Managing the Insider Threat: Real-time Monitoring of Access Patterns to ePHI

Mac McMillan (CynergisTek, HIMSS)
Jennings Aske (Partners Healthcare)
Mike Terra (Oracle Corp.)
Daniel Fabbri (U. Michigan)

Agenda

- Mac McMillan – Introduction
- Jennings Aske – A HealthCare Provider’s Perspective
- Michael Terra – A Vendor’s Perspective
- Daniel Fabbri – A Computer Scientist’s Perspective

Introduction

Introduction

Mac McMillan, FHIMSS, CISM
CynergisTek CEO
Chair, HIMSS Privacy & Security Policy Task Force

Why Auditing & Monitoring?

- Pervasiveness of information being made available electronically has resulted in Healthcare becoming a target of cyber-criminals.
- Healthcare initiatives such as health information exchanges, accountable care organizations, electronic health records, mobile devices, networked medical devices, patient portals, etc. increase availability and risk.
- Expansion of those who potentially have access to health information has increased with an average of 150 individuals accessing patient information during a routine hospital stay.
- The explosion of financial and medical fraud and identity theft with the advent of digitization of patient information.
- In general, Healthcare faces bigger risks going forward than the financial or retail sectors. The information retained is more valuable and greater access is expected.
- And of course, its required….

Auditing & Monitoring Today

- Fact: Insider abuse or misuse of privileges is still the number one threat to patient information and large liability for health care providers.
- Fact: Resources and technology (the lack of) are still the primary constraints to auditing and monitoring system and user activity.
- Fact: Most healthcare organizations are still predominantly reactive in their audit and monitoring practices.
- Fact: Auditing and monitoring is predominantly a (regulatory) rule based scenario.
- Fact: Auditing patterns are still focused on a small number of high profile scenarios such as snooping of fellow co-workers, family members, one own record, etc.
- Fact: A very small percentage of accesses are actually monitored or audited.
- Fact: Very few resources exist or are dedicated to this function.

Auditing & Monitoring for Tomorrow

- We need:
- Monitoring platforms that understand healthcare operations and workflows and can identify and alert on inappropriate actions
- Advanced analytical modeling capabilities that permits more complex scenario investigation and reporting, but we also need…
- Healthcare information systems that support auditing and monitoring
- Resources capable of conducting IT audits and monitoring duties

A HealthCare Provider’s Perspective

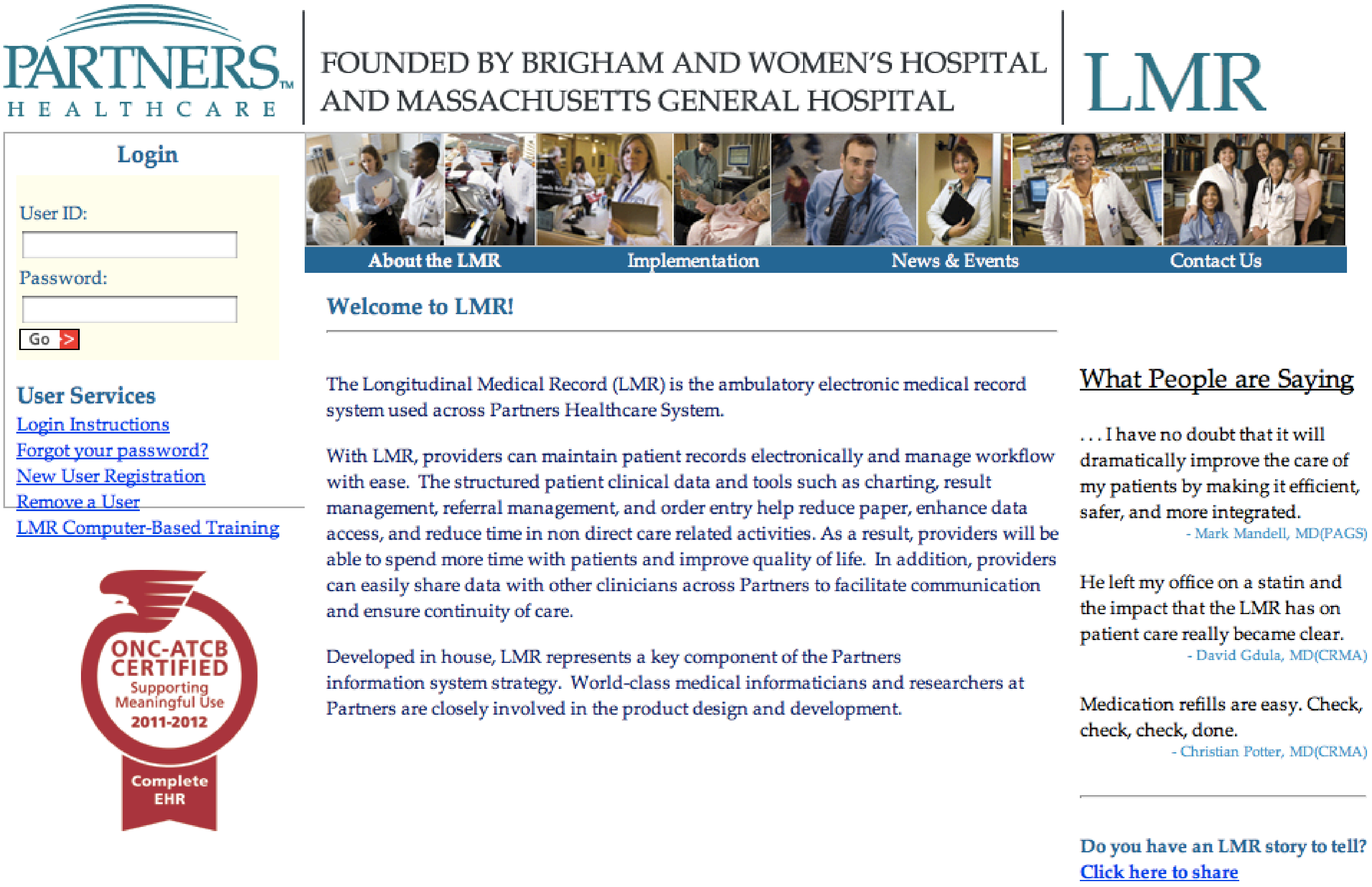
An Automated Approach to Monitoring Access Patterns (MAP) Within Clinical Applications

Jennings Aske, JD, CISSP, CIPP/US
Partners HealthCare System
Chief Information Security and Privacy Officer

Partners HealthCare System Overview

- Partners HealthCare System was founded by Brigham and Women's Hospital and Massachusetts General Hospital in 1994.
- Partners is an integrated health care system that offers patients a continuum of coordinated high-quality care. Partners is also one of the nation’s leading biomedical research organizations and a principal teaching affiliate of Harvard Medical School.
- The system includes primary care and specialty physicians, community hospitals, the two founding academic medical centers, specialty facilities, community health centers, and other health-related entities.
- The Partners system has over 50,000 employees, and includes over 2,500 licensed beds, and over 152,000 hospital discharges

Partners Clinical Application Suite



Login

User ID:

Password:

User Services

Login Instructions

Forgot your password?

New User Registration

Remove a User

LMR Computer-Based Training

ONC-ATCB CERTIFIED Supporting Meaningful Use 2011-2012 Complete EHR

Welcome to LMR!

The Longitudinal Medical Record (LMR) is the ambulatory electronic medical record system used across Partners Healthcare System.

With LMR, providers can maintain patient records electronically and manage workflow with ease. The structured patient clinical data and tools such as charting, result management, referral management, and order entry help reduce paper, enhance data access, and reduce time in non direct care related activities. As a result, providers will be able to spend more time with patients and improve quality of life. In addition, providers can easily share data with other clinicians across Partners to facilitate communication and ensure continuity of care.

Developed in house, LMR represents a key component of the Partners information system strategy. World-class medical informaticians and researchers at Partners are closely involved in the product design and development.

What People are Saying

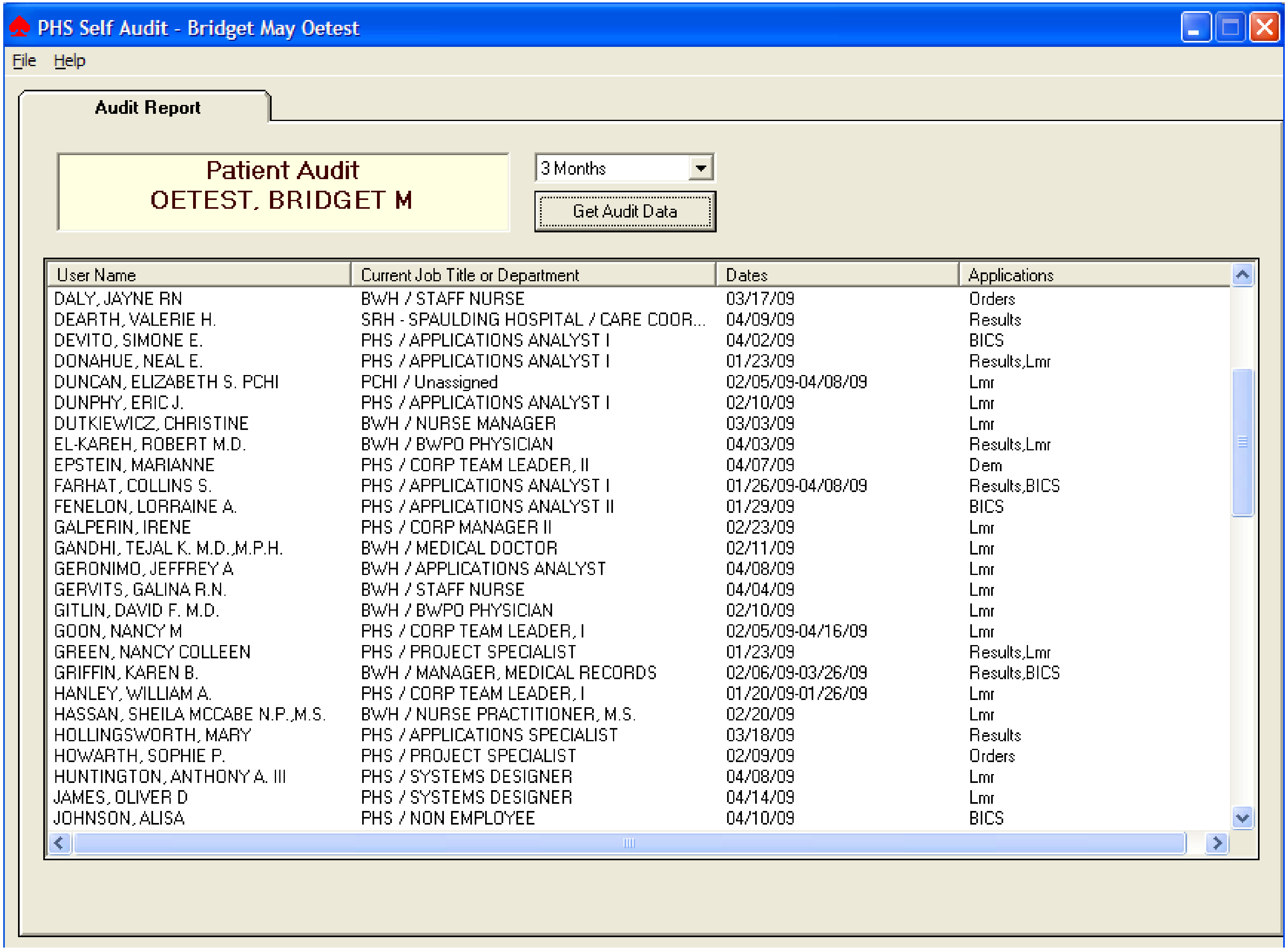
. . . I have no doubt that it will dramatically improve the care of my patients by making it efficient, safer, and more integrated.
- Mark Mandell, MD(PAGS)

He left my office on a statin and the impact that the LMR has on patient care really became clear.
- David Gdula, MD(CRMA)

Medication refills are easy. Check, check, check, done.
- Christian Potter, MD(CRMA)

Do you have an LMR story to tell?
Click here to share

Partners Self Audit Utility

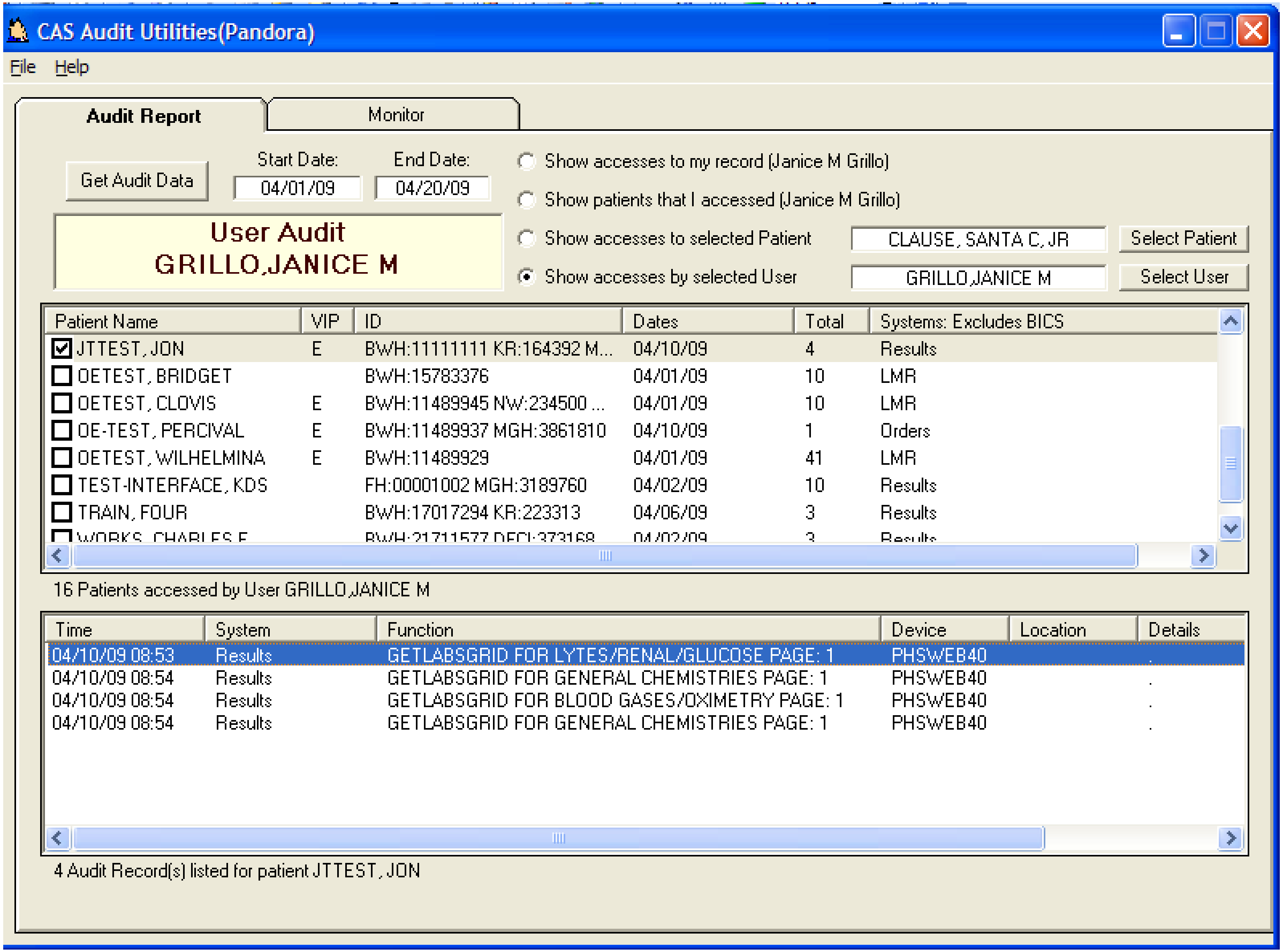


Patient Audit
OETEST, BRIDGET M

3 Months

User Name	Current Job Title or Department	Dates	Applications
DALY, JAYNE RN	BWH / STAFF NURSE	03/17/09	Orders
DEARTH, VALERIE H.	SRH - SPAULDING HOSPITAL / CARE COOR...	04/09/09	Results
DEVITO, SIMONE E.	PHS / APPLICATIONS ANALYST I	04/02/09	BICS
DONAHUE, NEAL E.	PHS / APPLICATIONS ANALYST I	01/23/09	Results,Lmr
DUNCAN, ELIZABETH S. PCHI	PCHI / Unassigned	02/05/09-04/08/09	Lmr
DUNPHY, ERIC J.	PHS / APPLICATIONS ANALYST I	02/10/09	Lmr
DUTKIEWICZ, CHRISTINE	BWH / NURSE MANAGER	03/03/09	Lmr
EL-KAREH, ROBERT M.D.	BWH / BWPO PHYSICIAN	04/03/09	Results,Lmr
EPSTEIN, MARIANNE	PHS / CORP TEAM LEADER, II	04/07/09	Dem
FARHAT, COLLINS S.	PHS / APPLICATIONS ANALYST I	01/26/09-04/08/09	Results,BICS
FENELON, LORRAINE A.	PHS / APPLICATIONS ANALYST II	01/29/09	BICS
GALPERIN, IRENE	PHS / CORP MANAGER II	02/23/09	Lmr
GANDHI, TEJAL K. M.D.,M.P.H.	BWH / MEDICAL DOCTOR	02/11/09	Lmr
GERONIMO, JEFFREY A	BWH / APPLICATIONS ANALYST	04/08/09	Lmr
GERVITS, GALINA R.N.	BWH / STAFF NURSE	04/04/09	Lmr
GITLIN, DAVID F. M.D.	BWH / BWPO PHYSICIAN	02/10/09	Lmr
GOON, NANCY M	PHS / CORP TEAM LEADER, I	02/05/09-04/16/09	Lmr
GREEN, NANCY COLLEEN	PHS / PROJECT SPECIALIST	01/23/09	Results,Lmr
GRIFFIN, KAREN B.	BWH / MANAGER, MEDICAL RECORDS	02/06/09-03/26/09	Results,BICS
HANLEY, WILLIAM A.	PHS / CORP TEAM LEADER, I	01/20/09-01/26/09	Lmr
HASSAN, SHEILA MCCABE N.P.,M.S.	BWH / NURSE PRACTITIONER, M.S.	02/20/09	Lmr
HOLLINGSWORTH, MARY	PHS / APPLICATIONS SPECIALIST	03/18/09	Results
HOWARTH, SOPHIE P.	PHS / PROJECT SPECIALIST	02/09/09	Orders
HUNTINGTON, ANTHONY A. III	PHS / SYSTEMS DESIGNER	04/08/09	Lmr
JAMES, OLIVER D	PHS / SYSTEMS DESIGNER	04/14/09	Lmr
JOHNSON, ALISA	PHS / NON EMPLOYEE	04/10/09	BICS

Partners Audit Utility



Start Date: 04/01/09
End Date: 04/20/09

User Audit
GRILLO,JANICE M

○ Show accesses to my record (Janice M Grillo)
○ Show patients that I accessed (Janice M Grillo)
○ Show accesses to selected Patient CLAUSE, SANTA C, JR
● Show accesses by selected User GRILLO,JANICE M

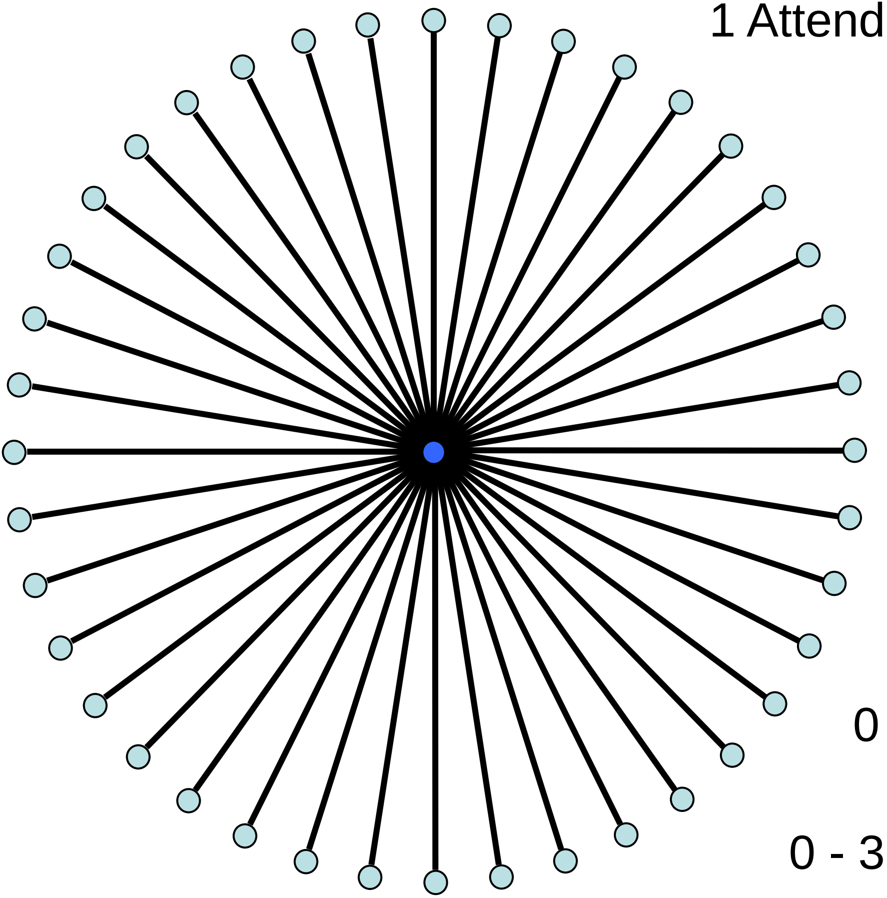
Patient Name	VIP	ID	Dates	Total	Systems: Excludes BICS
☑ JTTEST, JON	E	BWH:11111111 KR:164392 M...	04/10/09	4	Results
□ OETEST, BRIDGET		BWH:15783376	04/01/09	10	LMR
□ OETEST, CLOVIS	E	BWH:11489945 NW:234500 ...	04/01/09	10	LMR
□ OE-TEST, PERCIVAL	E	BWH:11489937 MGH:3861810	04/10/09	1	Orders
□ OETEST, WILHELMINA	E	BWH:11489929	04/01/09	41	LMR
□ TEST-INTERFACE, KDS		FH:00001002 MGH:3189760	04/02/09	10	Results
□ TRAIN, FOUR		BWH:17017294 KR:223313	04/06/09	3	Results
□ WORKS, CHARLES F		BWH:21711577 DFCI:373168	04/02/09	3	Results

16 Patients accessed by User GRILLO,JANICE M

Time	System	Function	Device	Location	Details
04/10/09 08:53	Results	GETLABSGRID FOR LYTES/RENAL/GLUCOSE PAGE: 1	PHSWEB40		.
04/10/09 08:54	Results	GETLABSGRID FOR GENERAL CHEMISTRIES PAGE: 1	PHSWEB40		.
04/10/09 08:54	Results	GETLABSGRID FOR BLOOD GASES/OXIMETRY PAGE: 1	PHSWEB40		.
04/10/09 08:54	Results	GETLABSGRID FOR GENERAL CHEMISTRIES PAGE: 1	PHSWEB40		.

4 Audit Record(s) listed for patient JTTEST, JON

One Hospital Day: 15 - 40 Users/Patient/Day



3 – 6 RN’s

1 Attending

2 - 6 Residents

1 Case Worker

1 – 2 Med Students

3 - 4 Secretaries

0 - 3
RT’s

0-1 OT

0-1 PT

1 – 2 Nutritionists

0 – 2 Consulting MD’s

2 - 3 Pharmacists

0 - 3 Researchers

1 - 3 Coders

1 - 3 Billing

Fundamental Beliefs

- Fundamentally, Partners HealthCare believes most EHR users are doing the right thing, accessing the minimum necessary information to treat a patient.

- Our research shows that the majority of EHR access is patient visit-based:

  - Outpatient, ED and inpatient visits;
  - Providers and support Staff; and
  - Coding and Billing.

- “We expect certain things to happen around visits”.

Real-World Issues

- An employee of a doctor's office used the doctor's password to access medical records on her estranged husband and his new girlfriend.

- 16 hospital employees were fired after looking at the medical records of a hospital employee who was shot in a grocery store parking lot.

- A medical center employee was fired for looking without authorization at the files of 431 patients, including those of acquaintances and neighbors.

- Seventeen hospital workers tried to access the record of former President Bill Clinton as he was undergoing heart surgery at a New York City Hospital.

Business Justification for MAP

- Partners CAS Audit utility does not provide real-time alerts related to unauthorized access. While functional, it is reactive, and not proactive.
- Our hospital’s Privacy Office’s struggle with running and reviewing reports related to access patterns. The CAS Audit was determined to not be a scalable solution in the long-term.
- Patient privacy complaints are the biggest cause of auditing activity, along with care delivered to VIP patients.
- Because of these concerns, Partners asked itself if we could automate audit monitoring similar to how credit card companies monitor for fraudulent transactions.

MAP Research Projects

- Partners proposed that by monitoring ongoing access patterns with near real-time *context* information we could identify potentially unauthorized access patterns.
- Partners engaged Siemens Corporation in two research projects that explored developing this capability. At a high-level, the projects followed a simple methodology:
    - Collect access event data *at the time of access*;
    - Collect user & patient data *near the time of access*;
    - File all data in relational database, connecting users/visits/patients;
    - Utilize data mining to find possible inappropriate accesses;
    - Develop reports collating this information to make actionable reports for privacy office staff to investigate; and
    - Review success of reports (e.g., false positives), iterate and re-iterate.

MAP Research Projects: Methodology

- Critical to the research was the identification of variables that linked EHR users with patients, and inferring the user's reason for access.
- Among the variables that were utilized:
  - Provider match;
  - Clinic match;
  - Care unit match;
  - Hospital match; and
  - Recent visit.
- The research determined that in most cases the presence of these variables meant the EHR user engaged in appropriate access to the patient record.

MAP Research Projects: Methodology

- The research also identified variables that linked EHR users to patients in a manner that *may* be suspicious:
  - Family name and address match;
  - Zip-Code match;
  - Department match;
  - Employee or VIP record; and
  - Deceased patient.

- Our research determined that in many cases the presence of these variables meant the EHR user *may* have engaged in inappropriate access to the patient record.
- These variables we referred to as “snooping variables”.

MAP Research Projects: Methodology

The research led Partners to conclude that the following use cases would be the highest value targets to implement:

- An employee accessing a VIP patient without consent;
- Excessive access by multiple employees of a single patient;
- An employee excessively accessing multiple patient records;
- An employee accessing a neighbor;
- An employee accessing a patient who is a co-worker;
- An employee accessing a patient who is a family member; and
- An employee accessing decedent records.

MAP Research Projects: Lessons Learned

- False positives cannot always be eliminated: many suspicious access patterns that were investigated were determined to be appropriate after investigation. Examples:
  - Employees are patients too and they may receive care from co-workers. A nurse accessing a co-worker’s record was deemed appropriate after it was determined the nurse failed document a flu-shot in the patient’s record.
  - The research suggested that access of a deceased patient’s record was typically problematic if there were no patient office visits, or the patient died, more than one year before the record was accessed. However, false positives occurred during the research due to:
    - A nurse following up on a device (IVC filter) that failed; and
    - A pharmacist doing chart reviews for a drug study.

MAP Research Projects: Lessons Learned

- The EHR is not the only system involved in proactively auditing access patterns. Other systems must be “queried” as part of the underlying data model, including HR systems of record.
  - Employee data is not always accurate (e.g., employee moved to a new home, and has not updated personal information in HR system).
  - Thus, the success of the monitoring is dependent on multiple systems.
- EHR systems generate millions of audit events a week. There has to be a means of “ruling out” specific events *before* the analysis occurs.

MAP Technology Implementation

- After conclusion of the research projects, Partners had to determine the most efficient means of:
  - Implementing the MAP technology; and
  - Operationalizing the investigatory processes.

- During this time, Partners met with Oracle Corporation, which was looking to introduce a fraud prevention platform to healthcare to assist healthcare organizations with proactive detection of potential privacy breaches.
- Partners decided to implement Oracle’s platform rather than develop the MAP technology in-house.
- Partners is currently engaged in an active project with Oracle and Aptec LLC to implement the Oracle Security Governor platform. Initial piloting was positive, and the second phase of this project starts in June 2013.

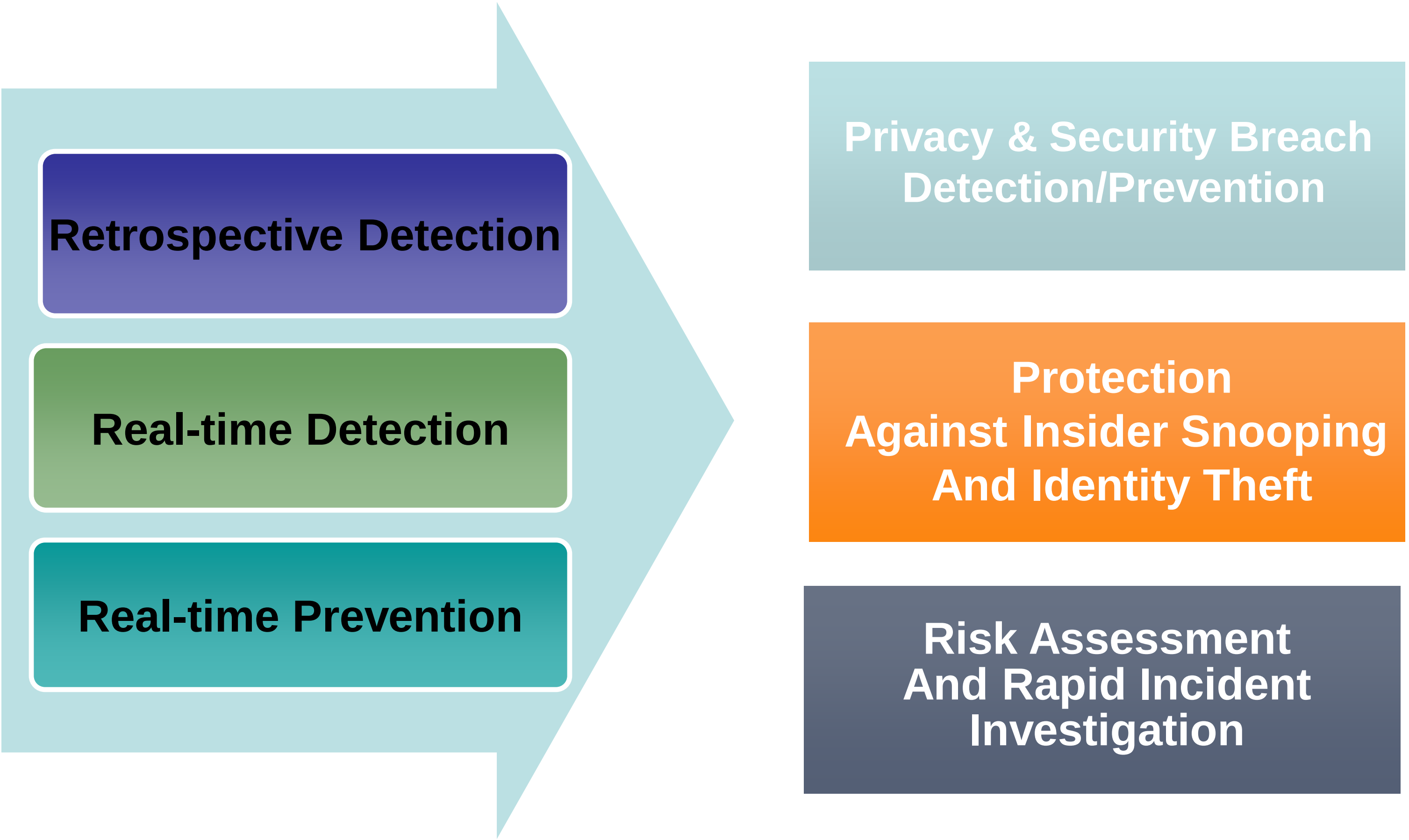
A Vendor’s Perspective

Oracle Adaptive Access Manager

Michael Terra, CISSP
Oracle Corporation
Security Sales Consulting Manager

Oracle Adaptive Access Manager

What does it do?



Retrospective Detection

Real-time Detection

Real-time Prevention

Privacy & Security Breach Detection/Prevention

Protection Against Insider Snooping And Identity Theft

Risk Assessment And Rapid Incident Investigation

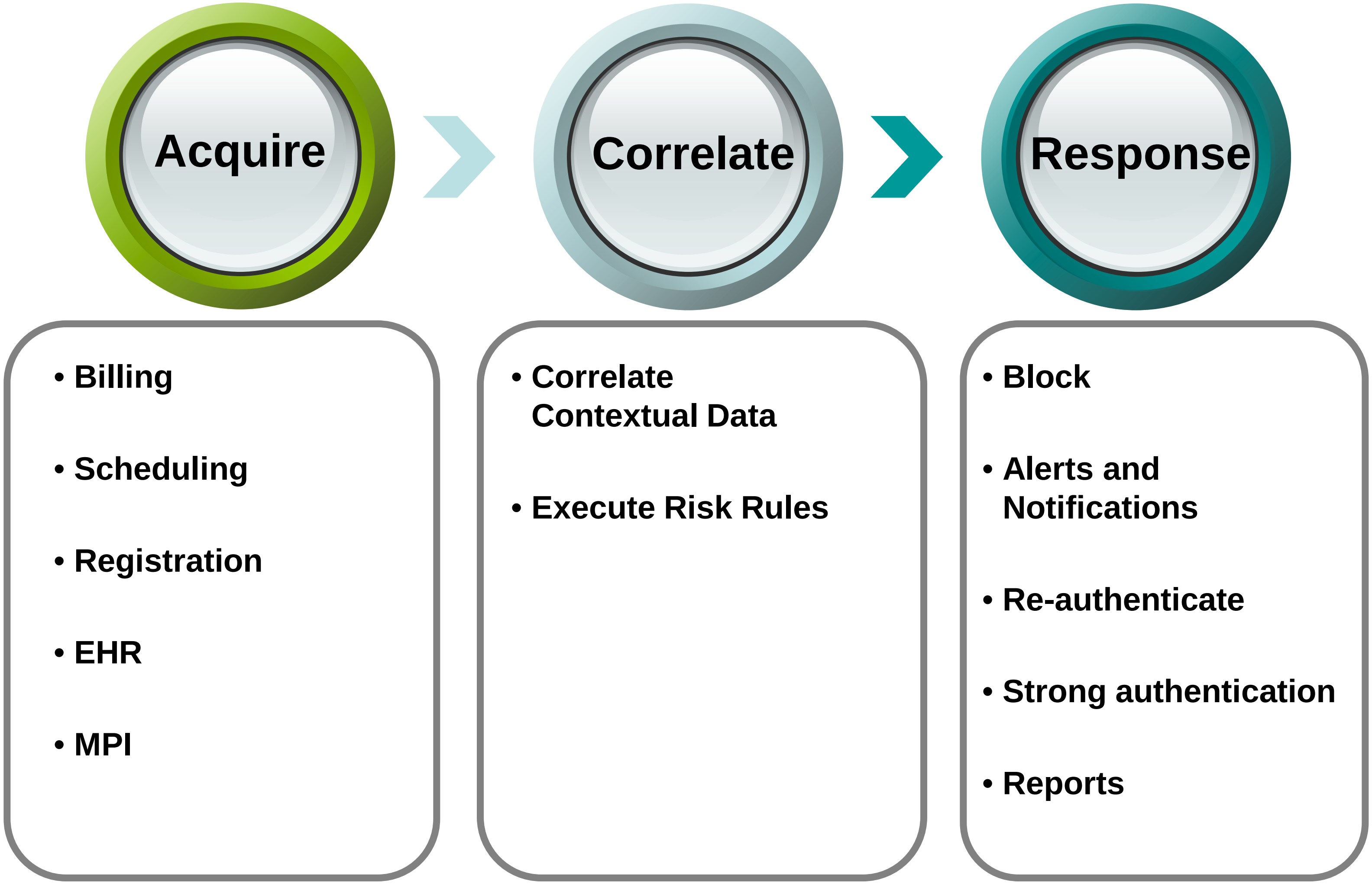
Oracle Adaptive Access Manager

Key Features

- Advanced Risk Engine
- Unique Risk Aware Fine Grained Authorization
- Real-time interdictions
- Integrated in-database data-mining and predictive analytics for anomaly detection
- Automated Privacy Audits via risk-analytics and reports
- Multiple integration options

Oracle Adaptive Access Manager

How does it work?



Acquire

- Billing
- Scheduling
- Registration
- EHR
- MPI

Correlate

- Correlate Contextual Data
- Execute Risk Rules

Response

- Block
- Alerts and Notifications
- Re-authenticate
- Strong authentication
- Reports

A Computer Scientist's Perspective

Explanation-based auditing: Bridging the gap between

complaint-based and real-time audits

Daniel Fabbri

University of Michigan

Computer Science and Engineering

Insider Inappropriate Use

Curious Employees

“`It’s pretty damn common’ for medical professionals to peek at files for unwarranted reasons” [Cotter, 2011].

“Most of the time, the motivation for the snooping is curiosity or concern about a coworker, family member or neighbor” [McGee, 2012].

Challenges of Securing PHI

Complexity of the clinical work environment

- Difficult to specify meaningful fine-grained access control policies
- Employees often have unrestricted access to medical records

  (makes data susceptible to snooping)

Large number of accesses

- Millions of accesses per week
- Manual audits do not scale for patient populations!

  (instead audit are preformed if the patient is a VIP or files a complaint)

Traditional Real-Time Auditing

Alert when ‘suspicious’ accesses occur

- Patient and employee have the same last name
- Patient and employee are co-workers
- Employee accesses more records than normal
- (many other possible *rules* to test)

What happens when there are more alerts than compliance officers can review?

Turn it off???

Complaint-Based Auditing

Patient files a complaint:

- "I believe Alice accessed my record and knows my HIV status."
- "I believe someone accessed my record after my car accident."
- Implicit complaint: a VIP is treated in the hospital

Compliance officers audit accesses:

- Contact employees and team leaders, read clinical notes, etc.
- Determine if each access is appropriate or not
- Manual auditing process can take days and/or weeks

Wasted Manual Auditing Effort

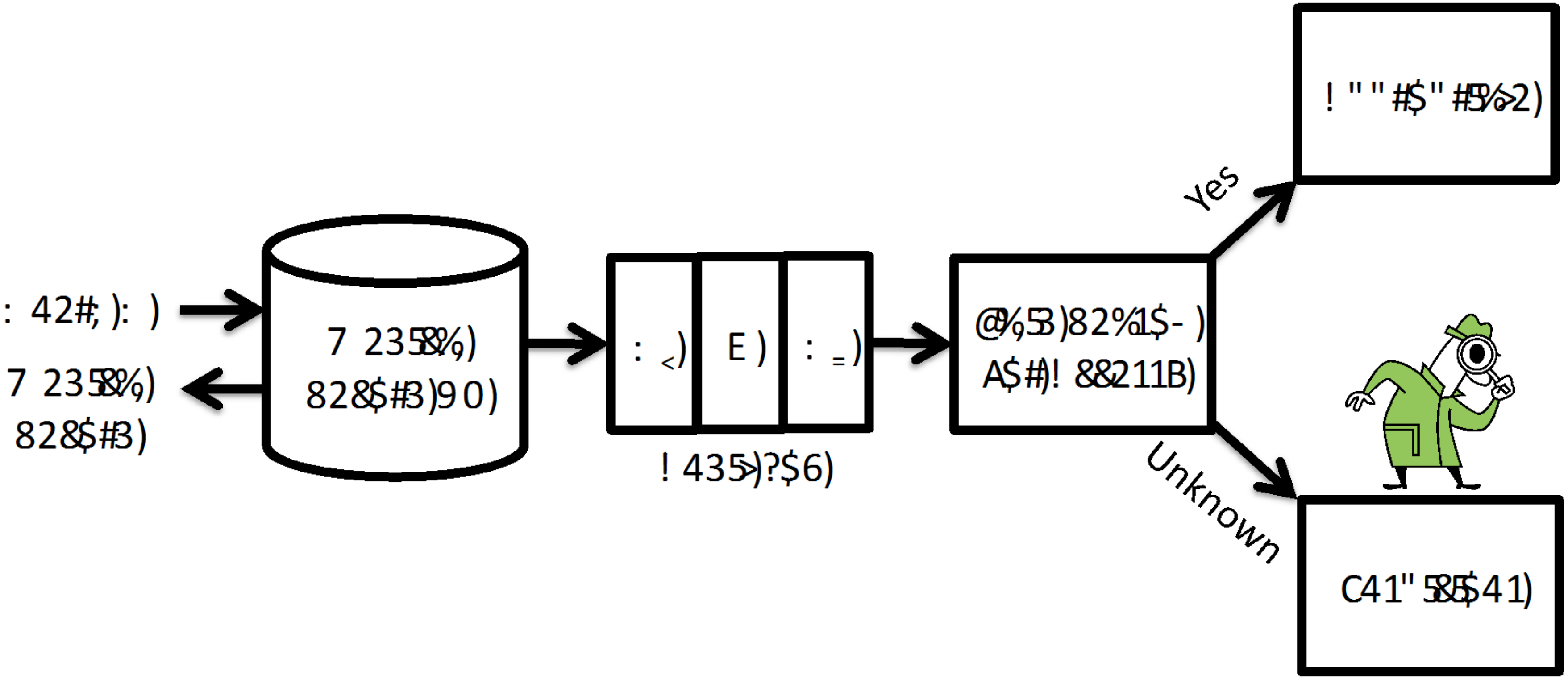
Most accesses are appropriate

- Occur for valid clinical or operation reasons to treat the patient
- Same reasons for access occur across patient population

University of Michigan Health System - Screen Saver

“Authorized access is limited to those with the need to know for purposes of patient care, billing, medical record review and quality assurance.”

Explanation-Based Auditing



Filter appropriate accesses so there are fewer for manual review.

Observation

There are many classes of valid reasons for access.

The main observation of this work is:

EMRs store data describing how a patient is treated, which can be used to explain why accesses occur (patient appointments, medication orders, etc.)

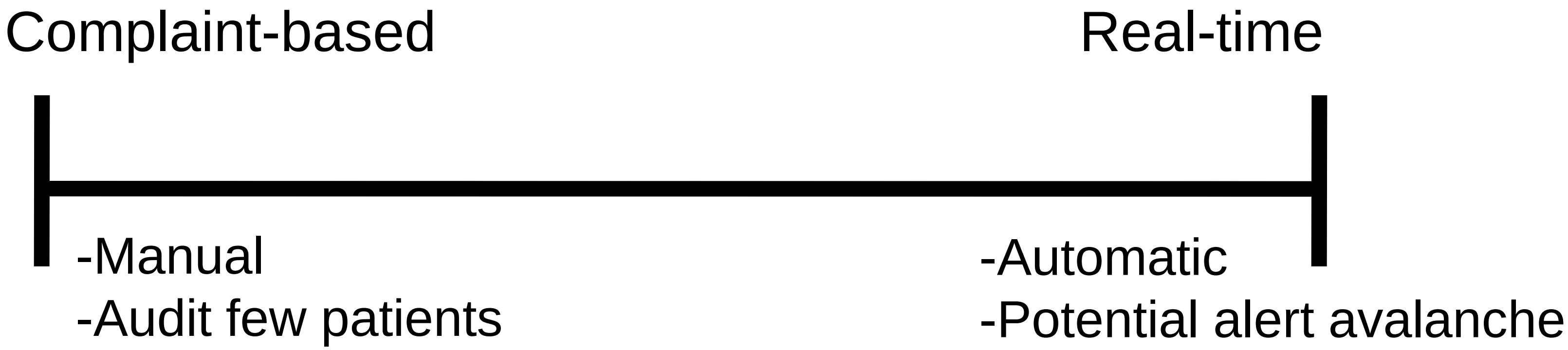
Bridging The Gap

Improve complaint-based auditing efficiency

- Fewer questions to ask and notes to read

Limited scope of audits

- Instead of alerts, compliance officers control what they review



Complaint-based

Real-time

-Manual
-Audit few patients

-Automatic
-Potential alert avalanche

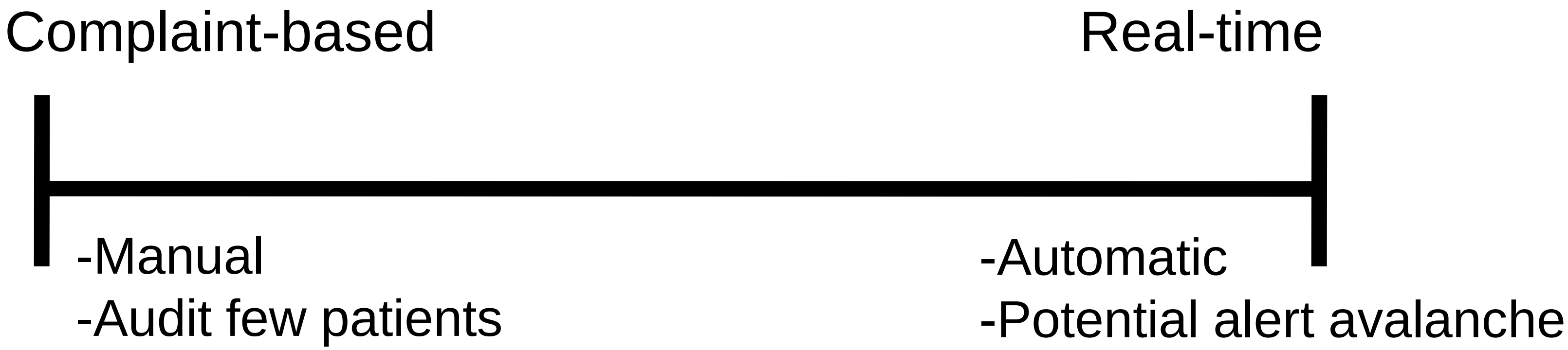
Bridging The Gap

Potential for ‘real-time’ random audits

- Efficiency gains allow for daily random audits
- Audits act as a deterrent for future misuse

Incorporate explanations into (alerting) real-time auditing

- Don’t warn if access occurred as part of valid treatment



Complaint-based

-Manual
-Audit few patients

Real-time

-Automatic
-Potential alert avalanche

Summary

Explanation-Based Auditing

- Filter appropriate accesses that occur for valid reasons
- Compliance officers have a smaller subset to review
- Aim to bridge the gap between complaint-based and real-time audits

Contact Information

- Mac McMillan – mac.mcmillan@cynergistek.com
- Jennings Aske – jaske@partners.org
- Michael Terra – michael.terra@oracle.com
- Daniel Fabbri – dfabbri@umich.edu