Privacy and Protected Health Information (PHI) Surveillance Technologies
Developed at UC Davis Health System

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

Submitting:
Mary Pat Curry - Health Information Management Department Manager

Project Team / Subject Matter Experts (SMEs)
Carlos Aguilar - SME Technology
Joshua Simon - SME Technology
John Nystrom - SME Technology
Erol Layiktez – SME Technology
Mark Sy - SME Surveillance Investigations
Eloisa Javier - SME Surveillance Operations
Monica Moldovan- SME Privacy, Security &Legal

Stakeholders
Michael Minear- Chief Information Officer
Anna Orlowski - Chief Health System Counsel & Privacy Officer
Teresa Porter- Chief Compliance Officer
Mary Pat Curry - Health Information Management Department Manager
Monica Moldovan – Privacy and Security Manager

Contents
Project Description - History, Problem, Opportunity, Solution .............................................. 1
Technology Used Design and Implementation ......................................................................... 3
Objectives and Customer Satisfaction Outcomes ..................................................................... 4
Conclusion ................................................................................................................................... 4
Appendix A .................................................................................................................................. 6
**Background**

The UC Davis Health System (UCDHS) is a comprehensive academic health system that strives to create a healthier world through bold innovation. The organization has invested tens of millions of dollars and years of hard work implementing an electronic health record (EHR), which recently was named “most wired” and integrated entity in the nation. The EHR is not only shared across all venues of care within the Health System, but also extends to community-based healthcare providers and patients, as well as their authorized family members. While there are tremendous advantages to having an electronic and more accessible patient record, there arose concerns about the privacy and security of protected health information and the privacy protection and legal responsibility providers now have to provide adequate protection against unauthorized access, use and disclosure of the protected health information.

This case study describes the state-of-the-art, nationally recognized unique technology development and approach taken by UCDHS to create a highly technical, multi-faceted EHR Privacy & Security Information System aimed at transforming how Privacy and Surveillance monitoring is performed in the healthcare industry. This technology and tools developed “in-house” at UC Davis were referred to as “some of the best privacy technical solutions in the nations” by HIMSS representatives. Other hospitals and integrated delivery health systems have modeled their privacy protections programs after UCDs developments.

**Project Description - History, Problem, Opportunity, Solution**

Adequately managing the privacy and security of over 2,000,000 patient records, over 8,500 EHR users, several thousand community-based users (e.g. referring physicians, researchers, reviewers, telemedicine users, etc.) and efficiently processing and tracking nearly 114,000 PHI disclosures per year seemed daunting.

Likewise, compliance with ever increasing regulatory mandates on health care privacy & security, which includes the protection of sensitive information (e.g. HIV, genetic predictive testing, mental health, self-paid visits) and high risk patients (e.g. public figures, celebrities, employees, etc.), can be particularly challenging for a complex academic health system. In addition, the focus on engaging patients and families in managing and making decisions about care (via MyChart, a tethered personal health record) and improving communication among caregivers (via PhysicianConnect, EHR view-only access for community providers to follow their UC Davis patients) opened new avenues and portals to access protected health information by various parties and entities, and with that, new privacy and security concerns arise.

UC Davis Medical Center, launched an intensive search to find a vendor/software solution that would bring the health system’s major clinical applications electronic audit and access logs into one repository, to allow for live and retrospective review of all staff activities within EHR and simultaneously validating the appropriateness of such access to PHI. After months of interviews and proposals, no ‘off the shelf’ products were found in the market that would centralize the major clinical systems audit logs and support our organizational objectives related to the mandatory privacy protections requirements. The decision was made to create the software internally. After roughly six months, the privacy Surveillance Information System (SIS) was developed, this
streamlined the privacy surveillance procedures and significantly increased the efficiency and effectiveness of the UCDHS Surveillance Program.

This report will focus on this breakthrough technology that UCDHS developed for the privacy surveillance monitoring and protection of sensitive protected health information as crucial elements of any comprehensive and successful EHR Privacy & Security Program, consequently minimizing any risk of State and Federal penalties tied to wrongful access, use and disclosure.

At the time of the SIS project initiation, UCDHS was already one of the Privacy leaders in the healthcare industry. UCDHS had developed a surveillance program that used technology to facilitate its core workflow of identifying high-risk patient population and conducting routine privacy surveillance of workforce access to the patients protected health information.

The foundation of the UCDHS Surveillance Program prior to this innovative development of the Surveillance Information System relied on:

- Using Crystal Reports to manually edit, run, and then analyze patient access data
- Maintaining file folders to track surveillance program analytics
- Creating custom data tables to provide meaningful use of audit logs from Epic’s Electronic Health Record system
- Manually entering, logging, and notifying stakeholders and users of potential violations

The goals of the SIS were to automate the fundamental surveillance business process, integrate several independent clinical systems audit logs into a single repository to create a complete picture of user access appropriateness to patient data and creating customized database objects that enhance the ability of a surveillance analyst to perform privacy surveillance reviews. Recognizing that technology and regulations rapidly change, the SIS was built with a scalable architecture that allows easily creating, updating, or removing any data management or business process functions.

Our innovative SIS development initiative required collaboration across venues of several key clinical departments, to accurately gather requirements and data attributes from each system. Some of our breakthrough milestones were:

- Creating the first of a kind data warehouse model to store the user identities consistently across major clinical systems
- Working with our clinical application vendors to incorporate audit logs from the major clinical systems and extract them into our data warehouse
- Transforming business processes, business rules, data marts, data algorithms, and the surveillance analysts knowledge into functional, technical requirements and user interface features to allow privacy and surveillance monitoring and investigations to be accomplished successfully (See Appendix – Application Views)

The end result of our development exceeded all our objectives, thus taking this industry leading privacy surveillance technology to the next level. This state-of-the-art tool consumes audit log files daily from the major clinical systems (See Appendix - Audit Log Visual), maintains and links data about user identities across different systems, incorporates the surveillance analysts’ thought process into the data management, analyzes these rules and displays data with decreased likelihood of false positives and conversely increasing the likelihood of potential violations, systemizes
notifications, integrates case tracking into a single database, and automate surveillance reportable data.

The heart of the SIS is the capability to take electronic build-in surveillance criteria, such as a user looking at patient who is a coworker within the same department, and presenting the cases to the surveillance analyst user, along with critical decision-making data attributes like:

- patient demographics and relevant hospital or clinical contacts,
- access audit trail from a user on a patient on more than one clinical system,
- user demographic information, HR data, and security level, and
- actionable case review functions for further review, potential violation notification to stakeholders, or simply closing as a false positive.

**Technology Used Design and Implementation**

UCDHS developed a unique centralized surveillance system in which risk-based “detective” privacy surveillance and complaint investigations are routinely completed. Some examples of periodic detective privacy surveillance focuses are: access to high risk patients, HIV or psychotherapy patients, hospitalized employees, co-workers within same work area, family members of users, or technical users accessing real patients in non-production environments. (see Appendix - for the UC Davis Health System SIS Implementation Timeline)

SIS made up of 3 primary components:

- **Data warehousing** - SIS consolidates all of the access logs from EHR and its ancillary systems into a single location. Access logs are compiled into “cases”
- **Web Front End** - Used for viewing and processing a case. Analysts use the web interface to assess each case and determine if a violation has been committed.
- **Legal and Regulatory Compliance** – when the SIS system auto creates a ‘privacy case’ based upon build-in legal and compliance business rules, indicating that a potential privacy violation may have been committed, the SIS can be used to centrally gather data and communicate with the workforce member who’s activity is under review, investigator and analysts working on the case.

**Application Software**

The SIS is written using Adobe ColdFusion 8, whose platform allowed us to rapidly build our scalable solution with fewer lines of code. The SIS is programmed using a Model-View-Controller Framework methodology, which promotes code re-usability and easily separates the HTML from the methods and program logic. To enhance the end user experience and efficiency of the application jQuery and Ajax are utilized. jQuery effectively allows the application to handle events and enables the Ajax functionality. A large portion of the application is built using Ajax and is inherently dynamic and interacts with the server and database without interfering with the display and avoiding pages from being refreshed.

**Database**

The SIS data resides on a Microsoft SQL Server 2005. There are 100 tables created to manage the entire application. Using Microsoft SQL Server allows for scalability in anticipation of extremely
large datasets. We have optimized the database with indexes to provide high performance data retrieval.

**Extract, Transform, and Load (ETL)**

The ETL packages for the SIS come three fold: (1) packages for populating the data warehouse with all the clinical applications audit logs, (2) packages for compiling the audit data together based on the surveillance criteria, and (3) packages uses for applying logic to the data to automate some of the analysis and minimize false positives.

All of the ETL packages are built using SQL Server Integration Services (SIS). SIS a component of the Microsoft SQL Server database software and can be used to perform a broad range of data migration tasks. SIS a platform we use for data integration and workflow applications. It features a fast and flexible data-warehousing tool used for data extraction, transformation, and loading (ETL).

**Objectives and Customer Satisfaction Outcomes**

Several breakthroughs were accomplished as part of the in-house development and implementation of this technology

1. Appropriate use and access to PHI is recorded and monitored in granular audit trails, that are reviewed periodically as part of the surveillance program. In 2011, HIM reviewed 24,000 instances of access in an effort to proactively protect the privacy and security of UCDHS patients.

2. Financial Impact - The strongest return on investment for a privacy and security program is the avoidance of material privacy breaches by workforce. To date, UCDHS has had no material breaches of protected health information that posed significant risk of financial penalties, reputation hindrance or harm to patients. A November 2011 study by the Ponemon Institute found that 96% of the 72 surveyed healthcare organizations had at least one data breach in the last 24 months; with an average annual impact of $2.2 million (Ponemon, 2011). Other breach cost estimates range as high as $13 million dollars per incident (MarketWatch, 2012). In the Sacramento area, one care provider was hit with a $1 billion dollar class action lawsuit in November of 2011 from the theft of a single computer that stored over 4 million unencrypted patient records.

3. Community and Patient Trust - While the financial penalties of a privacy breach can literally endanger the economic survival of a health care provider, a privacy breach also carries the intangible cost of damaging the community’s confidence in the organization, and impact patients’ willingness to trust care providers and researchers with their uniquely private health information.

4. Operational Efficiencies - Using the compiled data set and dashboard interface, surveillance analysts can review more cases with more accuracy than ever before. This technology brought specificity to the data they review for potential violations, filtering out all the noise and the false positives.

**Conclusion**
Recognizing that Privacy of Patient Health Information is a top priority mandated by both State and Federal Statutes, UCDHS committed to overcome challenges.

Prior to designing the UCDHS EHR Privacy Surveillance and Security Program, a steering committee was formed comprised of the Legal Counsel, Compliance, Privacy and Security Officer, Human Resources, Risk Management, Health Information Management (HIM) and IT. UCDHS’ philosophy was to provide EHR privacy and security protections without interfering with patient care, and hold all users personally accountable. This approach was successful only with the direct support of senior leadership. A combination of administrative policies and innovative IT tools were effectively embedded into business processes which allow for immediate, seamless and compliant access, use and disclosure of PHI.

Even the brightest vision cannot be executed without adequate funding. The biggest challenge for UCDHS has been limited financial resources aggravating competing priorities. The privacy and security program and tools were funded as part of operational costs. Another difficult challenge was overcoming the lack of an economical “off the shelf/plug and play” surveillance software system that would address the privacy monitoring needs of an integrated healthcare setting. Acquiring a scalable solution to maintain audit logs over time is an absolute necessity.

California laws allow the state to levy fines against hospitals and individuals for PHI security breaches. In June 2010, the Department of Public Health announced the first round of fines against hospitals and issued fines totaling $675,000 against five California hospitals. This is why a comprehensive Privacy and Security program that balances individual accountability with EHR access and surveillance monitoring is key to successfully avoiding such extreme penalties.

Developing proactive and cutting edge technological strategies is essential in sustaining a successful Surveillance Program. The Surveillance Information System (SIS) Technology once again brought us another step closer to our vision of “Transforming Healthcare Through Bold Innovation.”
Appendix A

UC Davis Health System SIS Implementation Timeline

<table>
<thead>
<tr>
<th>Phase I: Requirements Development</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>2004-2009</strong></td>
</tr>
<tr>
<td>• Development of Surveillance Workflows, Criteria, Audit Logic</td>
</tr>
<tr>
<td><strong>Summer 2009</strong></td>
</tr>
<tr>
<td>• Created and defined Project Charter</td>
</tr>
<tr>
<td>• Acquired hardware</td>
</tr>
<tr>
<td>• Meet with other system owners, prepared other systems to turn on and send audit logs</td>
</tr>
<tr>
<td>• Initial technical specifications where gathered and implemented</td>
</tr>
<tr>
<td><strong>November 2009</strong></td>
</tr>
<tr>
<td>• Data warehouse designed with scalability in mind and created</td>
</tr>
<tr>
<td>• ETLs where created and scheduled for Audit Data</td>
</tr>
<tr>
<td>• Audit data began to fill the data warehouse from other clinical systems</td>
</tr>
<tr>
<td><strong>Fall 2010</strong></td>
</tr>
<tr>
<td>• Implemented interim process for reporting on audit data using crystal reports</td>
</tr>
<tr>
<td>• Created web based centralized case tracking forms</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Phase II: SIS Development</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>January 2012</strong></td>
</tr>
<tr>
<td>• Goal was to complete end user experience and fully utilize audit data</td>
</tr>
<tr>
<td>• Requirements gathering and knowledge transfer of existing structure</td>
</tr>
<tr>
<td>• Application specifications and use cases created</td>
</tr>
<tr>
<td><strong>Spring 2012</strong></td>
</tr>
<tr>
<td>• Unit, Integrated and User Acceptance Testing</td>
</tr>
<tr>
<td>• ETL’s created for case management and surveillance criteria</td>
</tr>
<tr>
<td>• Integrated the web based centralized case tracking forms</td>
</tr>
<tr>
<td><strong>Summer 2012</strong></td>
</tr>
<tr>
<td>• Internal P&amp;P created</td>
</tr>
<tr>
<td>• Training provided</td>
</tr>
<tr>
<td>• Web Application Go Live</td>
</tr>
</tbody>
</table>

Surveillance Information System (SIS)