Agenda

- Purpose of Audit Logging
- Non-Coordinated Audit Logging
- Structured/Coded Audit Log Capture
- Accounting of Disclosures or Access Report
- FHIR as a SecurityEvent Resource
- Relationship to USA Meaningful Use
# NIST 800-53 Control Families

## 18 Families related to Security

<table>
<thead>
<tr>
<th>Access Control</th>
<th>Media Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Awareness and Training</td>
<td>Physical and Environmental Protection</td>
</tr>
<tr>
<td>Audit and Accountability</td>
<td>Planning</td>
</tr>
<tr>
<td>Security Assessment and Authorization</td>
<td>Personnel Security</td>
</tr>
<tr>
<td>Configuration Management</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td>Contingency Planning</td>
<td>System and Services Acquisition</td>
</tr>
<tr>
<td>Identification and Authentication</td>
<td>System and Communications Protection</td>
</tr>
<tr>
<td>Incident Response</td>
<td>System and Information Integrity</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Program Management</td>
</tr>
</tbody>
</table>

## 8 Families related to Privacy

<table>
<thead>
<tr>
<th>Authority and Purpose</th>
<th>Individual Participation and Redress</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accountability, Audit, and Risk Management</td>
<td>Security</td>
</tr>
<tr>
<td>Data Quality and Integrity</td>
<td>Transparency</td>
</tr>
<tr>
<td>Data Minimization and Retention</td>
<td>Use Limitation</td>
</tr>
</tbody>
</table>
## NIST800-53 - Audit and Accountability

<table>
<thead>
<tr>
<th>Audit and Accountability</th>
<th>AU-1</th>
<th>AU-2</th>
<th>AU-3</th>
<th>AU-4</th>
<th>AU-5</th>
<th>AU-6</th>
<th>AU-7</th>
<th>AU-8</th>
<th>AU-9</th>
<th>AU-10</th>
<th>AU-11</th>
<th>AU-12</th>
<th>AU-13</th>
<th>AU-14</th>
<th>AU-15</th>
<th>AU-16</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit and Accountability Policy and</td>
<td>P1</td>
<td></td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
</tr>
<tr>
<td>Procedures</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit Events</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Content of Audit Records</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit Storage Capacity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Response to Audit Processing Failures</td>
<td>P1</td>
<td></td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
</tr>
<tr>
<td>Audit Review, Analysis, and Reporting</td>
<td>P1</td>
<td></td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
</tr>
<tr>
<td>Audit Reduction and Report Generation</td>
<td>P2</td>
<td>Not Selected</td>
<td>AU-6 (3)</td>
<td>AU-6 (3)</td>
<td>AU-6 (3)</td>
<td>AU-6 (3) (5) (6)</td>
<td>AU-7 (1)</td>
<td>AU-7 (1)</td>
<td>AU-8 (1)</td>
<td>AU-8 (1)</td>
<td>AU-9 (2) (3) (4)</td>
<td>AU-10</td>
<td>AU-11</td>
<td>AU-12</td>
<td>AU-12 (1) (3)</td>
<td>AU-12</td>
</tr>
<tr>
<td>Time Stamps</td>
<td>P1</td>
<td></td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
</tr>
<tr>
<td>Protection of Audit Information</td>
<td>P1</td>
<td></td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
</tr>
<tr>
<td>Non-repudiation</td>
<td>P1</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
</tr>
<tr>
<td>Audit Record Retention</td>
<td>P3</td>
<td></td>
<td>P3</td>
<td>P3</td>
<td>P3</td>
<td>P3</td>
<td>P3</td>
<td>P3</td>
<td>P3</td>
<td>P3</td>
<td>P3</td>
<td>P3</td>
<td>P3</td>
<td>P3</td>
<td>P3</td>
<td>P3</td>
</tr>
<tr>
<td>Audit Generation</td>
<td>P1</td>
<td></td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
<td>P1</td>
</tr>
<tr>
<td>Monitoring for Information Disclosure</td>
<td>P0</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
</tr>
<tr>
<td>Session Audit</td>
<td>P0</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
</tr>
<tr>
<td>Alternate Audit Capability</td>
<td>P0</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
</tr>
<tr>
<td>Cross-Organizational Auditing</td>
<td>P0</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
<td>Not Selected</td>
</tr>
</tbody>
</table>
Standards

**ASTM E2147** – Setup the concept of security audit logs for healthcare including accounting of disclosures

**IETF RFC 3881** – Defined the Messaging Information Model (Informative)

**DICOM Audit Log Message** – Made the information model Normative, defined Vocabulary, Transport Binding, and Schema

**IHE ATNA** – defines the grouping with secure transport and access controls; and defined specific audit log records for specific IHE transactions.

**NIST SP800-92** – shows how to do audit log management and reporting – consistent with our model

**HL7 PASS** – Defined an Audit Service with responsibilities and a query interface for reporting use

**HL7 FHIR** - Defined a RESTful binding for the Security Audit Event, and thus provide a Query/Retrieve also

**ISO 27789** – the subset of audit events that an EHR would need
Why have an Audit Log?

- **Why?**
  - “document and maintain a permanent record of all authorized and unauthorized access to and disclosure of confidential health care information in order that health care providers, organizations, and patients and others can retrieve evidence of that access”

- Purpose is support of Security and Privacy

- **NOT:** Medical Records tracking, Error Logs, Performance Logs, procedure logs, quality…
ASTM E2147–Audit Log Content

7. Audit Log Content
7.1 Audit log content is determined by regulatory initiatives, accreditation standards, and principles and organizational needs. Information is needed to adequately understand and oversee access to patient identifiable data in health information systems in order to perform security oversight tasks responsibly. Logs must contain the following minimum data elements:

7.2 Date and Time of Event
7.3 Patient Identification
7.4 User Identification
7.5 Access Device (optional)
7.6 Type of Action (additions, deletions, changes, queries, print, copy)
7.7 Identification of the Patient Data that is Accessed (optional)
7.8 Source of Access (optional unless the log is combined from multiple systems or can be indisputably inferred)
7.9 Reason for Access (optional)
7.10 If capability exists, there should be recognition that both an electronic “copy” operation and a paper “print” operation are qualitatively different from other actions.
8. Disclosure Log Content
8.1 The date, name, and address of the individual or entity to which the information is sent; description of information sent, including patient identity; reason for disclosure; and the identity of the individual handling the disclosure should be logged. For routine or basic disclosure, the following are required:
8.1.1 Date and time of disclosure.
8.1.2 Reason for disclosure.
8.1.3 Description of information disclosed.
8.1.4 Identity of person requesting access.
8.1.5 Identity and verification of the party receiving the information.
8.1.6 Identity of the party disclosing the information.
8.1.7 Verification method of requesting the party’s identity.
Uncoordinated Audit Logs

■ Every System, Device, and Application
  ➢ Different audit logs
  ➢ Different formats
  ➢ Different methods on retention
  ➢ Not formally designed for the task
  ➢ Different functionality for investigation and reporting
  ➢ Not protected from abuse

■ Thus RFC-3881 was born
Security Audit Message

- **RFC-3881 – Defined a Data Model**
  - When a security relevant event happens, the appropriate information is gathered, assembled in a structured package, and sent to a special purpose Audit Record Repository
  - Audit Record Repository supports long term maintenance and reporting

- **DICOM – Finished the Model Normative**
  - Fixed many errors, Defined Schema, and vocabulary
Why an Audit Message?

- **Pull?** – Can be done by pulling proprietary logs and normalizing them.

- **Push – SYSLOG**
  - Model used in Firewalls, Routers, IT services, Unix/Linux, etc
  - Medical Systems – benefit is they don’t need to have audit log security, retention, reporting, and alerting functionality
  - Audit Maintenance and Reporting specialized tools
Example ATNA Audit Message

```xml
<?xml version="1.0" encoding="UTF-8"?>
<AuditMessage>
  <EventIdentification EventDateTime="2010-12-17T15:12:04.287-06:00"
    EventOutcomeIndicator="0"
    EventActionCode="E">
    <EventID code="110114" codeSystemName="DCM"
      displayName="UserAuthenticated" />
    <EventTypeCode code="110122" codeSystemName="DCM"
      displayName="Login" />
  </EventIdentification>
  <ActiveParticipant UserID="fe80::5999:d1ef:63de:a8bb%11"
    UserIsRequestor="true"
    NetworkAccessPointTypeCode="1"
    NetworkAccessPointID="125.20.175.12">
    <RoleIDCode code="110150" codeSystemName="DCM"
      displayName="Application" />
    <ActiveParticipant UserID="farley.granger@wb.com" UserIsRequestor="true"/>
  </ActiveParticipant>
  <AuditSourceIdentification AuditEnterpriseSiteID="End User"
    AuditSourceID="farley.granger@wb.com">
    <AuditSourceTypeCode code="1" />
  </AuditSourceIdentification>
</AuditMessage>
```
Distributed Accountability

- EHR System
- PM
- State run HIE
- ED Application
- Physician Office
- XDS Document Repository
- ATNA Audit record repository
- Community Clinic
- Lab Information System
- Lab Information System
- ATNA Audit record repository
- CT Time server
- ATNA Audit record repository
- ATNA Audit record repository
- ATNA Audit record repository

HIE boundary

State run HIE

Teaching Hospital

ED Application

PACS

EHR System

Provide & Register Docs

Maintain Time

Maintain Time

Maintain Time

September 26, 2013
HL7 PASS-Audit Service

Audit Event Source

Submit Audit Record

Privacy Reporting Component

Retrieve Disclosure Records

Retrieve Audit Records

Only "in-scope" use cases are shown.
Accounting of Disclosures

- ASTM E2147 - 8.1 The date, name, and address of the individual or entity to which the information is sent; description of information sent, including patient identity; reason for disclosure; and the identity of the individual handling the disclosure...

- NIST 800-53 – AR-8 accurate accounting of disclosures of information held in each system of records under its control, including:
  (1) Date, nature, and purpose of each disclosure of a record; and
  (2) Name and address of the person or agency to which the disclosure was made;
FHIR – SecurityEvent

- Security Event
  - Patterned after ATNA
  - DSTU ballot very aligned with ATNA
  - Slightly different XML encoding due to FHIR rules
  - Additionally supports JSON format

- HTTP POST - Alternative to SYSLOG

- Query/Retrieve – Could be used to enable reporting
  - HTTP REST binding for HL7 PASS Audit

- Needs security too, like other FHIR resources
FHIR Audit example

```
<SecurityEvent xmlns="http://hl7.org/fhir">
  <event>
    <type>
      <coding>
        <system value="http://nema.org/dicom/dcid"/>
        <code value="110114"/>
        <display value="User Authentication"/>
      </coding>
    </type>
    <subtype>
      <coding>
        <system value="http://nema.org/dicom/dcid"/>
        <code value="110122"/>
        <display value="Login"/>
      </coding>
    </subtype>
    <action value="E"/>
    <dateTime value="2013-06-20T23:41:23Z"/>
    <outcome value="0"/>
  </event>
  <participant>
    <userId value="95"/>
    <authId value="601847123"/>
    <name value="Grahame Grieve"/>
    <requestor value="true"/>
  </participant>
  <source>
    <site value="Cloud"/>
    <identifier value="hl7connect.healthintersections.com.au"/>
    <type>
      <system value="http://hl7.org/fhir/security-source-type"/>
      <code value="3"/>
      <display value="Web Server"/>
    </type>
  </source>
</SecurityEvent>
```
FHIR – Audit Reporting

Conclusion

- Security Audit informs Privacy Reporting
  - Not: Medical Records Log, Error Log, Procedure Log…
- Plenty of Standards that are all aligned and build on each other
  - Structured and Coded
- Most important to record that security relevant event happened
  - IHE-ATNA (DICOM, RFC3881, SYSLOG)
  - FHIR – In development
- Log Management, Reporting, and Alerting are specialized functionalities
Resources

HL7
* mHealth  http://wiki.hl7.org/index.php?title=Mobile_Health

IHE
* web  http://www.ihe.net/
* IHE Wiki  http://wiki.ihe.net/

DICOM  http://medical.nema.org/standard.html

My blog  http://healthcaresecprivacy.blogspot.com/