



**Testimony by David Cochran, MD
President and CEO, Vermont Information Technology Leaders, Inc.**

**For HIT Standards Committee hearing on
Health Information Technology Security Issues,
Challenges, Threats, and Solutions**

**Cybersecurity Panel
Nov. 17, 2009**

Overview

Vermont Information Technology Leaders, Inc. (VITL) is a 501(c)(3) non-profit organization that operates as a public-private partnership. VITL's mission is to collaborate with all stakeholders to expand the use of secure health information technology to improve the quality and efficiency of Vermont's health care system. VITL has been given responsibility by the Vermont Legislature for operating the statewide health information exchange network, which has been in use since early 2007. In addition, VITL has been working with physician practices, hospitals, and other health care providers to facilitate the adoption of electronic medical records, electronic prescribing, and other types of health information technology.

VITL receives funding from several sources. The Vermont Department of Health has a contract with VITL to provide health IT infrastructure for the state's Blueprint for Health initiative, as well as other programs. VITL is able to apply to use the proceeds of a 0.199 percent state fee on health insurance claims that was enacted by the Vermont Legislature to fund health IT projects. VITL has received approximately \$1.5 million in federal grants from the Health Resources and Services Administration, and has applied to be a regional extension center going forward.

The Vermont Health Information Exchange operated by VITL provides several services to health care organizations:

- A medication history service that is active in three hospital emergency departments, delivering approximately 100,000 medication lists to clinicians for consenting patients since 2007.
- An electronic clinical results delivery service that processes approximately 65,000 transactions per month.
- Interfaces which gather data from electronic medical records of physicians participating in the state's Blueprint for Health initiative and deliver the data in a continuity of care document format to a state-licensed registry for care tracking and quality analysis purposes.
- Bi-directional exchange of clinical summaries for consenting patients in the continuity of care document format. This service will be implemented shortly in one area of the state and will be expanded statewide.

In general, VITL's approach is to build its services incrementally. Rather than implementing the above services all at once, VITL started with the medication history service. Once that was operating smoothly, the focus turned to the Blueprint for Health and the clinical results delivery services. Now that those are working well, VITL is expanding into bi-directional exchange of clinical summaries between participating health care providers. Along the way, VITL has looked for opportunities to continuously improve the services that it provides.

Likewise, VITL's approach to cybersecurity is to build incrementally. Rather than trying to implement an extensive and highly complex security system all at once, VITL has chosen to focus first on the fundamentals. As those have been mastered, security systems have been expanded to keep pace with the needs of more extensive data services being provided to health care organizations. As systems have been implemented, VITL has tried to strike a careful balance between the security of data and the ability of authorized users to access the data.

Examples of Security Issues

The biggest issue that VITL has faced in the realm of security is connecting small physician practices to the health information exchange. In Vermont, about 40 percent of the physicians are in solo practices. Another 24 percent are in practices with between two and three practitioners. These small organizations often do not have staff with information technology expertise, nor can they afford to hire expensive IT consultants to assist them.

From a security standpoint, these small practices are potentially the weakest link in the system. If a small practice does not have up-to-date security measures in place, or has let a security measure lapse, that could be exploited by unauthorized parties to gain access to protected data.

VITL has moved to resolve this issue by negotiating partnership agreements with information technology services vendors. The companies will assist Vermont physician practices with managing the security and stability of their networks. Practices will be able to take advantage of preferred pricing negotiated by VITL for network support and disaster recovery services. A vendor will remotely monitor a practice's network and rapidly respond to any security issues from its central operations center. Physician practices will be relieved from the task of designing, building and maintaining a secure network, so they can focus on achieving meaningful use of electronic medical records. VITL will be assured that strong security is in place at even the smallest practices.

Another issue that VITL has faced is installing and configuring virtual private networks and firewalls to maintain data security. This approach has been used successfully at larger hospital and provider group endpoints in the Vermont Health Information Exchange. However, as the exchange is expanded to include smaller practices, the cost and complexity of this approach may prove to be too much.

To resolve this issue, VITL and its HIE prime contractor GE Healthcare are expanding into the use of Transport Layer Security (TLS) and Public Key Infrastructure (PKI) certificates. Placing these certificates on a server used by a participating provider organization, thus creating a node on the Vermont Health Information Exchange, is faster and less expensive than installing a virtual private network and configuring a router.

Trade-Offs and Operational Considerations

As previously stated, VITL realizes it is important to strike the right balance between strict data security and allowing authorized users to access protected data. The trade-off between using one-factor authentication versus two-factor authentication is a case in point.

Two-factor authentication (requiring users to have both a password and a physical means of authenticating their identity) could be preferable from a security standpoint to one-factor authentication of only being required to enter a valid password. However, requiring two-factor authentication would impact HIE usability for providers who move around from place to place within an organization, as it would take longer to gain access to the HIE. It would also increase cost as organizations would have to purchase and maintain the physical means of authenticating identity (e.g. security cards and readers).

The Vermont Health Information Exchange requires one-factor authentication into an “edge” system, which itself has been identified on the HIE network as a secure node. This has been coupled with VITL’s adoption of a security policy (see <http://www.vitl.net/uploads/1254380970.pdf>) which places responsibility on each participating health care organization to ensure that its employees and authorized users are complying with HIE usage policies and the HIPAA Security Rule. VITL believes this combination of one-factor authentication, plus contractual obligations, provides the right balance of security measures and accessibility to data at a reasonable cost.

Another example of a trade-off VITL has made between security and usability is the encryption of data “at rest.” Some states may require that protected health information stored on computers be encrypted. While that requirement may help mitigate the risks of data security being breached, it does place much more overhead on computer systems that serve and consume data. VITL has chosen to focus on protecting the HIE from unauthorized access via multiple methods, including automated intrusion detection systems, node authentication, and placing contractual obligations on participating provider organizations for security and access control.

It should be noted here that the ability of each state or health information organization to make trade-offs does make it difficult to synch systems and exchange data across jurisdictions. The difference between state policies on encryption of data is an example. VITL does urge the HIT Standards Committee to examine this issue and develop national standards that will enable the secure flow of data across states or regions.

VITL has implemented patient authorization and consent using the IHE Basic Patient Privacy Consent standard. The BPPC works well for basic opt-in/opt-out choices, which matches the current VITL patient consent policy (see <http://www.vitl.net/uploads/1254380946.pdf>). It is expected that the IHE BPPC (or any patient preference technology and standards) will need to evolve as the Vermont Health Information Exchange and its use cases proliferate, requiring more sophisticated patient privacy policies. For now, collecting and conveying a simple opt-in/opt-out flag from source systems is challenging, but feasible, and meets Vermont’s patient privacy requirements.

Standards Being Used

At the present time, all connections to the Vermont Health Information Exchange use virtual private networks with private network addresses; strict firewall controls with stateful inspection gateways, default denial of connectivity, RFC compliance with protocol standards, anti-virus and anti-spam services, intrusion detection devices, and limitation of available services.

The Vermont Health Information Exchange is deploying an architecture that meets IHE profiles. VITL’s affinity domain policy covers authorization, role management, definition of functional and structural roles, identity management policy and authentication, attestation and delegation policy, and node authentication requirements.

The VITL security policy requires organizations that connect to the HIE to employ security best practices regarding an internal security policy, asset management, human resources, physical and environmental security, communications and operations management, access control, information systems acquisition, development and maintenance, and information security incident management.

VITL's security policies were developed thru a public process to address security both within the systems that VITL operates and among the various systems that connect to the HIE. This policy is based on the risk assessment protocols in ISO 27001 as well as the HIPAA Security Rule. To support the VITL security policy, the VITL HIE architecture was modeled on several standards and specifications, including:

- IHE ITI Security Cookbook
http://www.ihe.net/Technical_Framework/upload/IHE_ITI_Whitepaper_Security_Cookbook_2008-11-10.pdf
- IHE IT Infrastructure White Paper HIE Security and Privacy through IHE Profiles
http://www.ihe.net/Technical_Framework/upload/IHE_ITI_Whitepaper_Security_and_Privacy_of_HIE_2008-08-22-2.pdf
- HITSP TN 900 Security and Privacy Technical Note
http://hitsp.org/ConstructSet_Details.aspx?&PrefixAlpha=5&PrefixNumeric=900

Other standards used by VITL and the Vermont Health Information Exchange are listed at <http://www.vitl.net/uploads/1257456198.pdf>

Challenges in Implementing Standards

The biggest challenge in implementing the standards that VITL has faced is a lack of knowledge about security among provider organization staffs. Achieving a high level of network security relies upon the parties at either end of the network bringing expertise and skills to the table. This expertise does exist within some Vermont organizations, including hospitals and larger physician practices, and they have made substantial contributions to the rollout of a secure HIE. But with other organizations, VITL has had to provide assistance and guidance, which tends to increase the implementation timeline.

The lack of security expertise within some organizations also tends to affect the internal data security of the organization. They may find it challenging to maintain and support necessary security measures. It is a challenge for VITL to ensure compliance with security standards when the internal policies and procedures of its partners are lacking. VITL's security policy addresses this challenge and requires VITL to do outreach and education to bring partner organizations up to expected security levels. VITL has chosen preferred information technology services partners to support smaller practices and ensure they have access to expert maintenance and support services at affordable prices.

Implementing a PKI certificate infrastructure specified with ATNA Secure Node requires federating the trust relationship for assigning certificates. For example, with very small and remote provider groups there are challenges with authenticating the users' machine and issuing machine-level certificates (and processes for authentication and installation of the certificates for each EMR system).

Current Limitations or Gaps in Standards

The main limitation regarding cybersecurity standards comes not in the standards themselves, but with training on them and the familiarity of provider organizations with the requirements. VITL urges the HIT Standards Committee to examine the resources available for education and training in cybersecurity. If more education for staffs in health care organizations is made available, we believe this will be a large step towards increasing the security of health information systems.

For organizations such as VITL, which do have a good knowledge of the standards, there is a need for a certification process to demonstrate compliance with the standards. A well-run certification program

would highlight organizations that are doing a good job in security, provide assurance to consumers who are served by those organizations, and help identify opportunities for improvement in organizations.

VITL recommends that the HIT Standards Committee examine developing a national certification program for health information security. The Electronic Healthcare Network Accreditation Commission (EHNAC) may serve as a good model for such a certification program, as it has been successfully used to certify healthcare EDI clearinghouses, which have very similar business needs and security risks.

Emerging Cybersecurity Issues

Currently, access to the Vermont Health Information Exchange is limited to authorized health care professionals. However, VITL recognizes the importance of providing consumers with access to their own data on the HIE. In the future, VITL will need to determine how to authenticate patient identities so that they can gain access to their own information and be restricted from accessing anyone else's.

Insofar as there are more granular expectations about incorporating patient preferences into consent and exchange processes, current consent processes may be unable to accommodate. If those expectations vary by state, the challenges will be greater.