Session 4.07 - Accountability for Use or Disclosure of a Patient's Electronic Record

Requirements for a Security and Privacy Audit System

Presented By: John Travis, CPA, MSA, CHFP
Director, Solution Management – Information Security and Patient Privacy
Cerner Corporation

Session Objectives

- To review the regulatory requirement for a system of accountability
- To identify possible sources of standards for what such a system should be
- To define the key goals and objectives for a system of accountability
- To discuss how to determine key events of interest for logging accesses to a record
- To identify key information for logging to an access audit log
- To discuss key requirements for analyzing logged access events

A System of Accountability

- Per the Privacy Rule – the explicit requirement is
  - To provide for an accounting of disclosures of certain types (from any source – paper, electronic, oral)
- Per the Privacy Rule – the implicit requirement is to support monitoring compliance with the Privacy Policy and Practices of the organization

A System of Accountability

- Per the Security Rule – the explicit requirement is to have in place audit control mechanisms to record and examine system activity
  - Entities have flexibility to implement the standard appropriate to the requirements of their own risk analysis
  - Should focus on assessing activities regarding protected electronic health information
  - Clearly distinct from the accounting of disclosures requirement of the Privacy rule – this does not satisfy that but does complement the objective to uphold organizational accountability for use or disclosure of the electronic record per their

Other Perspectives

- ASTM Guidelines (E2147-01)
  - A system of audit for electronic health records should
    - Be designed to provide a precise capability for organizations to see who has accessed patient information
    - Document and maintain a permanent record of all authorized and unauthorized access
    - Support audit of the use or disclosure in accordance with regulatory, legal, accrediting and consumer requirements for accountable privacy practices

Other Perspectives

- Per ASTM E2147-01, An audit system should be (Key items)
  - A record of actions performed on data by users
  - Identify and track user accesses in highly secure logs separate from the subject of the access events
  - Maintain before and after states of content linked to the patient record
  - Record and maintain information concerning breaches of access with notification capabilities
  - Allow for easy retrieval for analysis
  - Provide search capability by user and patient ID, type of data accessed, type of access event, etc
  - Support real time logging and retrieval
  - Help maintain chronology of the state of the access

Other Perspectives

- NIST 800-14 – Principles and Practices for Securing IT Systems
  - Audit Trails
    - Should support individual accountability by tracing user actions
    - Should support reconstruction of user actions by after the fact investigation of how, when and why
    - Should support intrusion detection as the events occur or after the fact
    - Should support problem identification through auditing and monitoring

Other Perspectives

- HL7 – Proposed Common Audit Message Guidelines
  - Key Objectives of Privacy and Security Policy Relevant Data Exchanged Between Systems
    - Provide data to support evidence of compliance with and violations of a healthcare enterprise's security and privacy policies
    - Depict the data that would reside in a common audit engine/database
    - Allow useful queries against audited events

To Sum - Privacy v. Security Accountability

Privacy Interests	Security Interests
-Confidentiality Upheld -Accountability to Patient -Proper Use and Disclosure -Focus on Personal Health Information	-Need to Know Enforcement -Accountability of Authorized Users -Intrusion Detection and Forensic Audits -Recreate the State of the User Access

Where to Start - Scope of Auditing

- What kinds of audit logging do you have today for patient record accesses?
  - For what applications
  - For what types of data
  - How are the audits used
- What policy objectives are supported by this auditing?
- What other audit logging is performed?
  - How is this information used?
- How are changes to reference data audited?
  - How is this information used?

Priority and Scalability of Audit Logging

How much audit information should be logged?

- At what level of depth?
- How should the volume of audit logging be controlled?
- When is full audit logging needed?
- When is exception based audit logging needed?
- How are exceptions defined for logging?

Audit Log Data Requirements

Are there different kinds of audit log entries or events?

For security related audit logging, what data elements are important?

Audit Log Viewing and Analysis - Security

For security related auditing, what routine reviews of audit data are used?

- Review of need to know policy?
- Fine tuning of access controls by organizational unit?
- Policing common kinds of heuristic analysis?
  - What kinds of predefined reports are used?
  - What ones are desired that are not available?
  - How would you want to manipulate the views of data?

When would you prefer an alert or notification to a report?

  - How should the alert occur?

When is sampling appropriate? By what methods?

Audit Log Viewing and Analysis - Security

How do you do pattern analysis of audit data?

- What information is useful for doing pattern analysis?

If you were to set up monitoring for particular kinds of accesses such as abuses or violations, how would you do this?

- When would you do this?

So As To Electronic Systems Maintaining Patient Information

What are some key events that should be audited?

- Authentication Events and Session Events
  - Log on failures
  - Abandoned sessions
- User Security Profile Modifications
- End User Access to Personal Health Information
  - Operations to Create, Modify, Verify/Complete, Error Correct, Query or Print PHI
- How Deep and How Broad?
  - Does the Requirement Differ By Type of System?
  - To What Depth? Persons? Visits? Clinical Data Objects Such As Orders, Results, Documents, etc?

Inventorying What Is Available

- Critical to understand what audit event data sources are there
  - In current systems
    - How do systems represent end user operations?
    - Are they auditable?
    - What data is available?
    - How is it made available for logging?
      - Activity Data State Change Logs?
      - History Logs?
      - Transaction Logs?
    - Do you need a common mapping of an audit schema?
      - Interleafing to one repository?
      - Each patient record keeping solution have its own?
    - Where to reposit the data
      - Separate?
      - Within systems? Problematic for requirement to prevent non-repudiation and obfuscation of audit trails

Auditable Events As Accesses

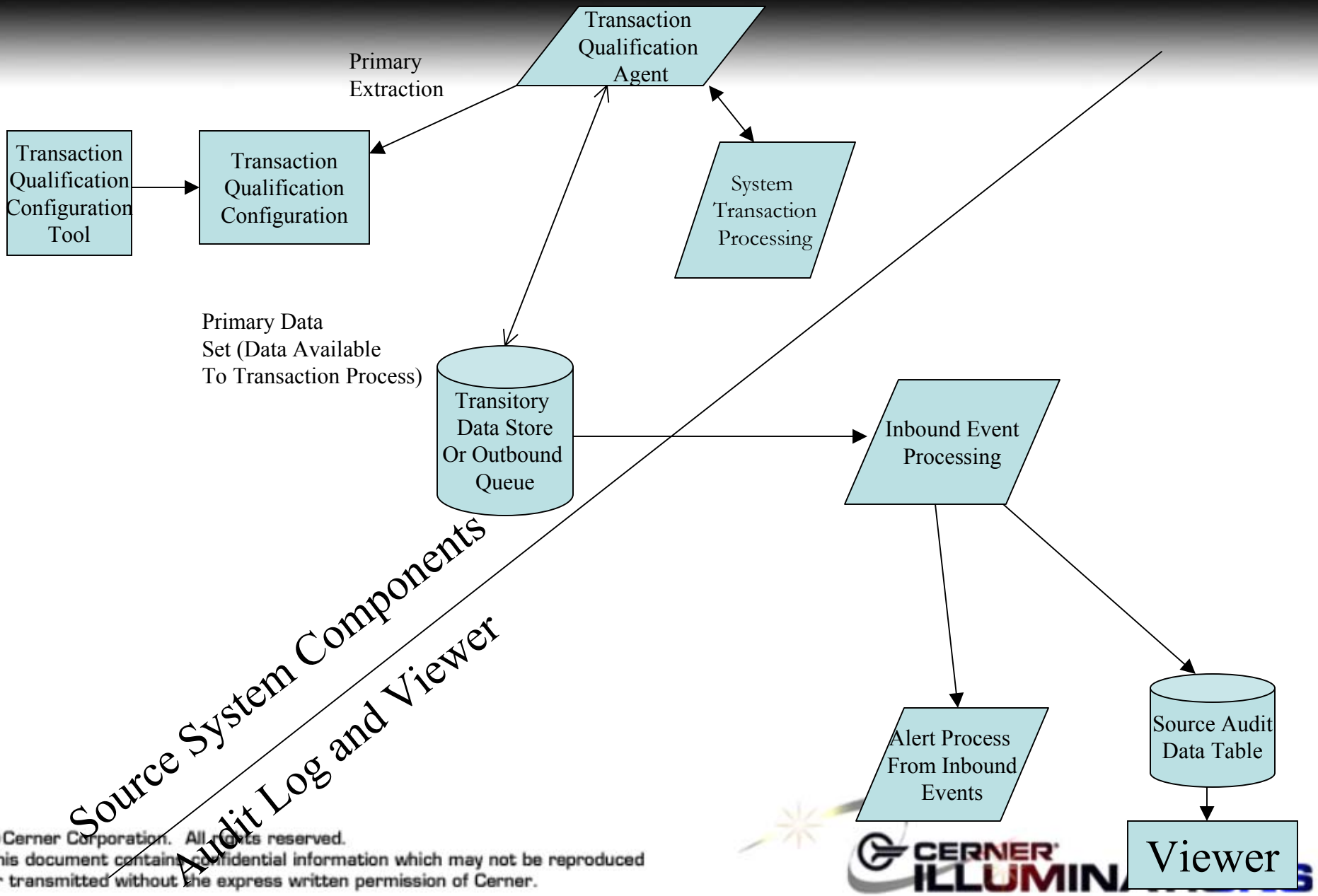
- Auditable Events Can Work to Be Primary Events or Access Paths
  - Person/Patient Searches
  - Clinical Event Accesses
  - Visit Accesses
- Auditable Events Can Work to Be Secondary Events Associated to a Primary Access
  - Reviewing Order History
  - Examining History for a Clinical Document
- Auditable Events Can Be Query Actions Only or Represent End User Operations Upon Data
- Auditable Events Can Be Print or Output Events
- Auditable Events Can Be Ad Hoc Report Writer Accesses

Audit System Overview

Basic Architectural Requirements to An Audit Solution

- Allow for specific events to be identified as those that view/add/modify targeted information
- The healthcare entity needs to be able to determine which of those events are to be audited
- When a user accesses a electronic patient record to commit a particular operation, the system captures information regarding the access through some process understanding of the operation execution for those events tagged as auditable
- The audit event information is passed to an audit repository
- Authorized users can view audit information

Sample Audit Logging Flow



Qualifying Auditable Events – One View

PPRAuditEventManager

Task Configuration View Help

Audit Event Name	Audit Event Type	Requests
View Patient	Retrieve	500280
View Orders	Duplicate Check Indicator	500173
View Orders	Info	500257
View Orders	Ingredient	500261, 500521
View Orders	Lab Status	500265
View Orders	Modify Details	500077
View Orders	Order Comment	500076
View Orders	Order Details	500235
View Orders	Order Flow Info	500332
View Orders	Order History	500078
View Orders	Order Info	500236
View Orders	Order Info Comment	500237
View Orders	Order Info History	500244
View Orders	Order Info Validation	500238
View Orders	Order Item	350030
View Orders	Order Profile	500430
View Orders	Retrieve	500017, 500320, 500415
View List	Orders to Sign	500331
View List	Serum Matches	1065336
View Encounter	Get Best Encounter	600394
View Encounter	Open Chart	100107
View Encounter	Patient-Provider Reltn	500267
Update Login In...	Pathology	265060

For Help, press F1 | DEVTEST_ALPHA | GG6481 | Thursday, December 05, 2002 | 7:26 AM

Qualifying Auditable Events – One View

PPRAuditEventManager

Task Configuration View Help

- Events
  - Abstract Chart
    - Abstract
      - 1120040
  - Access Encounter
    - Visit Summary
      - 600343
    - Radiology Mammo Study
      - 455120, 455121, 455122, 455123, 465011, 465022, 465023, 465025, 465065, 465066, 465099
    - Radiology Folders
      - 425017, 425034, 440003, 440011, 440018, 440032, 440047, 440049, 440050, 440053, 440058, 440064, 440065, 440073, 4...
    - Radiology Exams
      - 400176, 400181, 440013, 440017, 440109
    - Radiology
      - 400131, 400230
    - Pathology
      - 250212, 1037502, 1037508
    - Information
      - 114604
  - Access List
    - Transfer List
      - 265092
    - Reserved Pathology Cases
      - 200050

For Help, press F1 | DEVTEST_ALPHA | GG6481 | Thursday, December 05, 2002 | 7:27 AM

Some Typical Basic Analysis of Audit Events

Access by Patient

Access by Encounter

Access by User

Access by VIP Patient

Access by Confidential Patient

Access by PC Location

Access by Relationship Type to Patient

Access by Audit Event Type

Some Key Types of Audit Log Data Columns

Event Date & Time
Outcome Indicator
User ID
User's full name
User's position/role
Application
Task/Function
Person ID
Person name
VIP code

Encounter ID
Organization of Encounter
Medical Service
Location
Encounter Confidentiality
Encounter Type
Encounter Status
Admit date & time
Discharge date & time
Encounter MRN
Encounter FIN

Reason for relationship creation
Relationship creation date/time
Relationship created by
Relationship creation type
Relationship type
Participant Object Data Set
- Type
- ID
- Alias
- Operation

Possible Examples of Relating Events to Views and Analysis Uses

View Type	Significant Events	Key Uses
Accesses by Person	Person Searches, Person Inquiries through Registration or Common Searches	Monitor Access Patterns to Persons, Monitor Possible Surfing
Accesses by Visit	Relationship Access, Visit Inquiries through Registration or Common Searches	Monitor Access Patterns to Visits, Monitor Differences in User and Patient Location
Accesses by User	Person Searches, Visit and Person Inquiries, Clinical Data Accesses	Monitor Access Patterns by a User, Examine Possible Suspect Cases. Monitor Time of Day Access Issues
Accesses by Device	Person and Visit Accesses	Monitor Differences in User and Patient Location
Accesses by Event Type	Person Searches, Relationship use, Person and Visit Accesses, Sensitive Clinical Event Accesses	Monitor Sensitive Clinical Event Accesses, Monitor Suspect Access Events by Type
Accesses to VIPs	Person Inquiries through Registration	Monitor Accesses to Sensitive Persons
Accesses by Relationship Type	Self Declared Accesses, Proxies, Administrative Relationships, Overrides	Monitor Use of Self Declaration and Overrides, Monitor Use of Proxies
Accesses to Confidential Visits	Visit Inquiries through Registration	Monitor Accesses to Sensitive Visits

Possible Examples of Relating Key Filtering or Searches to Views

View Type	Filtering or Search Criteria
Accesses by Person	To a specific person, To a specific person by a user, To a specific person by time period, etc
Accesses by Visit	To a specific visit, To a specific visit within a time period, To a specific visit other than by certain relationships
Accesses by User	By a specific user, By a specific user of a particular event type, By a specific user to a person or visit, By a specific user within a time period
Accesses by Device	By a specific user, By a specific user to locations not expected, At certain time periods
Accesses by Event Type	For specific event types, For specific event types to particular sensitive data, For specific event types to particular sensitive data by users within or not within certain positions
Accesses to VIPs	By a specific user, For a time range, By users not within certain positions
Accesses by Relationship Type	For overrides, for self declared relationships, By specific users to specific patients
Accesses to Confidential Visits	By a specific user, For a time range, By users not within certain positions

The Importance of a Search Engine

DataShield - Search - Advanced - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites Media

Address http://192.168.1.251/datashield/cgi/index.cgi?

Go Links

CERNER

Home | Cerner Reports | Accounts | Resources | Reports | SecureTrack | Site

LOGOUT

Advanced Search : Users

Search on : Users Submit

Display Columns

Name
Service
Region
District
Location
Address Line 1
Address Line 2
City
State/Provence
Zip Code

Search Criteria

Join	Column	Op	Search Data
	Name	LIKE	
AND	Name	LIKE	
AND	Name	LIKE	

View 20 results per page

Search | Results Only | Undo
Remove A Field | Reset | Add A Field

Search Name : Users
Save

Name	Service	Region	District	Location	Date/Time Created	Status
System Administrator	Web				July 17/2003: 12:35:11	Active
Security Administrator	Web				July 17/2003: 12:35:11	Active
Audit Administrator	Web				July 17/2003: 12:35:11	Active
Web Administrator	Web				July 17/2003: 12:35:11	Active

Edit Access Go

Done Internet

Sample Report View

Case Tools

What do you do with audit data when you suspect an abuse?

- How do your auditors document investigative steps?
  - How are findings documented? Recommendations?
- When you have a suspected violation, how does this get reported?
  - To whom? In what format?
- How does the recipient of the notification respond?
  - Does this get documented?

If you have to respond to an internal or external auditor, how do you show them you have an effective system for identifying suspected violations?

Sample Case Tools

Summary

- Important to have policy objectives in mind for use of audit system
- Critical to understand what audit event data sources are there
  - In current systems
    - How do systems represent end user operations?
    - Are they auditable?
    - What data is available?
    - How is it made available for logging?
    - Do you need a common mapping of an audit schema?
    - Where to reposit the data?
  - Analytical Requirements?
    - What kinds of views do you need?
    - Do you need to be able to define case studies?
    - Do you need alerting?

Sources

-ASTM Citation – E2147-01 – Audit and Disclosure Logs for Use in Health Information Systems (http://www.astm.org)

-HL7 Citation – Common Audit Message – HL7 Security and Accountability Working Group (www.hl7.org)

-NIST 800-14 – Generally Accepted Principles and Practices for Securing Information Technology (http://www.itl.nist.gov/lab/specpubs/sp800.htm)

-Common Criteria v 2.1 – Functional Requirements – Section 3 – Security Audit (http://csrc.nist.gov/cc/Documents/CC%20v2.1/p2-v21.pdf)

Questions?

My Contact Information

John Travis
Director, Solution Management
Information Security and Privacy
Cerner Corporation
jtravis@cerner.com
(816)201-1465
Fax: (816)571-1465