

Content Management, Identity Management and eHealth – A Whitepaper

Author: Guy Huntington, President, Huntington Ventures Ltd.

Date: February 17, 2009

Table of Contents:

Table of Contents

Content Management, Identity Management and eHealth – A Whitepaper.....	1
Current Problems:.....	2
Content Management and Protocols.....	3
Fax, Paper and eHealth	4
Emergency Access.....	4
Summary	5

Current Problems:

I will pose the current problems eHealth initiatives face using three personal stories:

1. Paul and Suzanne are a husband and wife team of doctors, operating a small practice with two other doctors, and are my physicians. When you walk into their office there is a large wall containing all their patient's medical records contained in folders. Their technology consists of a computer, fax machine and phones. It is unlikely that they will soon digitize their records and adopt any eHealth initiative requiring them to invest money in technology.
2. Several years ago I traveled every week to Richmond, Virginia. I got to know a seat mate on the plane. Like me, she was a consultant, who was leading deployment of a digital health system for a hospital that did heart procedures. She told me all about her project. When I asked her how they interacted with other enterprises outside the hospital digitally, she rolled her eyes. They were back to using fax machines, couriers and paper.
3. I worked on the identity management project at Kaiser Permanente. I sat beside their security architects. They were wrestling with providing content management security for doctors in their hospitals. The doctors told them that when they walked into an emergency room, they and their nurses required all access to medical records. They ended up using proximity badges which is a weak form of security to accomplish this.

These three stories indicate the challenge in designing an eHealth system:

- Must scale from paper to electrons and back to paper again
- Must allow for multiple interactions between disparate health agencies and enterprises
- Must allow for security exceptions to be made in emergency situations

If you read HL7's Electronic Health Record – System Functional Model, Release 1 – Chapter Five; Information Infrastructure Functions, it talks about things like "An EHR-S should support Chains of Trust in respect of authentication, authorization, and privilege management, either intrinsically or by interfacing with relevant external services" and "Both users and applications are subject to authentication. The EHR-S must provide mechanisms for users and applications to be authenticated. Users will have to be authenticated when they attempt to use the application, the applications must authenticate themselves before accessing EHR 4 information managed by other applications or remote EHR-S'. In order for authentication to be established a Chain of Trust agreement is assumed to be in place. Examples of entity authentication include: - username/ password, - digital certificate, - secure token, - biometrics". All of which is a great goal but unachievable using today's technology. Why?

First of all it assumes that everything will be digital. When Paul and Suzanne deal with the digital system, how is the authentication going to be enforced?

Second, there are two main problems in content management systems today:

- You can't transfer a security policy from one content management system to the other
- The only way to enforce a content management security policy is to place foreign software agents from the content management system you're interacting with on your network

This results in people checking content out of a content management system and then emailing or faxing the documents to others. Further, given the wide number of people, departments and health agencies involved in a patient's care, it is very hard to provide chain of custody for a document that passes between numerous enterprise hands since it would require numerous content management software agents to be installed on all enterprise networks.

This paper seeks to address these problems. It will provide answers to these challenges.

Content Management and Protocols

Two years ago, I proposed an innovative solution to the current limitations of content management systems:

1. That Liberty Alliance, a non-profit standards organization, would develop a generic XML schema for content management security policies. This would allow for transfer of content management security policies between different content management vendors. Further, I then proposed that industry vertical XML schemas be developed. Healthcare is an obvious one and for which I proposed that HL7 would be the lead.
2. That XACML (eXtensible Access Control Markup Language)(an OASIS open standard) be extended to act as the universal content management enforcer for all content management systems. This would negate the use of external software agents. It would enforce the authentication, authorization and audit policies required by the security policy. I saw this as the way forward to provide a auditable chain of custody for all health and other documents.

At the time, I had support from Liberty Alliance but couldn't find a major sponsor for my ideas. Today, two years later, I believe the idea still holds much merit since the problems still remain.

If the Provincial and Federal Government would act as one of the main sponsors, I believe that within a year, the generic XML schema could be in draft form for review along with the HL7 health care XML schema. Within two years, the schemas could be accepted and vendors would be forced by governments and health enterprises procuring products to adopt these into their content management products.

I also believe that within two years, a working pilot could be in place for the first version of the XACML extension. This will take some time to come to agreement on the specs and get a pilot into place. Within three to five years, this could be built into all content management and identity management products.

This addresses two of the three challenges I listed at the beginning of this white paper. However, it doesn't address the third challenge which is illustrated by Paul and Suzanne. How can we design a

system that allows for the vast majority of physicians to participate in an eHealthcare system where they use paper and fax and likely will for many years to come?

Fax, Paper and eHealth

When a doctor's office sends patient information to the hospital, they usually use either fax or paper. I am proposing that they still continue to do so. However, I am proposing that the government develop with the doctors a cover form for the documents. This form should have the privacy conditions for the documentation. In most cases, the doctor or their assistant, will simply tick off or use a standard sheet telling the hospital or lab the privacy conditions. Exceptions need to be spelled out in the form.

When the documentation reaches a Local Health Integration Network (LHIN) or Regional Health District (RHD), they would be responsible for digitizing the content. For example, if it comes in via fax, the LHIN/RHD would use Optical Character Recognition (OCR) on the cover form to automatically assign the document's content management policy. The data is now digital in the form of a fax and can be attached to a workflow engine and/or converted.

When a document is going to be sent to the doctor's office, the reverse would happen. The LHIN/RHD would automatically create a cover letter with the privacy policy. Then the content would either be converted automatically to a fax or printed out and sent to the physician.

This is a system that scales from traditional doctors' offices to complete digital health systems. Is it perfect? No. In the case of a document requiring a digital authentication, the content management security policy must allow for faxing of the document to the doctor's office. However, in this situation, the fax will only be allowed to a specific phone/fax number so some security can be in place to protect the document from being faxed out to others.

Emergency Access

I believe that HL7 will adequately address how digital content can be accessed in an emergency situation. However, I think that the use of paper and faxes needs to be included in their strategy. For example, if a person is wheeled into an emergency room and the doctors need to access the patient's records which are sitting in a file in the patient's doctor's office, then an emergency privacy exception form needs to be used by the doctor's office fulfilling the request.

Summary

I am proposing that the Provincial and Federal Government should:

- Invest their time in developing protocols to allow for content management security policies to be passed between disparate health care systems and to provide for an XACML extension to act as the universal content management enforcer
- Develop with their physicians privacy cover forms for faxes and paper based information
- Develop LHIN/RHD digital collection points which:
 - Convert incoming faxes to digital content with their security policy
 - Convert incoming paper to digital content with their security policy
 - Convert outgoing digital content to faxes and paper with an attached security policy

All of this requires leadership. The Provinces and the Federal Government can be seen as a world leader and take the lead in bringing together other health agencies to work with them on these initiatives.