Case Study – Privacy and Security

University of California Davis Health System
2315 Stockton Blvd., Sacramento, CA 95817

Mary Pat Curry
Manager, Health Information Management Department
marypat.curry@ucdmc.ucdavis.edu

Monica Moldovan
Privacy & Security Manager, Health Information Management Department
monica.molovan@ucdmc.ucdavis.edu

Monte Ratzlaff
Manager, Information Technology Security
monte.ratzlaff@ucdmc.ucdavis.edu

Menu Item – Case Study

2012 National Patient Safety Goals and National Priorities Partnership Goals addressed in this case study

<table>
<thead>
<tr>
<th>Number</th>
<th>Goal</th>
</tr>
</thead>
<tbody>
<tr>
<td>NPSG.02.03.0</td>
<td>Improve the effectiveness of communication among caregivers</td>
</tr>
<tr>
<td>NPP Priority Goal</td>
<td>Engage patients and families in managing and making decisions about care</td>
</tr>
</tbody>
</table>

Executive Summary

UC Davis Health System (UCDHS) uses its electronic health record (EHR) to support and document all types of clinical care provided by the organization (inpatient, ED, ambulatory, home care, telehealth encounters). The EHR also supports affiliated and non-affiliated community-based healthcare providers (through direct access and health information exchange) as well as patients and authorized family members directly accessing clinical content in the EHR tethered personal health record (PHR).

UCDHS took a holistic approach to create a multi-faceted Privacy & Security Program aimed at achieving the careful balance between safeguarding protected health information (PHI) and avoiding overly restrictive access controls which could interfere with patient care. UCDHS created a number of innovative processes and software tools to manage access to clinical content. The organization has also made significant investments in modern security technology that is unusual for care providers, and has had a special focus on encrypting client computers, secure thumb drives, relevant emails, and computer backup media.
1. Background Knowledge
UCDHS has made the privacy of patient information an organizational core priority. UC Davis has used a combination of commercially available technologies and software, workflow, and policies created locally. The UCDHS clinical privacy program includes unique aspects related to the way in which access is managed in the EHR, and includes audit trails and surveillance tools.

This comprehensive approach to privacy and security has garnered much attention from other healthcare providers at Epic user group meetings, conferences, and forums. UCDHS has been a national leader in this topic, sharing knowledge and hosting site visits for a number of groups, including prior Davies Enterprise Award winners.

2. Local Problem Being Addressed and Intended Improvement
UCDHS is a large and complex academic medical center for which compliance with increasing regulatory mandates on privacy & security, which includes the protection of sensitive information (e.g. HIV, genetic predictive testing, self-pay visits) and high risk patients (e.g. public figures, celebrities, employees, etc.) can be particularly challenging. In addition, the focus on engaging patients and families in managing and making decisions about care and on improving communication among caregivers, opened new portals of access to the EHR, and generated a host of new security concerns.

Adequately managing the privacy and security of 2,224,333+ unique patients in the EHR, 8,700+ clinical EHR users, 2,000+ community-based users (e.g. referring physicians, researchers, reviewers, telemedicine users) and efficiently processing and tracking nearly 132,000 managed PHI disclosures per year; is a huge challenge. The prior process was (1) labor-intensive, (2) fragmented in clinical silos, and (3) plagued with an unmanageable number of EHR security templates, and overall, could not ensure the level of security the organization required. In order to protect the privacy of millions of patient records, the organization needed to change its approach to security. UCDHS’ goal was to ensure the protection of the privacy of PHI, and to eliminate potential for material breeches.

3. Design and Implementation
Prior to designing the program, a committee was formed comprised of the Legal Counsel, Privacy & Security Officer, Compliance Officer, Human Resources, Risk Management, HIM and IT. The starting philosophy focused on providing privacy and security protections that did not impede patient care. In addition, UCDHS made it very clear that all EHR users are held personally accountable for abiding by all organizational policies and applicable state/federal statutes. Other key aspects of the privacy and security programs are summarized below.

EHR Centralized Provisioning System and Security Management
UCDHS chose to design a unique, centrally-managed and automated provisioning system, coupled with Epic EHR’s security role-based access matrix. This supported staff reduction from 2.5 to 0.1 FTE for manual intervention of exceptions. Now, once a manager authorizes the IT system access request and the user provides proof of identification, HIPAA training and a signed confidentiality statement, the provisioning system automatically completes the request based on the user’s job title/functions, department and credentials.

EHR Surveillance Program
UCDHS developed a one-of-a-kind, centralized surveillance system in which risk-based privacy surveillance and complaint investigations are routinely performed. Some examples of periodic detective privacy surveillance concentrations are: access to high risk patients, HIV or psychotherapy
patients, hospitalized employees, co-workers within same work area, family members of EHR users, or technical users accessing real patients in non-production environments. An innovative new method for real-time monitoring of user access to EHR content was also developed. This surveillance process and technology tracks the users, locations, dates and times of all EHR transactions and supports live monitoring of EHR activity on high risk patients.

EHR Privacy of Sensitive Information
Several ground-breaking technologies were developed to provide additional safeguards for specific categories of patients and/or their record content.

- **Security System Alerts** - to dissuade privacy violations, customized “Break-the-Glass” and “Patient Highlights” (alerts) were developed and applied to the EHR of high risk patients, patients with visit restrictions, victims of identity theft, patients with sensitive information and “black-out patients” for which no information or even acknowledgement of patient’s presence at UCDHS may be given to anyone. “Break-the-Glass” occurs when access is requested to one of these patient records by a user who is not authorized to view the record. The user is required to document their reason for viewing the record and re-enter their password. Once authenticated, the user can continue in their workflow. A log of the request is created and reviewed for possible further investigation.

- **Genetic Testing Privacy and Security Protections** - to provide secondary protection against inappropriate disclosures that could result in potential discrimination, UCDHS designed and implemented an innovative Enhanced Medical Information Security (EMIS) process. Patients who request predictive testing for Huntington’s disease are assigned a pseudonym patient name, with Break-the-Glass functionality for additional privacy protection.

- **Psychotherapy Notes Security Access Restrictions** – to further safeguard this type of ultra-sensitive notes, system functionality was created to allow clinicians to sequester psychotherapy notes by marking them “sensitive”. This technical set-up enables UCDHS to restrict access to these notes only to individuals with an approved psychotherapy security role.

EHR HIPAA Risk Assessment
UCDHS has two full time information technology auditors in the independent Internal Audit Department who perform highly detailed audits and analysis of the health system’s technology infrastructure seeking out risks and security gaps. In partnership with Internal Audit and the Compliance Department, IT leadership also engaged an independent third-party audit firm in 2011 to perform an overall risk assessment of the EHR and its supporting processes. The final report from the extensive review stated, “UCDHS has taken a comprehensive approach in planning and budgeting for requirements. In comparison to other HIPAA projects we have seen, UCDHS followed leading practices in assessing critical success factors for post-HIPAA remediation.”

Technology Evaluation Process
To ensure the technology meets the security and infrastructure support requirements, UCDHS implemented a process to evaluate technologies prior to purchase and implementation. This process applies to new applications, new infrastructure that is not currently supported, new service providers requiring data (sent or received) or connectivity, new clinical devices that is not currently supported, and existing technology upgrades and/or modifications that are “material changes”. Evaluations include a questionnaire regarding security and one for technology infrastructure – both completed by the prospective technology vendor. The security questionnaire has 65 questions covering key risk
issues such as who sees/uses this data, data flow, third-party background checks, external or on premise application hosting, and many other questions regarding access, authentication, encryption, physical security, and other risk issues. UCDHS Purchasing is required to obtain approval resulting from the evaluation process for all in scope technology prior to purchase.

4. How was Health IT Utilized?
UCDHS created three new innovative software tools to manage access to the EHR, perform sophisticated surveillance of clinical software usage, and to track PHI disclosures.

- **User Provisioning System (PS)** - processes new EHR access requests, renewals and deactivations. The PS creates the appropriate security settings and loads the files into the EHR, and then uses specialized software agents to notify users of the status of their request. (written in Domino Designer powered by LotusScript)

- **Surveillance Information System (SIS)** - pulls access logs from multiple clinical systems. Specialized queries and analysis is performed to assess clinical software usage logs to identify potential privacy violations. Analysts in HIM review all potential violations and submit reports to the Compliance Department for review and action. All findings and actions are tracked. (written in SQL Server, uses a .NET framework, Adobe’s ColdFusion Markup Language, and the Microsoft IIS web server)

- **HIPAA Disclosure Tracking System** - pulls data from various clinical software and databases to create and manage outside PHI disclosure records. (written in Java, and uses VB script & VBA macros to connect to SQL databases via ODBC)

MyChart and PhysicianConnect are Epic EHR modules that deliver a tethered personal health record (MyChart) and secure read-only remote access to the EHR for community physicians and support staff (PhysicianConnect). These Epic secure web applications run on the .NET framework using ASP. The web application runs over an SSL/TLS 128 bit minimum encrypted protocol with a 1024 bit public key length to ensure that all data transmitted is secure.

Care Everywhere is an Epic Interoperability framework used by UCDHS that supports the exchange of patient records with other non-affiliated organizations that use Epic EHRs and with organizations that use EHRs from other vendors. Each transaction is secured by utilizing a public key infrastructure (PKI) to ensure secure communication between organizations.

UCDHS is a major center for clinical research, and given the breadth of research, the organization has focused on ensuring the privacy of any patient/subject data used in the research process. Two key initiatives are summarized below.

- **Cohort Discovery Research Support** – The i2b2 ‘Cohort Discovery’ software application was deployed (Informatics for Integrating Biology and the Bedside - an NIH-funded National Center for Biomedical Computing center based at Partners HealthCare System). UCDHS was among the first organizations to fully load a commercial EHR database into i2b2. Patient data is fully de-identified and obfuscated when loaded. The system supports investigators in performing query and hypothesis-validation studies without accessing patient identities or PHI.

- **Research Data Capture** - REDCap (Research Electronic Data Capture) is a secure web application for building and managing online surveys and databases. REDCap was created at Vanderbilt University, and this secure application replaces unsecure spreadsheets and other...
databases used in the past by researchers.

UCDHS has strongly prioritized encrypting all technologies possible to ensure the confidentiality of PHI and other sensitive data. There are multiple types of encryption technology needed.

- **Client Encryption** – deployed sophisticated encryption software on client computers (desktops and laptops) – 98.5% of all UCDHS clients are now encrypted.
- **Backup Media Encryption** – replaced backup systems to bring modern encryption technology to backup tapes. UCDHS has 436 software applications in production use and 99.8% of these now have fully encrypted backup tapes (when 1 remaining legacy system is replaced in the next 3-4 months, encryption will be at 100% of all applications.)
- **Mobile Phones** – for the 1,337 devices owned and managed by the Health System, 100% are encrypted, and have forced use of passwords, time-outs, and remote wipe capabilities
- **Secure Thumb Drives** – deployed 933 Iron Key secure thumb drives for faculty/staff that need to copy or store confidential data on portable media. These drives are centrally managed, enforce passwords, are fully encrypted and tamper resistant, and include anti-virus software
- **Secure Email** – technology was incorporated into the organization’s email system that supports easy to use encryption of email messages. Since deployment, an average of 775 secure emails are sent each week by the organization.
- **Encrypted Storage** – technology to encrypt hard drives has been assessed and is being deployed to the enterprise Storage Area Network (SAN) and Network Attached Storage (NAS). Initial storage encryption has been focused on the storage of data files with PHI or PII, and 44.9% of the SAN and 37.6% of the NAS that store this type of sensitive content are now encrypted.

Additional technology is being investigated to encrypt ‘data in motion’ (interfaces).

5. **Value Derived/Outcomes**

Because of its security policies and technology, **UCDHS is meeting the original goal of ensuring no material breaches of confidential patient information since implementation of the privacy and security policies and technologies described in this case study.** Implementation of a modern certified EHR across all venues of care created ability for simultaneous access to a patient’s complete medical record and helped improve efficiency throughout the organization in patient care, academics, research, coding, audits, statistics and many other functions.

Remote access and telecommuting helped improve efficiency, quality and continuity of patient care, physician convenience and satisfaction. For example in 2012, a total of 2,476 individual clinical users logged on after hours, weekends and holidays, totaling 461,058 instances of remote EHR access activity in the course of providing care. Without the many security processes and technologies that have been implemented, this remote access to the EHR would not be feasible.

Various EHR modules now provide a secure communication method with external caregivers who are not part of the UCHS system. In 2012, 569 physicians and their staff accessed the EHR remotely and 54,940 distinct patient charts were released electronically. In total, since February 2009, over 3,269 non-affiliated community physicians and their staff who do not use the Epic system accessed the UCDHS EHR remotely for read-only access via the PhysicianConnect system and a total of 262,218 distinct patient charts were securely released electronically. In 2012, 18,268 patient records were exchanged between affiliated and non-affiliated organizations using Epic Care Everywhere. The ability to share patient clinical data with appropriate community care providers and providers in
the UCDHS system is critical to support transitions of care, and would not be possible without security processes and technologies.

Over 73,342 patients have signed up to access their clinical data via the tethered PHR called MyChart and also 2,787 families access the system on behalf of patients through appropriate proxy access. Patients can also share secure messages with their UCDHS physician. Patient secured electronic access of their charts has helped UCDHS achieve greater patient involvement and satisfaction (94% rating its ease of use as Good, Very Good or Excellent).

*Appropriate use and access to PHI is recorded and monitored* in granular audit trails that are routinely reviewed by a team of 6 HIM analysts dedicating 10% time on a rotational basis. In 2012, over 56,464 instances of access were reviewed to proactively protect the privacy and security of patients, thereby helping avoid potential privacy breaches.

6. Lessons Learned

**Top-down Leadership is Critical**
With direct support of senior leadership, UCDHS’ philosophy to provide EHR privacy and security protections without interfering with patient care and hold all users personally accountable, has worked very well. A combination of administrative policies and integrated IT tools were effectively embedded into business processes which allow for immediate, seamless and compliant access, use and disclosure of PHI.

**On-Going Maintenance**
A phased EHR deployment and ongoing optimization are particularly challenging, but critical, when building the application security and user roles because analysis and security adjustments are frequently required. Furthermore, privacy & security analysts must keep abreast of clinical workflows for all live applications, in order to consolidate security templates for manageability and ruling out false positives from access logs.

**System Alert Fatigue**
Pushing out an extra alert screen upon entry into a chart should be used selectively so as not to delay patient care. All “Patient Highlights” are reviewed by a physician-driven Alerts Committee to ensure the alert warrants everyone’s attention and when possible, limited to the group of users that are potentially affected by the information it contains.

**Leveraging Technology Above and Beyond**
UCDHS has innovatively leveraged the Epic Release of Information (ROI) module. Rather than simply storing disclosure forms, UCDHS saw the potential of this module and configured it to centrally track all disclosure activity. Additionally, using the ROI module to manage subpoenas, court orders/search warrants (medical, finance, IT, HR) allows for monitoring of compliance with regulatory timelines and tracking these types of disclosures.

**Information Security Requirements for Research Grants and Contracts**
A foundational component of research activities is obtaining data and funding from various government grants and contracts. The agencies, both state and federal, require a specific level of information security controls in place prior to award and engagement. Examples of requirements include background checks, workstation/laptop encryption, server security, removable media devices, antivirus software, patch management, user ids and password controls, data destruction, system logging, transmission encryption, and intrusion detection. UCDHS has been able to acquire
Security is a Process – Not a Destination
Although a robust security program requires significant investments in security technology it also requires numerous processes supported by governance and qualified, highly skilled staff. UCDHS has committed to maintaining five IT Security FTE staff to assure the overall security, confidentiality, availability, and integrity of its technology and data assets and promote the secure use of its technology resources. These staff maintain security certifications such as Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), and Certified Information Systems Auditor (CISA) as well as staying aware of constantly changing threats and keeping current with their skills. Maintaining awareness of emerging threats allows the security staff to advise on which new technologies or processes are required to adequately mitigate the threats.

7. Financial Considerations
To secure 2.2 million patient records and over 7 million clinical images, to provide access to 8,700+ clinical EHR users, and to comply with state and federal regulations, the organization has made a $6 million dollar capital investment for modernized and robust security technologies and continues to invest $1.5 million annually in labor and maintenance costs. There are 20 distinct technologies that support information technology security objectives at UCDHS. These technologies fall into the following categories:

- Access Control
- Anti-Malware
- Encryption
- Authentication
- Threat Identification & Mitigation

The strongest return on investment (ROI) for a privacy and security program is the avoidance of material privacy breaches. To date, UCDHS has had no material breaches of information that posed significant risk of financial, reputation or other harm to patients. Occasional minor breaches, such as faxing a document to an incorrect fax machine, do occur, however these are minimal and addressed as soon as they are noted.

A solid privacy and security program is a healthcare provider’s best defense against privacy breaches, and defines how the organization manages the patient information they are entrusted with.
As of August 2013, UCDHS has encrypted 98.5% of the client computer use by UCDHS faculty and staff.

UCDHS has experienced the loss and theft of client computers, but the encryption of these devices has prevented a privacy breach.

Records for patients with special privacy conditions (such as victims of identity theft) are noted in the EHR.

A Break-the-Glass occurrence begins when one of these patient records is requested by a user. They are asked to re-enter their password and to document their purpose for viewing the record. Once authenticated, the user can continue in their workflow. A log of the request is created in the EHR and reviewed for possible further investigation.
There has been dramatic growth in secure messages between patients and UCDHS clinicians and care teams using Epic MyChart tethered personal health record (PHR).

969,163 encrypted messages shared between UCDHS clinicians and patients from February 2009 through February 2009 to August 2013.

UCDHS added the Axway technology to encrypt emails sent outside of the UCDHS email system when sensitive content must be sent via email.

101,828 encrypted emails have been shared between UCDHS faculty and staff and external entities from March 2011 to August 2013.
UCDHS has utilized the secure thumb drive technology from Imation called Iron Key. This product supports central IT management of passwords and similar functions.

The thumb drive is both encrypted and has anti-malware software.

These thumb drives are funded in the IT budget and provided to any faculty or staff that need to copy and transport sensitive data files.

From August of 2010 and August of 2013, 931 Iron Key thumb drives have went into production use.