting, including disclosures to or by business associates of the covered entity. Additionally, a covered entity must retain the documentation of the information required to be included in an accounting, the written accounting that is provided to the individual, and the titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.

Management Corrective Action

By March 31, 2015, HIMS will take the following actions:

1. Update Accounting of Disclosures Request Procedure to include reviewing AODs for sufficiency of information provided prior to sending out.

2. For AODs requests, HIMS will attach to the documentation the applicable requirements for AODs under the Health Insurance Portability and Accountability Act of 1996 and/or the new requirements under the HIPAA Final Omnibus Rule (whichever is appropriate).

B. Self-Pay Restrictions

1. Procedures relating to self-pay restrictions for some areas are absent or have not been updated.

Review of self-pay procedures at the selected locations identified the following:

- UCSFMC - Procedures were developed and distributed in 2010 for complying with the HITECH requirements for self-pay restrictions; however these procedures were not updated after the change to the APeX environment. Patient Financial Services (PFS) has recently created a Job Aid for how to handle self-pay restrictions in APeX; however this Job Aid has not been distributed to all groups who may receive self-pay restriction requests.

- LPPI - The procedure for handling self-pay requests does not detail how to document the restriction request in the PsychConsult[6] system, nor how long to keep the restriction request documentation. The current understanding by Registration is that the restriction requests will be kept for three years, which are not in compliance with the HIPAA six year requirements.

- OMFS - Procedures have not been written for processing self-pay restrictions in the WinOMS[7] system.

Under HIPAA § 164.30 Administrative requirements, covered entities must implement policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements and change its policies and procedures as necessary and appropriate.

Complete and updated documented policies and procedures provide guidance for employees to ensure awareness of and compliance with current

[6] PsychConsult is an integrated clinical workflow and revenue cycle system used by LPPI.
[7] WinOMS is a practice management system used by OMFS.

HIPAA regulations and also serve to reduce inconsistencies in how processes are carried out.

Management Corrective Action

By February 28, 2015, the below locations will take the following actions:

1. UCSFMC Patient Access – will distribute copies of the Job Aid for self-pay restrictions to all Patient Access groups and will provide training on how to process self-pay restrictions.

2. LPPI – will provide to the UCSF Privacy Office an update of the current registration policy to include how restriction requests are documented and the requirement to keep the documentation for six years.

3. OMFS – will develop written procedures for processing self-pay restriction in WinOMS and provide this to the UCSF Privacy Office. Additionally, training on these procedures will be provided to staff.

C. Breach Notification

1. LPPI does not have written procedures in place for breach notification.

LPPI does not have written procedures regarding incident investigation or breach notification. Although LPPI is covered by UCSF Campus Policy 200-30, clarification of procedures is needed due to its unique situation and processes.

Under HIPAA §164.30 Administrative requirements, stipulates that covered entities must implement policies and procedures with respect to protected health information that are designed to comply with the standards, and to change its policies and procedures as necessary and appropriate.

Complete and updated documented policies and procedures provide guidance for employees to ensure awareness of and compliance with current HIPAA regulations and also serve to reduce inconsistencies in how processes are carried out. Without these policies in place, there is risk of non-compliance with HIPAA requirements.

Management Corrective Action

By March 31, 2015, LPPI will create Breach Notification and Incident Investigation procedures and distribute these to staff.

V. PROCESS IMPROVEMENTS

During the course of this review, potential opportunities for improvement were noted for enhanced process efficiency. When self-pay restrictions are requested, the form is sent to Patient Relations, who then sends it on to PFS and HIMS. This is an extra step that may unnecessarily delay the process, as Patient Relations does not use the forms other than to send them on to PFS and HIMS. On average, the self-pay restriction forms take over four days from when they are signed to when they are received by PFS. The longer the forms take to reach PFS, the greater the risk that these visits will be sent out for payment in violation of the restriction request. This process was in place prior to Enterprise Content Management (ECM) implementation. A potential solution would be to either have the staff collecting the self-pay restrictions scan the form into APeX or send it directly to PFS and HIMS. The Revenue Cycle team is evaluating whether the self-pay restriction form can be incorporated into the ECM process and where the appropriate place for maintaining the scanned form in APeX would be.