Security and Access Control

This page is devoted to discussion and design related to security and access control. It arises from a Developers Forum meeting held June 20, 2013, and includes all the material from the notes of that meeting. During the meeting, we tried to catalog inadequacies of and alternatives to our current access control system as the first step in a process of deciding whether and at what priority we might want to upgrade our current access control system. We welcome peoples' experiences and ideas either in writing or in person.

USE CASES, PROBLEMS AND REQUIREMENTS

1. What standards are we trying to meet? In US, HIPAA and states make the rules; Europe has privacy standards. What about the countries we are working in? Are there minimal good practices that we should try to propagate? UNAIDS/PEPFAR have issued security and privacy guidance. US FDA has special requirements for drug trials; as I understand them, they deal more with auditing than with privacy. See Resources below.
2. We would like to have the ability to limit access to patient and encounter data by location. This handles two use cases: (a) a multi-facility installation, either internet connected or synchronized; and (b) a location within a facility with special privacy requirements, typically a psychiatric ward or an STD clinic. We should discuss whether a treating physician (or others) without special privileges should be able to access these records.
3. We would like to have the ability to limit access to patient and encounter data by role. Registration clerks and administrators should not have routine access to patient health data. Do we need to limit access any further? E.g., should community health workers doing programmatic outreach have access to observations/encounters not related to the program?
4. We would like to have the ability to limit access to providers who have a relationship with the patient. See the British Medical Association principles in the Powerpoint presentation by Dominic Duggan below.
5. Aggregate reports should always give the same results, regardless of who runs them. This probably requires us to distinguish between reads for the purpose of aggregating and reads for the purpose displaying detail; we might be able to have reporting tasks run as a different, trusted user. Should a registration clerk be able print out a flow sheet?

WHAT DO WE HAVE NOW AND WHAT HAVE WE TRIED

1. Our basic role-based security involves basic SQL CRUD permissions on each table. In addition, we have permissions for viewing/editing forms. We have encountered the same issues described in Dominic Duggan's presentation – many privileges to assign, many facilities avoiding problems by giving people more rights than they should have.
2. Restrict by roles module https://modules.openmrs.org/modules/view.jsp?module=restrictbyrole. This is currently unsupported and apparently did not work quite as desired. It can do both location and role limitation if each location is given its own role.
3. In OpenMRS 1.10 it is possible to define a privilege required to view or edit an encounter. TRUNK-3377
4. A prototype implementation of the British Medical Association (BMA) security model was created as part of a senior design project. See this wiki page..
5. Lasantha Ranaweera created an XACML version of OpenMRS, see the discussion at https://groups.google.com/a/openmrs.org/forum/?fromgroups#!topic/dev/ZABGquZ8vdg and the Resources below
6. Philip Fong and Syed Zain Rizvi have implemented a Relationship-Based Access Control (ReBAC) system in OpenMRS. An important feature of ReBAC is the explicit tracking of relationships between individuals in the system, and making authorization decisions based on these relationships. Role-Based Access Control (RBAC), which OpenMRS implements, provides a reasonably robust mechanism for restricting access to information; however, OpenMRS does not yet have a mechanism for restricting access to specific data (e.g., a clinician is allowed to access the record of patient X, but not patient Y; or, a clinician is permitted to access a patient's data except for specific lab results). An important feature of ReBAC is the explicit tracking of relationships between individuals in the system, and making authorization decisions based on these relationships. See Resources below.

ALTERNATIVES

Dominic Duggan made a presentation which is attached to this page and available here.

RESOURCES

Information on HIPAA

- http://www.secureworks.com/compliance/hipaa/
- http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2528047/figure/fig1/

UNAIDS/PEPFAR Confidentiality and Security Guidelines

- http://data.unaids.org/pub/manual/2007/confidentiality_security_interim_guidelines_15may2007_en.pdf

Relationship-based Access Control

- General Information on REBAC methodology
- ReBAC Source Code

General information on XACML

- https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml
- http://en.wikipedia.org/wiki/XACML

Lasantha Ranaweera's implemention of XACML for OpenMRS

- Introductory video http://www.youtube.com/watch?v=vdQZEDOWnA0
- http://xacmlauth.googlecode.com/files/UserGuide.pdf
- http://xacmlauth.googlecode.com