Cutting Edge Provisioning & EHR Application Security Management Tool
Developed at UC Davis Medical Center

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

Submitting
Mary Pat Curry – Health Information Management Department Manager

Project Team
Gloria Ayala-Partida – Business Requirements External Users Subject Matter Expert
Desiree Garcia – Business Requirements Internal EHR Users Subject Matter Expert (Project Lead)
Carlos Aguilar – Business Requirements Subject Matter Expert & EHR Security (Project Lead)
Erol Layiktez – Technical Subject Matter Expert & EHR Security
Joshua Simon – Technical Subject Matter Expert & EHR Security
John Nystrom – Technical Subject Matter Expert & EHR Security
Mark Sy – Technical Subject Matter Expert & EHR Security
Maurice Hamilton – UCD IT Dominos Lotus Notes Programmer
Dan Cotton – UCD IT Manager
Monica Moldovan – HIM Privacy & Security Manager

Stakeholders
Vincent Johnson – UCDHS Chief Operating Officer
Michael Minear – UCDHS Chief Information Officer
Mary Pat Curry, RHIA – UCDHS Health Information Management Department Manager
Monica Moldovan, JD, MIS, CHPS – UCDHS Health Information Privacy & Security Manager
Health Information and Clinical Informatics (HICI) Oversight Committee

Contents
Background................................................................................................................................................... 2
Project Description – History, Problem, Opportunity, Solution................................................................. 2
Technology Used, Design and Implementation............................................................................................. 5
Objectives, Project Timeline and Customer Satisfaction Outcomes ............................................................ 5
Appendix....................................................................................................................................................... 7
Background

The UC Davis Health System (UCDHS) is a comprehensive academic health system that strives to create a healthier world through bold innovation. UCDHS manages an Electronic Health Record (EHR) that is shared across all venues of care within the Health System, it extends to community-based healthcare providers, our patients, and authorized family members. To ensure the highest level of patient care delivery, patients’ engagement and satisfaction, it is vital that our UCDHS clinicians have timely access to EHR to deliver prompt care and communicate with the patient and other members of the treatment team. Likewise other nursing and clinical staff must have compliant and appropriate level of EHR security, as quickly as possible to deliver care. Delays in accurate system level access may hinder providing critical care.

This case study describes how the development team at UC Davis Medical Center (UCDMC), transformed our manual, time consuming, error-prone EHR access provisioning process into a ‘state of the art’ computerized, algorithm based provisioning system that grants compliant EHR access clearance based on system definitions, legal requirements, unique user attributes from various sources systems, and without any staff manual intervention. The speed and accuracy of this web based system is unparalleled in the industry, where most health organizations still rely on overly complex processes, import/export spreadsheets, EHR vendor support, manual processing of the access and manual management of the EHR security. The application is highly extensible, allowing new and expanded business rules, policy and/or regulatory changes. A recent survey of our customer, indicated that this innovative technology is notably “significantly more accurate” and “much faster” than previous systems used for managing security and provisioning our clinical end user. The EPIC Research and Development team, other nationwide hospitals and integrated delivery systems have solicited our team to share and participate in countless technical knowledge sharing sessions, with the intent and interest in modeling their EHR provisioning system and EHR application security management after UCD’s innovative tool, ‘also known as’ OPAL (Online Provisioning Access to the Legal medical record) fully designed, developed and deployed at UC Davis Medical Center.

Project Description – History, Problem, Opportunity, Solution

UC Davis Medical Center is an early adopter of EHR, in 2003 we went live with our EHR system and with it, came the ongoing challenge to correctly manage an ever changing workforce with dynamic roles and regulatory needs to provide the correct access for users in the course of delivering critical patient care. The EHR vendor, from 2003 to present, provided no technical integrated solution to centrally and electronically provision and manage the EHR application security and its components. This resulted in each record of approximately 10,500 users be managed manually through the use of complicated import spreadsheets, technical specification documents, coupled with collection and manual entry of a multitude of user data from different source systems, such as Human Resources System, Clinician Credentialing, Licenses and Privileges System - a mainframe repository, and other separate data sources, ultimately working towards acquiring required user values and mapping each access security level type, for each clinical venue (i.e emergency room, inpatient, ambulatory, hospital based clinic and etc) and provide timely, legally compliant, and correct level of system access clearance for our EHR users.

Adding to the complexity of managing users access, was the HIPAA compliance regulations requirements of maintaining records pertaining to access controls, identity proofing, HIPAA confidentiality training, track system authorizations and approvals, through disparate systems that had to continually be updated and maintained to keep UC Davis in compliance with State and Federal regulations. As a teaching hospital and highly regarded health care facility in the region, our user types (Appendix, Figure 1) that needed to be provisioned and maintained, kept evolving and churning. Some of the unique users were international medical students, rotating residents, visiting internists, locum providers and external referring providers. Each one of our 88 EHR security templates contains a combination of
system security points, security classes, security roles and system profiles specific to each user type and also specific to the clinical venue, which is why extensive research and collection of user attributes is critical before an EHR security template could be selected.

Prior to the development of this innovative state of the art tool, the labor-intensive process to create a user account involved several administrative steps and manually receive signatures on papers for identity proofing, sponsor authorizations and HIPAA Privacy and Security Training. Another example of manual inefficiency was the communication for additional information from users, sponsors, managers, requesters, and then manually collecting the response values, copy and paste them into the EHR EPIC system approved import sheets. We also has to manually validate the data against “source systems of truth”. For example, we would have to log on to the HR PeopleSoft system, look up staff information and then take each determinant value, enter it in our system and manually find the correct EHR access type.

The manual steps of the provisioning process described above were required during account creation, for all account updates and for revocation of access. Meaningful reporting was especially challenging, cumbersome, impossible due to lack of discreet fields, and even inaccurate. The management of the EHR application security and the entire provisioning process, via manual steps was problematic to maintain due to the complexity of user attributes from multiple source systems, the complexity of EHR integrated system security and its 30+ EPIC applications/modules currently in production at UC Davis Medical Center. As the clinicians rely mainly on the EHR tool to deliver their care to patients, the process of keeping track of system security, as well as user provisioning algorithms, and clinical venue would often fail due to the manual and administrative steps from all cross-functional teams involved. Often our EHR user satisfaction would fail on account of:

- Access delays, due to data entry errors on the initial user request
- Inability to properly identify the EHR users’ job function resulting in the incorrect EHR access
- Delays in timely processing of new user by other departments (HR, Provider Credentialing)
- Prolonged turnaround times for all requests due to need for users and managers additional signatures and attestations.
- Lack of duplicate record checks
- Loss of data integrity checks, pertaining to the user information inconsistent in source systems and subsequently this information being shared in downstream shared files across many users
- Manual troubleshooting of existing accounts to determine correct access and root cause issues
- Inefficient steps to identify, receive and maintain documentation for all staff that required legally compliant signature

As the requests for access increased, use of multi-interdisciplinary EPIC EHR applications/modules continued to grow, and the legal requirements for access controls continue to expand, it was determined that a pioneered, groundbreaking and scalable technical solution would be necessary to meet all our complex mandatory regulations, and keep all user identities relevant to EHR, centrally managed.

The utmost value of a user account to the EHR at UCD, is appropriate access in the most expedient manner possible, enabling the ultimate goal to provide immediate patient care. The new access system would have to meet an array of business rules, legal requirements and compliance with regulatory bodies including the following:

- **Patient Care Expediency**: Accurately create EHR user accounts with the access that provides the correct privileges and functionality within one hour of an access request being submitted
• **Leverage Disparate UCD Source Data Systems:** Information from Human Resources, Provider Information Tracking System, Windows Active Directory, and the EHR Clarity Database would be setup in ETL (extract, transform and load) and then made available through a structured manner that specifically supported the new tool and provided a standard SQL based way of validating data sources and user’s identity.

• **Role Based Access:** Every job code at the UCD would be analyzed and specific type of user access templates would be derived from all the available data for each user, including specific clinician privileges such as determining who can document in a chart and order procedures or medications for a patient. (Appendix, Figure 6)

• **Standard Data Management:** Create and maintain the full data elements that provide all access request audit information, including the 5 Ws and recording all communications and system functions for each user/access request.

• **System Based Processing:** System should electronically intake access requests and process them through a tree based decision for data accuracy and validation. Maintain and provide all communication and electronic signature pathways to remove paper base processes. System should provide intuitive way for analysts to resolve any exceptions through find and click functions and resolve errors. The system will maintain audit trail of all system activities.

After a significant amount of development work, UCDHS was able to create an innovative, state of the art technical tool solution dubbed “OPAL” (Appendix Figure 3). The web based technology is able to meet all the requirements from external and internal regulatory bodies and can deliver a solution that provides the ability to gather separate data sources and ensure the user received access in a timely fashion.

Additionally, OPAL ensures that the UCD workforce is compliant with regulations by having the right level of access through a series of automated logical maps that defined the user’s job role in their work department (Appendix, Figure 1), and provides built-in administrative business rules that continue to maintain the user accounts long after the initial account creation. Processes that safeguard against improper access such as account revokes, expired HIPAA documents, clinical providers with outdated privileges reviews are all included in OPAL to continually ensure proper access. In the event that an access request could not be resolved automatically, OPAL has an interface that gives an analyst an intuitive point and click solution to resolve anything preventing the delivery or removal of access. (Appendix, Figure 3)

Beyond the foundational needs of OPAL to meet electronic user account regulations, OPAL was able to extend past its original framework to provide:

• A public facing secure web portal for external community physicians that allows for the self-enrollment to the UC Davis Physician Connect portal which allows non UC Davis providers to view their patient’s data at UC Davis.

• New electronic web forms that use secure industry standard electronic signature captures to provide a rapid documentation process that eliminates the need for email, fax, or paper scans.

• All communication to the customer regarding log-in information, requests for supplementary information and the like are automatically generated from the system.

• Clinician records are created automatically with all of the appropriate access and security to deliver care.

• Complete account maintenance mechanisms and automations, such as access renewals, access revoke, attributes changes and updates, all are now handled automatically, based on the end dates in the system and input from sponsors via online web forms.

• Built-in business rules to assure compliance with State and Federal regulations.
- Electronic inventory of our EHR security structure and all its 30+ integrated applications/modules
- Live interfaces and built-in ETL (extract, transform and load) processes that centrally process and acquire user attributes
- Live account creation imports that run automatically without user management or intervention

**Technology Used, Design and Implementation**

OPAL is programmed using ColdFusion 10 with Model-View Controller (MVC) Framework which promotes code reuse and extensibility. MVC easily separates presentation layer from program logic and database interactions. OPAL is a web based application and can be run on any standard web browser. The core of OPAL consists of the application software and user interface, database, integration components and the data integrity and automation tools.

**Application Software and Database**

OPAL is written using Adobe ColdFusion 10, a platform that allowed us to rapidly build our scalable solution with fewer lines of code. To enhance the end user experience and efficiency of the application jQuery and Ajax are utilized. The data relevant to OPAL is stored on a Microsoft SQL Server 2008 database. The table structure is maintained in third normal form to optimize performance. As OPAL interacts with several other source systems, including Active Directory, there are elements of Java mixed into the code base.

**Integration**

Full Integration with secondary UCDHS source systems allows for a collection of data not previously possible. This is one of the key drivers of automation and saves analysts significant amounts of time. Prior to OPAL analysts needed to log in and out of several systems to gather information or open various MS Office files. OPAL automatically interacts with more than seven external UCDHS systems including:

- Central Authentication System (CAS) – Authentication
- Active Directory – Allows access to employee IT records, including login name
- Campus LDAP Server – Allows access to medical student demographics
- PITS (UCDHS Provider Tracking system) – Allows access to provider records
- PeopleSoft (UC Payroll System) – Allows access to employee demographics
- HP Service Manager (UCDHS Service Request System) – Self Service Portal to request EHR Access
- EHR Reporting Database – Allows for cross checking of EHR user data

**Data Integrity and Automation**

OPAL processes most requests automatically and transmits the user record directly to the EHR server; therefore, creating accounts without human intervention. The requests that need review or manual input stop and are processed via the analysts’ graphical user interface. Automated emails are sent to the users to inform them when access has been created, or to request additional information as needed. Checks and controls are always in place to reduce errors. All input is cross checked against multiple data sources and when necessary, OPAL automatically assigns an analyst to review an exception or data conflict. The OPAL database is managed and backed up by UCDHS IT department and it is also clustered. Role based tools in OPAL allows analysts to override system decisions as necessary without the need of an application developer.

**Objectives, Project Timeline and Customer Satisfaction Outcomes**

The two most critical components of EHR security access provisioning are **timeliness** and **accuracy**. Providers must be granted access as quickly as possible as to not inhibit patient care and that access must be correct for the same patient care reasons. Previously, the provisioning process relied on the speed and accuracy of a person processing the request. The transition to OPAL allowed us the opportunity to move away from manual/error prone processing to automatic processing, whereby the system does most of the decision handling.
Even the brightest vision cannot be executed without adequate funding. The biggest challenge for UCDHS has been limited financial resources aggravated by competing priorities. Another difficult challenge was overcoming the lack of an economical “off the shelf/plug and play” provisioning software system that would integrate with our EHR (EPIC) and address the complex application security and the access provisioning needs of an integrated health care setting like ours.

Due to the lack of a precedent similar technology in the healthcare industry, with capability to work with EPIC specific security components, our project was approached in 3 main phases (Appendix, Figure 5). We first automated the process for UCD workforce in 2009 over a period of eight months. Later in 2010, as part of phase two, we added the community based physicians and other memebers of the treatment team over a period of thirteen months. Finally in 2012 after several lessons learned and an intensive ten months effort to acquire all technical and business requirements, we developed and deployed OPAL to handle both internal and external users, as well as the 30+ EPIC applications/modules security components.

Several breakthroughs were accomplished as part of the in-house development and implementation of these technologies. The foremost customer satisfaction comes from the ‘patient care centered’ turnaround time of our process. The patient care focus can be grouped into four areas:

- **Near real-time provisioning** reduced provider downtime and dissatisfaction (Appendix, Figure 4) and ultimately improved our patient safety outcome. Automatic access template assignments reduce the risk of the wrong access being granted due to human error.
- **Sophisticated exception handling technology** allows administrators to quickly identify and correct problems hindering the completion of EHR access security request. (i.e incomplete demographics, unauthorized approvers and bad data from external systems)
- **Advanced logging protocols allow auditors** to view all actions by the system taken to grant access, including meeting compliance requirements via automatic decision making and automatic emails.
- **Integrity checking across multiple systems** allows for data to be corrected in external systems that might otherwise go unnoticed.

Another area of success where this provisioning system meets crucial objectives is centered on external technology and HIPAA audits. The EHR security management, access/provisioning processes, the tool itself and the HIM Privacy and Security team have undergone many internal and external audits and received complements on the state-of-the-art tool, our procedure and detailed documentation we use in our process. The system maintains safeguards and access controls, ensuring the right person gets the right access; assuring UCDHS is compliant with State and Federal laws and avoids fines.

This award winning creative processes coupled with the innovative tool, served as the building blocks that aided UCDHS to obtain the HIMSS Stage 7 designation and a HIMSS Davies Award signifying excellence and outstanding achievement in the implementation and value of EHR. OPAL has successfully passed several Joint Commission and CMS audits. These regulatory bodies define an objective review and distinguish the system for all its adjudications.

UCDHS’ philosophy to provide EHR access accurately and timely without interfering with patient care was successful only with the direct support of senior executive leadership. A combination of administrative policies and innovative IT tools were effectively embedded into business processes which allow for immediate development of the OPAL tools needed to be successful.
Appendix

**Figure 1 - UCDHS Role Based Access**

Who are our users? What functions do they perform?

<table>
<thead>
<tr>
<th>Role</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anesthesia</td>
<td>17%</td>
</tr>
<tr>
<td>ED</td>
<td>4%</td>
</tr>
<tr>
<td>Nursing</td>
<td>3%</td>
</tr>
<tr>
<td>P-Technical/Clerical</td>
<td>2%</td>
</tr>
<tr>
<td>MD/NP/PA</td>
<td>1%</td>
</tr>
<tr>
<td>Medical Student</td>
<td>1%</td>
</tr>
<tr>
<td>Non-Clinical</td>
<td>1%</td>
</tr>
<tr>
<td>Nursing Student</td>
<td>1%</td>
</tr>
<tr>
<td>OP-Technical</td>
<td>1%</td>
</tr>
<tr>
<td>OP-Nursing</td>
<td>1%</td>
</tr>
<tr>
<td>Pharmacy</td>
<td>24%</td>
</tr>
<tr>
<td>Psychology</td>
<td>3%</td>
</tr>
<tr>
<td>Administration</td>
<td>5%</td>
</tr>
</tbody>
</table>

**Figure 2 – Access Request Timeliness by Month**

![Graph showing access request timeliness by month.]

**Figure 3 - Screenshot of OPAL**

![Screenshot of OPAL software interface.]

**Figure 4 – Customer Satisfaction Data**

Please rate the timeliness at which EMR access requests are processed now as compared to a year ago.

- Much faster
- Somewhat faster
- About the same
- Somewhat slower
- Much slower

**Figure 5 – Project Timeline**

<table>
<thead>
<tr>
<th>Month</th>
<th>Activities</th>
</tr>
</thead>
</table>
| Apr 2009 - Nov 2009 | - Phase I - Created and defined Project Charter for Provisioning  
- Technical and business requirements gathering  
- Developed and deployed interim Domino solution |
| Jan 2010 - Feb 2011 | - Phase II - Created and defined scope for external users  
- Technical and business requirements gathering  
- Developed and deployed interim Access solution |
| Oct 2012 - Apr 2013 | - Phase III - OPAL Development Planning  
- Technical and business requirements gathering  
- Integrate external and internal users into one tool  
- In Scope evaluation of end user experience  
- Application Development |
| Apr 2013 - June 2013 | - Development Complete  
- Unit and User Acceptance Testing  
- ETL's created for access request extraction  
- Integrated the web based processing system  
- Internal P&P created for administrators  
- Go Live |