OFFICE OF THE Auditor General of British Columbia

Report 7, 2009/10 - The PARIS System for Community Care Services: Access and Security

As at July 2010

Introductory comments from Vancouver Coastal Health Authority

Vancouver Coastal Health Authority (VCH) is pleased to report that 9 out of the 10 recommendations listed below have either been fully or substantially implemented and the remaining one has been partially implemented. With the combination of enhancements to technical security measures, the development of comprehensive information management and security policies, and the creation and implementation of a new access model with stricter controls based on healthcare team membership, need-to-know and user job functions, VCH is confident that PARIS is now more secure than ever.

VCH intends to continue to address all outstanding recommendations to find solutions to enable quality client care while protecting the confidentiality of clients' personal health information.

Recommendations

RECOMMENDATION AND SUMMARY OF PROGRESS	STATUS
Recommendation 1: User access to client records be granted based on the principle of "need-to-know." Doing so will require assessing users' job functions, business workflows, team memberships, profession coding, menu structures, and security levels applied to client records.	Fully or substantially implemented

Actions taken, results and/or actions planned

Significant enhancements have been made to the provision of access to client records based on the principle of 'need-to-know'. These include the implementation of additional functionality and workflows to further restrict access as well as a review to determine appropriateness of access according to job function. A committee has been established to review and implement the response to these recommendations. All (100%) of new team-based groups are implemented in accordance with these new protocols. For current teams, a pilot project was established for three team-based care groups and access changes were subsequently implemented for 85% of these teams. Planning is underway to finalize enhancement changes in the remaining teams. A detailed job function analysis was performed for all clinical and non-clinical users of the three pilot teams and confirmed that need-to-know access was appropriate for all professional staff with reduction opportunities for some program support staff. Appropriate changes to the PARIS access model are being made to reflect these findings.

Recommendations continued...

RECOMMENDATION AND SUMMARY OF PROGRESS	STATUS
Recommendation 2: Multiple layers of security be implemented. In particular: ◆ firewall and router controls should be strengthened; ◆ standards to secure all systems should be developed; ◆ additional firewall layers should be employed; ◆ intrusion detection systems and intrusion prevention systems should be positioned properly; ◆ timely and mandatory system patching should be carried out; ◆ regular vulnerability testing should be performed.	Fully or substantially implemented

Actions taken, results and/or actions planned

The PARIS environment has been secured behind multiple layers of security as follows:
- *Firewall and router controls have been improved to ensure that all changes are recorded and tracked.*
- *Security standards developed (ie hardening guides) and applied to the PARIS environment.*
- *PARIS environment now secured behind internal corporate firewalls in addition to the existing external firewalls.*
- *Intrusion Detection/Prevention systems deployed .*
- *Patch management policies and processes have been strengthened.*
- *Dedicated vulnerability assessment server deployed and used to scan networks and systems.*

Recommendation 3: Comprehensive, up-to-date security policies, approved by senior management, be developed, implemented and enforced.	Fully or substantially implemented

Actions taken, results and/or actions planned

The following policies have been developed or updated and made effective with the approval of VCH senior management as of June 2009:
- *Information Security*
- *Controls for Malicious Code*
- *User Identification and Passwords*
- *Remote Access*
- *Wireless Networks*
- *Internet Access*
- *Records Retention*
- *Access Administration*
- *Role-based Access Control*
- *Cellular and BlackBerry Devices*
- *Standard Software Patches*
- *Acceptable Use of Technology*
- *Printing of Electronic Health Records*
- *Auditing Access to Electronic Health Records*

Recommendations continued...

RECOMMENDATION AND SUMMARY OF PROGRESS	STATUS
Recommendation 4: Databases be secured by: ◆ Restricting database privileges on a "need-to-know" basis; ◆ removing continual access from vendors; ◆ securing roles; and ◆ ensuring that direct access to the database is available only to authorized users through a secure channel.	Fully or substantially implemented

Actions taken, results and/or actions planned

PARIS database security has been improved as follows:
• Database privileges have been reviewed and appropriate restrictions have been applied.
• Vendors no longer have continual access (access granted on a case-by-case, as needed basis only).
• Work ongoing with regards to performing the necessary system upgrades to ensure that database roles can be further secured.
• All direct access to the PARIS database servers is only permitted to authorized users via a management console and only through a secure channel.

Recommendation 5: Controls be implemented to reduce the risk of data leakage. Such controls include: ◆ content monitoring; ◆ audit trail monitoring; ◆ properly isolating and firewalling database servers; and ◆ appropriate access to privileges.	Fully or substantially implemented

Actions taken, results and/or actions planned

The following new data leakage prevention controls have been implemented:
• System deployed to closely monitor and log PARIS database activities.
• Daily auditing in place with plans underway for further enhancements to auditing capabilities.
• PARIS database servers isolated and firewalled behind internal corporate firewalls.
• A review of database roles was completed to ensure they are appropriate and some system privileges were removed from support staff.
Formal processes have been implemented to separate duties of support staff in the development and production environments.

Recommendations continued...

RECOMMENDATION AND SUMMARY OF PROGRESS	STATUS
Recommendation 6: Logs be: ◆ monitored regularly and all pertinent information collected from them; ◆ managed to allow for proper analysis; ◆ secured from tampering; and ◆ positioned properly to ensure they are effective in preventing and detecting attacks, troubleshooting and tracing activity.	Fully or substantially implemented

Actions taken, results and/or actions planned

The logging environment has been improved as follows:
- *Critical logs stored and analyzed by enterprise SIEM (Security Incident and Event Management) system.*
- *SIEM environment collects and correlates logs from multiple sources to allow for quick detection of attacks and configuration problems.*
- *All logs are securely stored in the SIEM environment to protect from tampering.*
- *SIEM environment monitored by IMIS Security Services staff.*

Recommendation 7: To address improper access maintenance: ◆ application, network, operating system and remote access accounts be properly managed to ensure that only authorized users have access; and ◆ processes be followed to ensure access is removed promptly when users no longer require access because of employment status changes.	Fully or substantially implemented

Actions taken, results and/or actions planned

Account management controls have been improved as follows:
- *Remote access account provisioning/de-provisioning processes have been strengthened.*
- *Access maintenance procedures have been enhanced and implemented. Procedures are in place to ensure that PARIS access accounts are managed and documented and that only authorized users have access.*
- *All current PARIS accounts have been validated to ensure accuracy and ongoing processes and procedures have been put in place and/or enhanced to validate the staff membership on PARIS teams with authorized managers/delegates on a regular basis. In addition, processes have been implemented to validate staff access against payroll records and to receive termination notices when a staff member leaves the organization and updates are regularly made in PARIS.*

Recommendations continued...

RECOMMENDATION AND SUMMARY OF PROGRESS	STATUS
Recommendation 8: Access methods that could potentially allow unauthorized entry into the network be removed or secured. In particular: ◆ remote access servers allowing dial-in access should be disconnected; ◆ network access should be disabled for all unaccounted-for laptops; ◆ network access points in common areas should be better controlled; and ◆ VPN access should be properly restricted. **Actions taken, results and/or actions planned** *Network access controls have been improved as follows:* • *Remote Access Servers dial-in servers have been decommissioned.* • *AD accounts for all unaccounted laptops have been disabled.* • *Analysis is ongoing with regards to better securing network access points in common areas.* • *VPN access controls have been strengthened.*	Fully or substantially implemented
Recommendation 9: To address inadequate traffic control on the internal network: ◆ servers should be positioned in different network segments with proper traffic filtering; and ◆ access control restrictions should be implemented to permit only legitimate traffic to reach critical servers. **Actions taken, results and/or actions planned** *The following network traffic controls have been implemented:* • *PARIS database and middle tier servers isolated from the network behind internal corporate firewalls.* • *Access to/from PARIS servers is restricted to only legitimate traffic.*	Fully or substantially implemented

Recommendations continued...

RECOMMENDATION AND SUMMARY OF PROGRESS	STATUS
Recommendation 10: An appropriate record classification, retention and disposal scheme be developed, approved and implemented to identify and subsequently remove or archive records on a regular basis.	Partially implemented

Actions taken, results and/or actions planned

VCH has developed a Records Retention policy as of June 2009 setting out retention periods for various types of records including health records. It also sets out standards for the secure disposal of confidential information contained on various media. VCH has established a committee to explore possibilities for the archiving of information in PARIS. Archiving is not currently a feature available in PARIS and would likely require significant changes to PARIS in order to implement. Any archiving process developed for PARIS must take into consideration that different types of health information will have differing degrees of relevancy over time. For example, immunization histories remain relevant over long periods of time while other types may not. Such archiving processes must also not impede access to historical information where such information is relevant and necessary to a client's care.