3 Health and Wellness: Capital Health and IWK Health Centre Personal Health Information Systems

Summary

Numerous and significant weaknesses in IT controls to protect personal health information contained in computer systems at Capital Health and IWK Health Centre allow an unnecessarily high risk from internal threats. The overall level of control is inadequate and must be improved. We identified IT security vulnerabilities as well as deficiencies in the management of information technology which also need to be addressed.

Stronger controls are required to protect the privacy of personal health information. Both Capital Health and IWK need to improve controls over authorizing, granting and removing access to computer systems; applying security and other software patches; monitoring network activity; and logging system user actions. Encryption of sensitive data and controlling system changes at Capital Health also need to be addressed. These improvements are needed to guard against unauthorized access to health care systems and the potential disclosure, modification or deletion of personal health information.

Control weaknesses unnecessarily increase the risk of inappropriate access and use of Capital Health's computer systems and some of IWK's databases by employees and contract staff. While external hackers are sometimes the more widely-feared threats to computer systems, IT security industry statistics indicate insiders are the predominant threat. In addition, since the primary network used by Capital Health and IWK is also shared with other district health authorities, the risk of inappropriate access to, and abuse of, information by insiders expands beyond the two agencies we audited.

Both organizations need to improve their processes and plans for ensuring continuous operation of computer systems. We recommended better protection of the physical security of their information technology as well as improved preparations for recovering from a disaster that could put information systems, including those dealing with patient care, out of service.

Deficiencies exist in the management of information technology at both organizations. Most of IWK's published policies and procedures are not up-to-date and there is no process to keep them current. While Capital Health conducts some risk assessments as part of its project management process, it needs to implement a comprehensive, overall IT risk management framework to identify, assess and mitigate all significant risks.

At both Capital Health and IWK, there is no periodic assessment of overall IT controls to ensure they are appropriately designed and working effectively.

3 Health and Wellness: Capital Health and IWK Health Centre Personal Health Information Systems

Background

3.1 Capital Health is the largest tertiary health care provider in Nova Scotia, operating nine hospitals and many other health centres and community-based programs throughout Halifax Regional Municipality and the western part of Hants County. IWK Health Centre (IWK) is a tertiary care facility providing care to women, children and families throughout the maritime provinces. These two organizations potentially serve all of Nova Scotia.

3.2 Capital Health and IWK rely heavily on information technology to collect and maintain patients' personal information, monitor patients' health, and record medical procedures and diagnoses. In our view, based on the potential negative health effect that a loss of service could cause, and the hardship and anxiety that patients could be subjected to if their personal health information were exposed to people who have no need to see it, these two health organizations operate some of the most critical information systems in the province. Accordingly, we believe Capital Health and IWK information operations and systems need to be subjected to a very high standard of control. Our audit was designed to determine if they meet this standard, while being cognizant of the organizations' need to not allow IT controls to negatively impact patient health.

3.3 Capital Health's IT Department (eHealth), which consists of approximately 360 staff members, supports over 200 unique computer applications and provides support services to more than 12,000 employees, physicians and learners and approximately 1,900 volunteers. Within eHealth, 160 employees are responsible for managing Capital Health's local area network, servers and desktops, as well as establishing and removing access to the network and most applications. eHealth also provides IT services such as project management to various clinical departments, including making changes to existing technology or introducing new technology into the organization. In some instances, the clinical departments are completely responsible for the management of their own applications and only rely on eHealth to host their systems.

3.4 IWK's Technology, Programs and Services Department consists of 62 employees and supports 19 clinical applications, as well as health services provided by over 3,200 employees and 800 volunteers. They are responsible for managing the IWK local area network, servers, desktops and access to the network and various applications. Clinical departments are not responsible for managing information technology at the IWK.

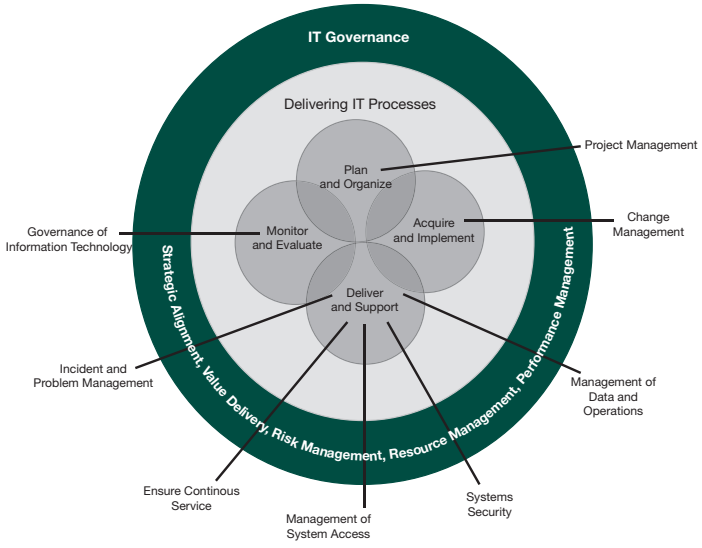
3.5 Information technology services at each entity are supported by Health Information Technology Systems Nova Scotia, which is an entity mandated by the Department of Health and Wellness to provide *"a centralized provincial IT infrastructure to facilitate the delivery of health care in Nova Scotia"*. This includes assisting IWK by managing several IT areas, such as service desk activities, email, wide-area network access and network security.

Audit Objective and Scope

3.6 We completed an audit at Capital Health and the IWK Health Centre in the fall of 2012. The purpose of our audit was to determine if these organizations adequately protect patient health care by minimizing the risk of information security breaches, data corruption and downtime due to disruption of IT services. We examined information technology infrastructure and processes supporting various systems containing personal health information.

3.7 The specific objective of our audit was to assess the adequacy of controls over the development, maintenance and operation of information technology that protects the confidentiality, integrity and availability of electronic personal health information. In conducting the audit, we used criteria from the IT Governance Institute's Control Objectives for Information and related Technology (COBIT 4.1) to assess the IT business processes. COBIT is a widely accepted international source of best practices for the governance, control, management and audit of IT operations. The exhibit below presents the key control areas under the COBIT framework. We addressed each of these in our audit, and report our observations in this chapter.

COBIT Framework



Source: Figure 23, COBIT 4.1

3.8 The audit objective and our use of COBIT criteria were discussed with, and accepted as appropriate by, members of management responsible for the systems we audited.

3.9 Audit fieldwork was conducted in accordance with Sections 18 and 21 of the Auditor General Act and auditing standards established by the Canadian Institute of Chartered Accountants. We conducted our audit between October 2011 and October 2012 on IT process transactions that occurred between November 1, 2010 and November 1, 2011. Adequacy of IT configuration was assessed at various points in time throughout the fieldwork period. We examined supporting operating systems, databases and infrastructure for a sample of 10 significant computer systems containing personal health information at Capital Health, and five at IWK to support our opinions on the organizations' overall management and control of personal health information.

3.10 We did not examine safeguards to prevent external threats to Capital Health and IWK systems through the Nova Scotia Health Network (e.g., firewalls) because they are managed by an external entity – Health Information Technology Systems Nova Scotia – that was not included in the scope of this audit.

Significant Audit Observations

Ensure Continuous Service

Conclusions and summary observations

Capital Health and IWK make a copy of all electronic clinical data so that it can be restored should it become lost or corrupted. Disaster recovery plans for Capital Health are not based on risk or business impact assessments and system prioritization did not consider input from user departments. The IWK's disaster recovery plan is outdated, which may affect its ability to recover from a disaster in a timely manner. Neither organization has tested its disaster recovery plan or provided training to staff on how to implement it during a time of crisis. In the event of a disaster that affects the physical integrity of either Capital Health's or IWK's data centre and its servers, neither entity has a dedicated secondary site which could be used to rebuild systems and restore IT services.

3.11 *Continuous service* – All large organizations require formal plans for the maintenance and restoration of business functions and the information technology that supports them in the event of a disaster. If such plans are not in place, there is a risk that services provided by the organization will be unavailable for an excessive length of time.

3.12 *Capital Health* – There is a process to back up Capital Health's electronic data by storing a copy of it on systems located at the Provincial Data Centre. In addition, some of Capital Health's data is being recorded on tape and taken to a vendor's site. This backed up data can be used to restore Capital Health's systems in the event of

data loss. However, the process to restore data is not documented, which may cause delays in recovering data in the event key personnel are not available to perform the tasks.

3.13 We are also concerned that the Provincial Data Centre, where the copies of data are stored, may be subject to some of the same external risks (e.g., extreme weather events, extended power outages) as the primary site due to their close proximity. Management informed us that there are plans to review a shared resource approach with other hospitals and the province which would result in their data being stored at a secondary processing site that is sufficiently separated from their primary data centre.

Recommendation 3.1
Capital Health should document its data backup and restoration procedures.

Capital Health Response:
Capital Health (CH) accepts this recommendation. CH currently has some procedures which are well documented. CH will consolidate all the procedures and review them with the regular cycle of policy reviews.

3.14 Capital Health's disaster recovery plan is reasonably current; it was last updated in 2010. Our review of the plan identified that no business impact assessment or risk assessment was performed to support the plan's priority of systems to be restored. The prioritization is based on the assessment of eHealth's management without input from the various departments administering and using the IT systems. In addition, the plan assigns estimated restoration times for only the most critical systems.

3.15 There has been no testing of the disaster recovery plan or training for those responsible for implementing it in time of a disaster. Capital Health does not have a secondary location at which it could recover its IT infrastructure if a disaster causes its data centre to be unfit for use. This could be alleviated if management implements the shared resources approach noted above.

Recommendation 3.2
Capital Health should consult with all relevant departments when prioritizing systems for recovery after a disaster.

Capital Health Response:
CH acknowledges this recommendation. CH has a Disaster Recovery Plan dated 2010. This plan will be reviewed and updated to ensure the current classifications in the plan for system recovery are still valid.

Recommendation 3.3
Capital Health should provide adequate testing and training for all significant processes described in its disaster recovery plan.

Capital Health Response:
CH accepts this recommendation and will formalize its testing and training for significant processes. CH currently schedules monthly maintenance on various systems and those systems are taken out of service for maintenance and any updates or fixes, and are brought up within the time scheduled. All departments have downtime procedures and CH has a well coordinated communications plan if the systems will be off line longer than scheduled. In addition CH has testing and training experience resulting from a significant downtime exercise due to major work on the servers. CH's current approach is cognizant of the nature of healthcare and the integration of several systems, specifically the requirement to minimize downtime as a result of impact on clinical programs. CH has demonstrated in several cases that there is an ability to take the systems down and bring them up and to communicate with CH's stakeholders as to the status of any issues. CH will also review its business recovery plan more frequently.

Recommendation 3.4
Capital Health should have a secondary site at which to restore its systems in the event a disaster damages its data centre.

Capital Health Response:
CH accepts this recommendation and has been in planning with the provincial government over the last year to complete a two phase project:

1) *A provincial health project has redundancy of storage between 2 current data centre sites. This is 95% complete.*
2) *To, over time, relocate data processing to the Provincial Data Centre. Planning has started and some applications have recently been set up at that site.*
3) *To work with the province on selection of a secondary recovery site. Due to the number of stakeholders (education, justice, healthcare, finance, etc) the provincial data centre has the lead. CH is working with them to ensure that CH is included. Currently the RFP is being drafted.*

3.16 *IWK* – All five applications we examined at IWK are backed up regularly. Copies of data are sent electronically through a secure channel to the Provincial Data Centre. However, the Provincial Data Centre may be subject to some of the same external risks (e.g., extreme weather events, extended power outages) as the IWK data centre due to their close proximity.

3.17 IWK has produced a disaster, continuance, and recovery plan, but the plan has not been updated since 2003. Management recognizes the need to update the plan. The plan indicates that prioritization of systems is based on a risk assessment; however, that assessment does not identify the risks or the prioritization criteria for systems. A risk assessment and systems prioritization chart was prepared in 2006, but the disaster, continuance, and recovery plan was not updated to reflect the new system prioritizations.

3.18 We also observed that the disaster plan has not been tested and no testing strategy exists. In addition, no training has been provided to IT employees on their roles and responsibilities and the procedures to follow in the event of a disaster. Like Capital Health, IWK does not have a secondary location for its IT infrastructure to recover from a disaster that causes its data center to be unfit for use. Management has indicated the merged services initiative discussed earlier would provide IWK with such a site.

Recommendation 3.5
The IWK Health Centre should update its disaster recovery plan.

IWK Response:
IWK agrees with this recommendation. The IWK has adopted an All Hazards Approach to Emergency Response and has been working with the IWK Emergency Preparedness Coordinator to update the plan to accurately reflect the needs of the health centre. It is recognized that the IWK and HITS NS is in active planning discussions to move the IWK data centre to the Provincial Data Centre in the coming months. Following the move, the IWK Disaster Plan will be aligned with the HITS Disaster Recovery plan. It is anticipated that the IWK Disaster Recovery Plan will be updated by June 30th, 2013.

Recommendation 3.6
The IWK Health Centre should test its disaster recovery plan and ensure IT employees have been trained on their roles and responsibilities.

IWK Response:
IWK accepts the recommendation of testing the disaster recovery plan. Realistic testing of the recovery plan periodically is necessary and can be facilitated through a number of procedures, however full interruption test activities are costly, disrupts normal operations and within healthcare delivery, will increase patient risk and safety concerns, as critical patient care systems would not be available during a full interruption. Disaster planning and testing in health care is very complex and problematic. The IWK will develop and implement testing procedures through structured walk-through testing, checklist testing, simulation testing and table top scenario testing by June 30, 2013.

Recommendation 3.7
The IWK Health Centre should have a secondary site in which to restore its systems if a disaster damages its data centre.

IWK Response:
The IWK agrees with this recommendation. The RFP for a secondary site is expected to be posted later this year by the NS Government. The IWK is aware that the Provincial Data Centre can be subject to the same risks, and this has been mitigated by the IWK backups that are cloned to the provincial data centre are also cloned again to the CDHA data centre. The IWK has three copies of data and also a copy to tape.

The IWK will continue with the planning to move the IWK data centre to the provincial data centre and utilize the IWK data centre as a backup site while the province moves forward with the planning and implementation of a provincial secondary data centre; Meditech will be relocated by March 31, 2013 and the other clinical systems will be relocated by March 31, 2014.

Systems Security

Conclusions and summary of observations

The latest fixes from IT equipment vendors for security vulnerabilities have not been applied to all computer systems at Capital Health or IWK. IWK has not implemented network monitoring or network access controls. Capital Health has implemented network monitoring and controls, but there are weaknesses in its design and operation. There are critical security vulnerabilities because of the configuration and management of IT systems within Capital Health. We identified critical vulnerabilities with some databases at IWK as well. There are weaknesses in the management of physical security of each entity's data centre and related infrastructure. Vulnerability assessments have not been completed at either site.

Network Security

3.19 The IT network which enables computer systems to exchange data needs to be protected by technology that monitors, restricts and reports on data that could potentially be harmful, such as a virus or illicit intrusion.

3.20 *Capital Health* – Capital Health is monitoring network traffic through an external vendor, which provides reports on suspicious behavior. Capital Health has also implemented technology to restrict an individual at one of its computers from attacking other computers containing personal health information. We identified a design and implementation flaw with this protective measure and, as a result, it is not providing the level of security intended.

Recommendation 3.8
Capital Health should re-evaluate its network controls to restrict harmful traffic between systems and mitigate against identified risks.

Capital Health Response:
CH acknowledges this Recommendation which relates, in part, to aspects of the provincial security umbrella. CH agrees to work to comply with the recommendation to the extent possible within its realm of control. CH participates within the provincial health network, a single flat network model design, placing all districts within a single managed domain, which can introduce a threat to each other's operational status.

CH will update its systems/structures by placing computers classed as security threats in a quarantined area and additional security services will be implemented to improve server network to strengthen security.

3.21 *IWK* – The IWK does not monitor network traffic for suspicious behavior and has not implemented technology to restrict an individual at one of its computers from attacking other computers.

Recommendation 3.9
The IWK Health Centre should implement network security measures to monitor and restrict malicious network traffic.

IWK Response:
IWK agrees with this recommendation and has previously submitted the request to purchase a solution, however funding for the solution and the associated human resources was not available given competing clinical care resource pressures. The IWK does monitor for virus and malware utilizing industry standard products. HITS security analysts monitor for malicious activity through nshealth.ca perimeter firewalls. Purchasing and implementing a solution requires appropriate funding for both the solution and the human resource required to maintain the system. As part of Merged Services Nova Scotia (MSNS), HITS will be implementing network access controls over the whole nshealth.ca network which will provide the health centre with the ability to monitor and restrict malicious network traffic. Target implementation for a network access control solution at the IWK would be March 31, 2014.

System Vulnerability

3.22 Systems are vulnerable when they do not restrict access to authorized individuals only, and when they do not adequately protect confidential information. Vulnerabilities can be minimized by:

- using strong passwords that cannot be guessed;
- disabling programs with weaknesses;
- applying fixes to faulty computer code that could allow someone to gain access without the use of a password;
- only allowing people access to information that they require; and
- ensuring sensitive data is encrypted before being sent to other computers.

3.23 *Capital Health* – We examined 10 applications and the 49 computers (servers) and 14 databases that support those applications. We found critical security vulnerabilities that could prevent systems from being available or could allow unauthorized individuals to gain access to personal health information. These include:

- personal health information, and usernames and passwords which are not encrypted when sent between computer systems;
- failure to change default settings in programs that could be exploited, affecting the availability of the application and its data;
- existence of a blank password, which was associated with an administrator-level account permitting full access to personal health information;
- use of vendor-supplied usernames and passwords;
- an employee with computer accounts that are no longer required as part of that employee's roles and responsibilities within the organization;
- systems that do not lock out users who try to crack passwords;
- systems that do not require users to periodically change their passwords according to policy; and
- password settings that permit the use of weak passwords, as well as the actual use of very weak passwords.

3.24 We are particularly concerned about the use of weak passwords. We ran a cracking program for 10 minutes on 18 servers. We were able to crack 363 passwords, out of a total of 2,605 tested. Two of those accounts had administrator-level privileges, which make them more dangerous in the hands of an unauthorized user. Such privileges enable the running of powerful computer programs that could damage systems or expose data.

Recommendation 3.10
Capital Health should better secure its servers and databases by:

- ***increasing the strength of acceptable passwords;***
- ***reviewing for the use of weak or blank passwords;***
- ***disabling, or at least changing the default passwords, for user accounts no longer required; and***
- ***encrypting all sensitive information that is sent between systems if there is risk that it may be viewed in transit by persons not authorized to see it.***

Capital Health Response:
CH accepts this recommendation and will re-evaluate its password management by doing a review of all patient care systems. CH currently balances security risk with the need for care providers to have no significant delays in care. CH will improve the consistency of password management as it relates to strengthening password protocol and more frequent updates of default password. CH does have an encryption email service and will work with its provincial partners to further improve the security on its email system. CH

is currently implementing secure layer on systems as they are approved by vendors. As new systems are acquired and upgrades completed CH will provide documented security standards for all vendor applications.

3.25 *IWK* – We examined five applications and the 12 computers (servers) and seven databases that support those applications. We found security vulnerabilities that could increase the risk of exploitation or allow unauthorized individuals to gain access to personal health information, including the following.

- Use of a database system that is no longer supported by its vendor.
- A database containing personal health information that is not protected from unauthorized copying. Copies of that database can be read using a widely known and available application.
- Users can bypass an application and directly access a backend database which contains personal information.
- Password settings do not require users to have complex or strong passwords.
- Settings allow users to reuse old passwords after they have been changed.
- Settings do not lock out accounts after a number of failed login attempts.
- There are employees with computer accounts that are no longer required as part of their roles and responsibilities within the organization.
- Improper permissions are assigned on shared folders, one of which contained personal health information.

Recommendation 3.11
IWK Health Centre should better secure its systems by adding additional controls or processes to protect databases including:

- ***upgrading or replacing databases that are no longer supported by vendors;***
- ***ensuring only authorized users can copy or move databases; and***
- ***restricting end users from directly querying backend databases.***

IWK Response:
The IWK agrees that the best practice for restricting and securing Microsoft Access databases will require existing databases to migrate to a SQL environment. Our current practice for development of new databases is to utilize this secure environment. Additional human resources will be required to redevelop existing databases. IT will develop policy, procedures and a communication plan to prioritize for redevelopment.

The On Line Service Solution that was implemented in November 2011 is now in Phase 2 of development. Phase 2 is configuring the new functionality whereby staff transfer between internal departments will have an electronic means to notify and receive approval from

managers regarding their removal and additional access to information systems required for new roles.

Recommendation 3.12
IWK Health Centre should better secure its systems by increasing password and account controls which include:

- ***requiring users to use complex passwords;***
- ***preventing users from reusing previous passwords; and***
- ***locking accounts after a number of failed login attempts.***

IWK Response:
IWK agrees with this recommendation which will require additional funding. The IWK utilizes the provincial standard for passwords; therefore introduction of multiple complex passwords for a single care provider introduces risk to patient safety. Physicians and clinical care providers are required to access health systems at the point of care in emergent situations; therefore, balancing timely access to systems with reasonable, intuitive passwords is essential to the safe delivery of patient care.

The IWK is aware that securing systems is fundamental to protecting confidential information. Our aging information systems do not always provide full functionality of preventing users from reusing previously used passwords and locking accounts after a number of failed login attempts. A review of clinical systems is underway to ensure that systems where there is functionality to better control usage of passwords and locking accounts is enforced.

Recommendation 3.13
IWK Health Centre should better secure its systems by restricting access to shared folders to authorized individuals only and reviewing active employee accounts and their permissions on a periodic basis to determine if they are still required.

IWK Response:
The IWK agrees that reviewing active accounts and their permissions on a periodic basis will enhance security and is currently developing policies and procedures to address this requirement. This will be implemented by March 31, 2013.

Patch Management

3.26 Software sold or freely provided by vendors can have flaws that require fixing. These flaws can negatively affect computer system performance and can create security vulnerabilities. Individuals with malicious intent research these flaws and attempt to use them to hack computers. To help prevent this from occurring, vendors routinely provide fixes (patches), or groups of fixes (service packs). Such fixes need to be made on a timely basis to reduce the opportunity for someone to use a flaw to hack a computer system.

3.27 *Capital Health* – We assessed 49 servers and 14 databases to determine if they were updated with the latest vendor fixes. We discovered that 43 of the servers and eight of the databases were not up-to-date with their patches or service packs; some were years behind.

Recommendation 3.14
Capital Health should evaluate, test and install vendor-recommended security patches on a timely basis.

Capital Health Response:
CH acknowledges this recommendation. Capital Health does install vendor recommended security patches when CH can validate that it will not interfere with the clinical functionality/performance of the applications or other systems that are connected. CH has a complex system of applications, interfaces and back end data centre. CH applies patches when they are tested and validated by the vendors and there can be more than one vendor involved. If the OS and applications patches are not supported by a vendor CH evaluates the risk to patient care, operating system and application team will determine the correct source of action. CH makes these decisions after an assessment of the risk. CH will complete an inventory of systems to document patches in place and plans for any outstanding updates.

3.28 While testing the servers and databases, we found that one operating system and seven databases were at the end of their life and are no longer supported by their vendors. As a result, the vendors are no longer releasing patches to fix security vulnerabilities.

Recommendation 3.15
Capital Health should upgrade or replace end-of-life systems to ensure all systems are fully supported by their vendors.

Capital Health Response:
CH acknowledges this recommendation. CH has some (very few) end of life systems which continue to be required from a clinical perspective. CH is working with clinical areas to transition to more current systems.

3.29 *IWK* – We assessed the six databases and 12 servers supporting our sample of applications to determine if they were updated with the latest vendor fixes. We noted four were behind in service packs and six were behind in security patches. Were not able to assess patches on two operating systems because the reports required could not be generated due to vendor restrictions. Four databases were not assessed because the IWK did not have access to, or did not support, the database, or patching was not applicable to the database technology being utilized.

Recommendation 3.16
IWK Health Centre should assess, test and install vendor-recommended security patches.

IWK Response:
IWK agrees with this recommendation. Current process is to update servers with the latest patches on a monthly basis. The exception to this practice is those vendor health systems that prohibit the IT staff to update without vendor approval as clinical information systems are complex and therefore require downtime periods whereby clinical care providers will not have access to patient information while patches are being tested, installed and then tested prior to allowing clinical staff to utilize the system. The IT Department will follow up with those vendors where security patches have not been installed for the above stated reason, to develop the plan for assessing, testing and installing vendor related security patches by December 31, 2012.

Logging and Monitoring

3.30 Computer applications, operating systems and databases often have the ability to log users' actions; this is referred to as auditing. Systems may keep a record of when a person logs into a system or when they view, modify or delete data. These records can be viewed to investigate a suspected security violation, or routinely to look for unauthorized activity.

3.31 *Capital Health* – Of the 10 applications reviewed, only six log user actions. One of those six only logs changes to data; the viewing of data is not recorded. None of the logs are proactively monitored to determine if system users are accessing information that is not required as part of their roles within the organization. No logs were maintained for any of the databases we reviewed which support those applications.

Recommendation 3.17
Capital Health should enable auditing on all patient-related applications that have the ability to do so.

Capital Health Response:
CH accepts this recommendation. While some auditing is currently underway, CH will be implementing Fair Warning and will implement scheduled auditing based on an assessment of risk for patient related applications.

Recommendation 3.18
Capital Health should set a requirement that all new patient-related applications implemented within the organization have the ability to audit user actions, including viewing, modifying and deleting of data.

Capital Health Response:
CH accepts this recommendation. When implementing new patient related applications, appropriate risk assessment will require consideration of the need for the system for specialized and possibly unique services which are of critical importance for patients against the risks associated with a vendor's lack of audit ability.

Recommendation 3.19
Capital Health should, on a sample basis, periodically audit patient-related application logs to determine if users are accessing information that is not required as part of their job responsibilities.

Capital Health Response:
CH accepts this recommendation and as indicated is working with its provincial partners and is implementing a system called Fair Warning. This system will run random checks on the system. It is early implementation stages at CH and CH expects this to be more fully functional in 2013.

3.32 *IWK* – Of the five applications reviewed at the IWK, three of them log user actions. None are being proactively monitored to determine if system users are accessing information that is not required as part of their roles within the organization. Logs for one application were being reviewed, but this was stopped when it was determined that the information in the logs was incomplete. Three supporting databases we reviewed do not maintain logs. We noted that system auditing of user actions is now a requirement for all new databases developed by the IWK. No support was provided to show that this is also required for vendor-supplied applications.

Recommendation 3.20
IWK Health Centre should enable auditing on all systems that have the ability to do so.

IWK Response:
IWK agrees with this recommendation. Various systems have different risks according to the amount of personal health information, sensitivity of the personal health information, the number of users of the system and the frequency of use of the systems. Based upon these criteria, the IWK has prioritized the Meditech HCIS as the highest priority for conducting audits of user activity. The IWK has an audit plan in place and implemented proactive audits utilizing a new provincial audit solution in September 2011. Extensive work between IWK, HITS and the vendor has been underway to address the technical difficulty encountered between the two systems which have extended the go-live date for proactive auditing. The IWK has identified that auditing multiple information systems will require additional human resources to meet this recommendation. Technical difficulties should be resolved by December 31, 2012; with all clinical systems included in a phased in approach by 2014

Recommendation 3.21
IWK Health Centre should ensure that all new vendor-supplied applications implemented within the organization have the ability to audit users' actions, including the viewing, modifying and deleting of data.

IWK Response:
The IWK agrees with the importance of this recommendation and reports that a process has already been established and implemented for more than 1.5 years, whereby all new

Request for Proposals (RFP's) require a Privacy Impact Assessment be completed by the vendor of choice prior to the signing of a purchase agreement.

Recommendation 3.22
IWK Health Centre should, on a sample basis, periodically audit application logs to determine if users are accessing information that is not required as part of their job responsibilities.

IWK Response:
IWK agrees with this recommendation. Audit logs are a record of sequential activities maintained by an application or system. Application logs cannot determine if users are accessing information inappropriately, but rather the IWK requires a complex auditing solution which will identify trends or sequences of events, in concert with additional resources to successfully implement periodic and ongoing monitoring within multiple health information systems.

Currently the IWK Privacy Manager is a representative on a Provincial Audit Policy Working Group which has a mandate to develop a provincial audit policy applicable to all electronic information systems of the Department of Health and Wellness as well as the IWK and District Health Authorities that contain personal health information to ensure alignment with the provisions of the new Personal Health Information Act (PHIA) and its regulations. PHIA is expected to come into effect early 2013.

Physical Environment

3.33 Organizations implement safeguards to physically protect their computer systems. Risks to the physical security of systems come from both people (e.g., accidents or vandalism) and environmental factors (e.g., water, heat or electrical interruption), each of which could cause significant damage to IT systems and possibly interrupt the organization's core services and operations.

3.34 *Capital Health* – We observed a number of good practices at Capital Health which help mitigate some of its physical security risks.

- A security company has been hired to manage access to various hospital sites, including the data centre.
- There is a staff member in the data centre 24 hours a day.
- Visible identification is to be worn at all times.
- Access to the data centre is logged.
- The data centre is equipped with devices that continually monitor and alert staff when certain environmental thresholds are met (e.g., temperature, humidity).
- Network cabling closets are locked.

- The data centre has an uninterrupted power supply and backup generator, in addition to dual power feeds from the power company.

3.35 However, we also observed some potential threats and weaknesses in the physical security and management of IT infrastructure at Capital Health.

- There is no approved list of who is authorized to enter the data centre.
- Visitors are not required to have an escort when they are in the data centre.
- The hospital's water tanks are located above the data centre, and any significant leakage that reaches the data centre could cause damage to IT equipment.
- IT policies do not address physical security against environmental factors (e.g., excessive temperature, water damage).
- There is no record of the maintenance performed on the data centre air conditioners.
- The physical locks for the data centre have not been changed even though there has been a change in who manages these keys and there are problems with obtaining keys from staff who have left the organization.
- No vulnerability assessment has been performed on the physical security of Capital Health's data centre and related infrastructure.

Recommendation 3.23
Capital Health should strengthen the security over its IT infrastructure by creating physical security policies, better controlling access to the data centre, and addressing structural issues such as mitigating water hazards and documenting equipment maintenance.

Capital Health Response:
CH health accepts this recommendation and is updating the Key Control Policy that will address obtaining keys from former employees, who is authorized to have a key, etc. The data centre locks will be changed.

The Director of Security has requested CH's security provider to provide key control practices they have implemented at other major hospitals.

The equipment in the mechanical room was located during the original building design and relocation is not an option given current physical restrictions. Much and ongoing work, including but not limited to work on the AC units; system wide maintenance and inspection in each of the last two years and warranty based work, has been completed and oversight in this area will be continued. CH is also currently putting efforts on relocation to another site and is working with the province on acquiring a secondary site.

Recommendation 3.24
Capital Health should have a vulnerability assessment completed on its data centre and related infrastructure.

Capital Health Response:
CH accepts this recommendation. CH has completed a review in the past and this has prompted current activities related to relocation to the new centre and efforts associated with finding a secondary site.

3.36 *IWK* – We found a number of maintenance procedures and controls at IWK that protect the physical security of its systems.

- The location of the data centre is protected from intrusion by having only one access point, which requires a key-card to enter.
- The data centre is monitored 24 hours a day.
- Physical security measures are regularly tested to assess their effectiveness.
- There is environmental monitoring (e.g., temperature, humidity) using sensors and software.
- Visitors are required to be accompanied by an IT staff member at all times.
- Only one vendor is allowed in the data centre at a time.
- Employees and vendors are required to wear visible identification badges.
- Physical security awareness training is provided to new hires.
- Uninterrupted power supply units are in place, as well as dual underground power feeds and two backup generators.
- Regular maintenance and inspections are performed on equipment by authorized personnel.

3.37 However, we also observed some potential threats and weaknesses in the management of the physical security of IT infrastructure at IWK.

- Management informed us that approvals are required for issuing data centre key-cards, but they were unable to provide support that employees currently accessing secured areas had received such approval.
- Data centre key-card access logs are available, but management was not reviewing them.
- Visitor access to the data centre (which does not involve key-cards) is not logged.

- The emergency procedure for responding to a power disruption is outdated and requires modernizing to reflect the current IT environment.
- No vulnerability assessment has been performed on the physical security of IWK's data centre and related infrastructure.

Recommendation 3.25
IWK Health Centre should strengthen the security over its IT infrastructure by improving controls over physical access to the data centre including:

- ***regular review of updated access lists for proper approvals;***
- ***implementation of logging procedures for all guests;***
- ***regular review of visitor logs; and,***
- ***updating emergency procedures.***

IWK Response:
IWK agrees with this recommendation. A new On-Line Service Request solution was implemented in November 2011. This solution requires a request form to be initialized by the requester to the appropriate manager requesting a number of services to be completed by the IT Department or Protection Services. This system tracks all requests and approvals/ rejections for all requests submitted. This new system is utilized for requesting key swipe access throughout the health centre, including physical access to the data centre. The retention schedule for the approval for all requests is seven years. This new system allows for the regular review and updating of access lists to those employees who have access to the data centre.

IT will restrict all physical access to the IT offices effective November 15, 2012. A manual log has been reestablished to log all guest access to the server room.

Recommendation 3.26
IWK Health Centre should have a vulnerability assessment completed on its data centre and related infrastructure.

IWK Response:
IWK agrees with this recommendation and recognizes that it is industry standard to have a vulnerability assessment completed by an outside agency, however this is a significant funding issue. Networks are dynamic, they evolve and change constantly; current practices of patch management, system updates, virus and malware monitoring are part of securing the network; however an assessment should be set to run constantly to assist in informing the administrator of potential threats to the network. Within the last two years the IWK requested and received a proposal for an Information Technology Review; however funds were not available at the time to move forward with the assessment. The IT Department will submit the request for a vulnerability assessment in the 2013/14 Capital Equipment funding process.

Management of System Access

Conclusions and summary of observations

Both Capital Health and IWK systems have existing or past employees with active user accounts which are no longer required. Additionally, individuals have been granted access to systems based on requests of persons not authorized to grant such access. At Capital Health, two applications are managed by a department other than the IT department and they do not adequately document granting and terminating of access to those applications. We noted that the Capital Health help desk uses the same temporary passwords when creating new accounts or resetting passwords, making the accounts more vulnerable to unauthorized use.

Access Management

3.38 Access management is the process of providing employees with computer accounts, setting and changing their ability to access different types of information, and removing computer accounts when employees are no longer with the organization. Employees only need the level of access that allows them to perform their job. Those with more access than necessary have an increased ability to see confidential information or perform unauthorized transactions. Employees terminated by an organization could retaliate by disclosing, modifying or deleting sensitive information if their user accounts are not deactivated at the time of termination.

3.39 *Capital Health* – Capital Health employs ticket tracking software to record requests for access to the network and some applications. However, not all requests to provide or modify access to applications were recorded using this software; notably when access to applications was managed by a department other than the IT department. In such cases, some requests were only recorded in the email inboxes of the department administrators managing the applications. As a result, we could not be sure all access changes were recorded and properly managed. In addition, the IT department was not always notified when individuals leave the organization and thus needed to have systems access removed.

Recommendation 3.27
Capital Health should establish a process for every system containing personal health information that ensures all requests to grant, modify, and terminate access are consistent and traceable.

Capital Health Response:
CH accepts this recommendation and will work to ensure consistency across departments in terms of granting access, modifying and terminating access. CH will work on documenting those procedures for all areas with information technology so management across the organization will be applying a consistent framework.

3.40 We tested a sample of 60 transactions to grant, change and remove access and found the following weaknesses.

- The help desk ticket only records that access is required for an application, not the level of access required.
- We found two instances in which individuals requested system access for another person, but were not authorized to make such a request. In both instances, the request was granted.
- We noted two instances in which the employee's computer accounts were not disabled even though they were no longer employees. Management has recently implemented a process to confirm that employee's accounts have been removed when staff leave.
- We noted the same temporary passwords were used frequently when accounts are created. This enables an individual with knowledge of the frequently used password to log into another account if it has not yet been changed by its new owner.

Recommendation 3.28
Capital Health should use unique temporary passwords when resetting locked-out accounts or creating new accounts.

Capital Health Response:
CH accepts this recommendation and will review and work to ensure compliance with all current password protocols.

Recommendation 3.29
Capital Health should ensure that all systems access is only approved by individuals authorized to do so.

Capital Health Response:
CH accepts this recommendation. CH does have a process to ensure systems access is only approved by individuals authorized to do so and will document and ensure all departments are applying the same standard.

3.41 *IWK* – Upon review and testing of the system access processes at the IWK, we noted some good procedures to control access to IWK's network.

- Forms approved by authorized staff are required.
- Individuals permitted to submit and approve requests are clearly identified.
- Temporary passwords are generated and delivered to new users in a secure manner and are changed upon initial login.
- Vendor accounts are only activated when they require access to systems.

3.42 We tested a sample of transactions and found the following weaknesses.

- There is no process to require users (at hire and periodically afterwards) to explicitly acknowledge that they received, understand and accept relevant IT policies, standards and procedures.
- Signed confidentiality pledges were provided for 56 of 60 employees tested. A periodic refresh of confidentiality pledges is not required.
- System access forms were not always approved by persons authorized to do so.
- Access was not removed for nine employees no longer employed by the IWK.

3.43 An online access process was implemented during our audit. Its design includes reducing the risk of improper approvals. The effectiveness of this design feature was not audited.

Recommendation 3.30
IWK Health Centre should ensure that access to all systems is only approved by individuals authorized to do so.

IWK Response:
IWK agrees with the recommendation. The New On Line Service request solution was designed and configured in two phases; Phase 1 was implemented in November 2011 which provided an electronic method for all requests for purchasing IT equipment, requesting access to systems and requesting swipe card access to secure departments requiring Manager approval; Phase 2 was the configuration and addition of new forms for staff internal transfers; enhancement of the functionality of the system will require departing and accepting new managers to remove and add appropriate access to systems dependent upon the employees role. This enhancement of functionality is targeted to be implemented by March 31, 2013 and will retain the manager's approval for seven years.

Recommendation 3.31
IWK Health Centre should enhance its processes to ensure that all users' access is removed once their employment has ended.

IWK Response:
The IWK agrees with this recommendation. The current process between Human Resource Services and the IT Department requires that the IT Department receive weekly notification of employees who have resigned or terminated. This IWK practice will change from a manual process to an electronic process following the implementation of the phase 2 configuration of our new electronic service request solution noted in Recommendation 3.30. As part of the quality improvement process, Human Resources will review the current workflow notification to incorporate IT notification. There will be a monthly review of staff who have resigned or been terminated to ensure access to

information systems have been removed. This improvement process will be implemented by November 30th, 2012.

Dormant Accounts

3.44 Dormant accounts are active computer accounts that have not been used within a significant period. An individual with knowledge of the username and password of a dormant account could use it to gain unauthorized access to information and perform operations that would be difficult to trace back to the individual.

3.45 *Capital Health* – We analyzed user accounts for the network, the 10 sample applications, and the supporting operating systems and databases we audited at Capital Health. We identified a high volume of dormant accounts on the network – 30% of all accounts. 22% of applications accounts and 7% of database accounts we tested were dormant. We could not assess dormant accounts on four applications and six databases because the information required to do this could not be generated by the systems.

Recommendation 3.32
Capital Health should have a process that ensures all new systems are capable of recording when user accounts are set up.

Capital Health Response:
CH accepts this recommendation and will ensure a process is implemented that records the date of set up.

Recommendation 3.33
Capital Health should have a process for the regular review of systems for dormant accounts. All unnecessary dormant accounts should be deactivated.

Capital Health Response:
CH accepts this recommendation and will update its procedures for account management.

3.46 *IWK* – We examined user accounts for the network and our audit's five sample applications. We identified a high volume of dormant accounts on the network, totaling about 25% of all accounts.

Recommendation 3.34
IWK Health Centre should have a process for the regular review of systems for dormant accounts, and all unnecessary dormant accounts should be deactivated.

IWK Response:
The IWK agrees with this recommendation. The IT department will work in consultation with the Privacy Office in developing policy and procedures to facilitate regular reviews and disabling unnecessary accounts; and will be implemented by March 31st, 2013.

Incident and Problem Management

Conclusions and summary observations

Capital Health and IWK have weaknesses in their incident and problem management processes. Neither entity has documented incident response procedures. Capital Heath does not have guidance for service desk staff to prioritize service requests, and does not monitor the nature of calls to the service desk and the resources used to resolve them in order to ensure the service is properly resourced. There is no problem management process at Capital Health or IWK that investigates or documents the underlying causes of incidents.

Incident and Problem Management

3.47 Incident management is the process of identifying and resolving any IT-related event that has a negative effect on the organization's computer systems. This process focuses primarily on fixing the issue and not attempting to determine why it occurred. Problem management is the process of investigating why such incidents occur and attempting to fix the underlying issue that caused the incidents. If these two processes are not in place and operating effectively, there could be extended interruption of computer services.

3.48 *Capital Health* – Service tickets produced at eHealth are prioritized, but there are no standards for deciding which types of incidents should be classified as high, medium or low priority. While any incident that affects patient care is automatically considered high priority, help desk staff are required to assess the situation and assign a priority classification based on their own view. If in doubt, staff members are instructed to make the ticket a high priority. Without consistent, documented guidelines, an improperly assigned priority could affect the resolution time of a real high-priority incident.

Recommendation 3.35
Capital Health should provide guidance for prioritization of IT service requests.

Capital Health Response:
CH accepts this recommendation and is currently partnering with the provincial system (HITS NS) to implement a new system called Axios. This upgrade should be underway at CH in 2013. Axios is fully ITIL compliant and with this implementation CH will be updating all procedures and the helpdesk will adopt ITIL framework with that implementation. CH can make some minor updates in its current system and will do so while ensuring appropriate investment is made in implementation of the new system which will the functionality will provide a more secure environment with improved auditing, and record logs.

3.49 There are no documented incident response procedures or a formally organized incident response team. In the event a staff member believes something should be escalated, it is communicated to the team leaders, who assess the issues and communicate with management. For large-scale incidents, management will come together with the various divisions of IT (i.e. security, telecommunications) to address the issue.

Recommendation 3.36
Capital Health should document incident response procedures and ensure its eHealth staff members are trained to use them.

Capital Health Response:
CH accepts this recommendation and with implementation of the new system will provide an improved way to document incidents at the helpdesk.

3.50 Management monitor the volume of service request calls received on a monthly and annual basis, as well as the number of unresolved requests in the queue at any particular time. However, little attention is given to the performance of the help desk in regards to time taken to resolve problems, appropriateness of solutions applied, service desk client feedback, or making comparisons to industry standards.

3.51 There is no organized problem management process in place at Capital Health to address the root causes of incidents reported to the help desk. There have been some attempts to implement a process and the help desk software has a problem management module, but we were informed that implementation has not been possible due to a lack of resources. In addition, when the module was last used, the number of service tickets generated crashed the help desk software.

3.52 eHealth does not generate or monitor metrics on distribution of time among tasks for IT staff. These employees can include help desk staff, administrators, programmers and project managers. Without such information, management cannot ensure there are enough employees to service information technology and the users of the technology. This could negatively affect the availability and security of computers and the support of computer users. Management has indicated that the recording of employee time is being rolled out throughout the organization in the next few years.

Recommendation 3.37
Capital Health should monitor the nature of service desk calls and the resources used to resolve them to ensure the help desk is functioning effectively and efficiently and to ensure significant problems resulting in repeat incidents are being analyzed and fixed.

Capital Health Response:
CH accepts this recommendation. Please refer to response for recommendation 3.35.

3.53 *IWK* – A service desk application is used at IWK and a log is maintained of all open service request tickets. Incidents are to be recorded in the service desk application managed by HITS-NS and assigned to technology, programs and services staff at IWK. There are no documented incident response procedures to guide staff. Turnaround times are established for tickets based on priority, and monthly reports are provided regarding timeliness of responses. Incidents are closed after an issue is resolved.

3.54 Management reviews monthly reports of service desk activity and follows up on issues if required. The reports contain metrics for service desk employee performance. Although there is no detailed reporting to management, regular meetings occur between IWK IT managers and the HITS-NS service desk manager to discuss results and address performance issues.

Recommendation 3.38
IWK Health Centre should document incident response procedures.

IWK Response:
The IWK agrees with the recommendation. Current process for documentation of incident responses is through the Provincial Service Desk Express application which is hosted by HITS. A procedure document will be developed outlining the documentation criteria which will encompass a quality improvement process to review those incident responses and ensure there is consistent comprehensive documentation within the service desk tickets. This will implemented by December 31, 2012.

3.55 IWK does not have a comprehensive problem management process. It does not identify or document the underlying causes of reported incidents. The organization maintains an index of common problems and fixes, but it is not based upon a root cause analysis of service desk tickets.

Recommendation 3.39
IWK Health Centre should implement a problem management process to document the identification, classification, investigation and resolution of IT problems.

IWK Response:
The IWK agrees with this recommendation. Our current process for IT related sentinel events and/or recurring events is the monthly review at our Information Management/ Information Technology Quality Improvement Committee. This process requires consultation and collaboration with other stakeholders involved in the incident to identify, investigate and resolve through process improvement practices to correct or mitigate these occurrences for the future. These process improvements are documented within the quality improvement framework and provide feedback to the stakeholders involved. As part of the quality improvement framework, adoption of a similar process will be implemented for non-sentinel events to facilitate review and root cause analysis, with appropriate documentation to ensure there is not an extended interruption of services. A new provincial incident and problem management platform is being implemented this fall/winter with HITS NS.

Change Management and Project Management

Conclusions and summary of observations

Deficiencies in the change management process at Capital Health include the lack of auditing in the help desk software to detect and deter unauthorized changes. There is a process to manage changes to systems within the IWK, but it is not documented. Project management processes are not consistent among Capital Health's various departments, and IT services are not always recognized as a stakeholder in IT projects if a project is managed by another department. IWK has a project management process that is overseen by project managers, but there is no central project listing to track all projects.

Change Management

3.56 Adequately secured systems have a rigorous change management process. Such a process requires all changes relating to IT infrastructure and applications, including emergency maintenance and software patches, to be managed and controlled to prevent and detect unauthorized changes.

3.57 *Capital Health* – Procedures exist at Capital Health to handle requests for changes to applications, operating procedures and processes, system and service parameters, and the underlying hardware platforms. The procedures include defining roles and responsibilities, classifying and defining priority levels, and guidance for the functioning of the organization's Change Advisory Board, which examines and approves change requests.

3.58 We found deficiencies in Capital Health's use of Service Desk Express, the application used to manage and monitor changes. Many change tickets produced by the system did not have start and end dates, and some tickets were created after the change occurred, even though they were not emergency changes. The system is configured to permit editing of fields by any user and does not log such editing. The risk is that unauthorized system changes could be entered into the system and noted as approved.

Recommendation 3.40
Capital Health should record proper dates for each ticket produced by the system used to track and manage changes.

Capital Health Response:
CH accepts this recommendation. Please refer to response for recommendation 3.35.

Recommendation 3.41
Capital Health should configure its help desk system so that it blocks unauthorized editing of its data.

Capital Health Response:
CH accepts this recommendation and will implement changes at the helpdesk to block any editing. Improved functionality for all helpdesk functions will be implemented with Axios.

3.59 Capital Health's change management process is not adequately designed to reduce the risk of unauthorized changes occurring. We observed the following deficiencies.

- For an application managed outside of the e-Health, there is no process to detect and inform the change manager of unauthorized changes.
- Of a sample of 60 change tickets reviewed, 11 did not have evidence of approval by either the change manager or the Change Advisory Board.
- There are no policies requiring administrators to always use the application to perform data modification instead of circumventing the application and posting changes directly to a database.
- The disciplinary consequence of an employee making an unauthorized change is not documented.

Recommendation 3.42
Capital Health should implement a process to detect and deter employees from making unauthorized changes.

Capital Health Response:
Capital Health accepts this recommendation. See response to recommendation 3.35.

3.60 *IWK* – Our testing at IWK revealed the presence of some change management controls, including change requests and approval requirements. However, these controls are not documented. There is no IT Change Advisory Board at the IWK, but Technology, Programs and Services relies on representation from various committees to ensure IT issues are addressed when implementing new systems or changes.

Recommendation 3.43
IWK Health Centre should document its change management process.

IWK Response:
IWK agrees with the recommendation. The IT department has a current process in place for documenting a change management process that ensures the change request has been initiated, the change plans and approval of the change is accepted, all coordination between departments, staff notification and training has occurred prior to the implementation of the change request. Development of the supporting documentation for these processes and procedures that are currently in place will be completed by March 31st, 2013.

3.61 New systems or large-scale projects at IWK have committees established and a project manager assigned. There is a provincial requirement to take new systems or major IT

projects to the provincial IT group. All changes require approval by the Department of Health and Wellness' Chief Information Office.

3.62 Large applications have separate test and production environments, which help prevent development projects from damaging the Health Centre's live systems. Smaller applications do not have their own dedicated test environment. We were informed that in such cases, a temporary copy of a production environment is made to perform testing of the change prior to moving it to production.

3.63 Emergency changes, often required when software or a piece of hardware fails, do not follow a defined process. They are generally subject to the standard incident response process, which was found to be informal and without documented procedures (discussed earlier in this chapter). However, the size of the IT department at IWK is small enough that management is accessible to approve emergency changes.

3.64 Technology, Programs and Services is currently enhancing its change management process and recently implemented a new procedure for documenting change requests and approvals. The new procedure requires completion and approval of an electronic request for change form before changes can be made. We concentrated our testing on the new process.

3.65 As a result of our testing, we found one change was implemented before being approved. We also identified an instance in which there was no documented evidence that testing was completed prior to implementing a change.

Project Management

3.66 Best practice in IT project management recommends having specific project controls and phases to ensure that what is implemented is in line with agreed-upon expectations and outcomes. This requires proper testing, clear implementation roles and procedures, and a post-implementation review to help improve future projects.

3.67 *Capital Health* – eHealth has a list of active IT projects for which it is responsible, but management informed us there are projects run in other departments that have an IT component. Sometimes eHealth is not aware of these projects until later in the project life cycle.

3.68 Privacy impact assessments are required for any new application or system that contains personal health information.

3.69 IT project managers at eHealth use a generally accepted project management framework. There are specific requirements for project documentation and the selection of mandatory project components (e.g., design, testing) are determined on a project-by-project basis.

3.70 We examined two projects. The first was an application upgrade managed through eHealth. We found eHealth's project management framework was followed. For

example, the vendor provided training, there was a test plan, and a post implementation review was performed.

3.71 The second project was managed at another department. Reasonable project management processes were followed, but documentation was less than adequate due to much of it being stored in the administrator's email. Without the administrator, another individual would not be able to determine which projects were completed and whether reasonable processes were followed.

Recommendation 3.44
Capital Health should follow eHealth's project management processes for all significant IT projects throughout the organization.

Capital Health Response:
CH accepts this recommendation and will work to improve the consistency across departments in terms of how projects are managed. CH will work on documenting the project management procedures and educating/supporting other departments with their Project Manager.

3.72 *IWK* – Technology, Programs and Services does not have a central list of all active IT projects for which it is responsible. Large projects are assigned project managers and steering groups monitor progress. Technology, Programs and Services should have a list of ongoing projects with status reports and target milestone dates.

3.73 All new systems or changes to systems are required to have a privacy impact assessment completed prior to implementation. This involves input from an IT Security representative and a Risk Management representative. The Risk Management department obtains the vendor's privacy policies to assist in preparing the privacy impact assessment for the new or upgraded system. Additionally, all requests for proposals include a privacy component that must be addressed in the proposal. We reviewed five applications and found that privacy impact assessments were prepared for each.

Recommendation 3.45
IWK Health Centre should maintain a central list of ongoing projects and their status.

IWK Response:
IWK agrees with the recommendation. Development of a central list of ongoing IT projects and their status is currently in development utilizing Microsoft Project. This will be implemented and monitored by November 30th, 2012.

Management of Data and Operations

Conclusions and summary of observations

Capital Health and IWK have policies and procedures to provide guidance in the management of data. Both entities acknowledge that their systems will not be able to comply with all of the requirements of the new Personal Health Information Act that is expected to be proclaimed soon. Capital Health and IWK forecast IT capacity requirements. Capital Health does not forecast capacity requirements for the human resources necessary to provide IT services.

Management of Data

3.74 Best practices in data management include identifying and classifying an organization's data requirements and specifying how each group of data is to be used and secured (e.g., identifying and limiting access to highly confidential data). It also includes effectively managing data storage media libraries (e.g., data tapes), maintaining copies of data off-site in case it is inadvertently destroyed, and securely disposing of used data media so that confidential information is not exposed.

3.75 The province is expected to proclaim a new Personal Health Information Act, which will potentially give patients the right to limit or revoke their consent for personal health information to be disclosed to other health professionals. Management at both Capital Health and IWK told us that existing information systems do not have the capability to limit access to information at the detailed level that may be required by the new legislation.

3.76 *Capital Health* – Capital Health has implemented policies and procedures to identify and apply security requirements to the receipt, processing, storage and output of data. However, no data classification model has been designed so the level of security can be matched with the sensitivity of the various types of data stored.

3.77 Capital Health has a data storage and retention policy, as well as a process to maintain a recorded inventory of stored and archived storage media. This helps ensure the usability and integrity of stored information. When the retention period is over, Capital Health has a process to securely dispose of sensitive data and software.

Recommendation 3.46
Capital Health should implement a data classification policy.

Capital Health Response:
CH accepts this recommendation and will develop and implement a data classification policy by fiscal 2014.

3.78 *IWK* – Data storage and retention arrangements are in place at IWK. As a directive from its Privacy Office, the retention period of electronic records is consistent with

that of paper records. Secure disposal policies exist and require removal of patient information from all storage media before any hardware leaves the hospital site. Media containing sensitive data are physically destroyed before disposal.

Management of Operations

3.79 Good management of IT operations includes defining operating policies and procedures for effective and efficient infrastructure performance (e.g., operating servers, monitoring network capacity, running routine computer processes), and ensuring the adequacy of hardware preventive maintenance.

3.80 *Capital Health* – Not all operational procedures are documented to provide sufficient information to ensure that operations staff members are familiar with all the tasks and problem solving measures relevant to them. For areas that do have reference materials, most of the documents are not dated or are outdated. There is also no consistency as to the level of detail and direction provided to staff responsible for individual applications.

3.81 Capital Health uses software that provides automatic notification of hardware faults and errors. In addition, an annual preventative maintenance process looks at the life cycle of the servers and the warranty remaining.

Recommendation 3.47
Capital Health should implement a process to ensure operational procedure documents contain sufficient information to guide operations staff in their responsibilities. Operational procedure documents should be kept current.

Capital Health Response:
CH accepts this recommendation. CH has been working on updating its standards of practice documentation and will update all procedure documents by end of fiscal 2014.

3.82 *IWK* – In its management of IT operations at IWK, Technology, Programs and Services has documents containing information to assist staff members with the tasks and problem solving measures relevant to them. These IT operational procedures exist in the form of instructions to solve user problems and are available on the IWK intranet. IT infrastructure is monitored using software and a dedicated operations team. Problems are addressed as they arise. A preventative maintenance plan for hardware is in place at IWK.

Manage Resources

3.83 Best practices in IT resource management include monitoring the performance and capacity of IT resources and forecasting of future needs so that performance and capacity issues are detected before they occur.

3.84 *Capital Health* – Capital Health uses software to monitor current capacity and performance levels and issues are handled as they arise. However, due to an information request from our office, Capital Health managers discovered that a Windows server was not being monitored for hard drive space. At the time of discovery, its maximum capacity was almost met. This was close to affecting the performance of the server and the databases it supported.

Recommendation 3.48
Capital Health should ensure all servers are being monitored for hard drive capacity.

Capital Health Response:
CH acknowledges this recommendation. CH currently monitors all critical systems for their capacity needs. CH forecasts IT capacity requirements for critical patient care systems. All new projects include a budget to purchase storage and redundancy to ensure capacity will meet demand. Each year CH budgets for added capacity. CH will review, within financial capacity, current server planning to evaluate where improvements can be made.

3.85 Human resources capacity management is not performed at Capital Health to ensure sufficient staff is available for managing IT infrastructure and providing IT service. Management informed us that this is being addressed over the next few years through implementation of a case costing application that will require employees to record their time.

Recommendation 3.49
Capital Health should implement processes to monitor existing human resources levels and forecast future capacity requirements for providing IT services.

Capital Health Response:
CH accepts this recommendation and will review systems and the alignment of human resources currently to ensure that CH has the capacity for future requirements. CH is currently undergoing a provincial review process to investigate opportunities for merged services. This may have an impact on the human resources and how they are allocated and/or managed. CH will work to implement an improved way of aligning resources and projecting future needs.

3.86 *IWK* – IWK forecasts IT capacity requirements annually when prioritizing capital equipment requests for the organization. Software is utilized to monitor current capacity and performance levels, and issues are handled as they arise. The capacity and performance of human resources supporting IT is managed by way of a personnel time-tracking system and regular meetings between staff and managers.

Governance of Information Technology

Conclusions and summary of observations

There are deficiencies in the IT governance framework of both entities. Processes in place to identify and manage risks relevant to health IT systems at Capital Health are inadequate. At IWK, there is no overall assessment of IT controls and IT policies are not maintained. Capital Health does not centrally document identified risks, and its focus on risk mitigation is at the project level, rather than at an organizational level. IWK maintains a record of identified risks and the action plans prepared to mitigate those risks, but does not identify residual risk in its risk register.

IT Governance

3.87 In a well-run organization, information technology fully supports the organization's vision, mission and strategic goals. To ensure this occurs, management governs how IT is implemented and used. This includes ensuring IT strategies align with organizational strategies, having rules to govern how technology is to be used and controlled, monitoring the performance of technology and the human resources supporting it, and identifying and mitigating technological risks.

3.88 *Capital Health* – We observed alignment between Capital Health's strategic goals and the strategic plans of its IT division (eHealth). IT projects link directly to the accomplishment of the organization's goals. The five strategic streams outlined in the organization's business plan are integrated into the employee performance appraisal process. This ensures that employees align their priorities with Capital Health's objectives. The business plan also includes an information management strategy outlining related priorities and initiatives for IT at Capital Health.

3.89 *IWK* – Members of Technology, Programs and Services participate in organization-wide, cross-functional committees to obtain funding, monitor achievement of objectives and manage risk. A process is in place to update the Division's stakeholders annually on its activity.

3.90 Technology, Programs and Services takes direction from the IWK Strategic Plan and provincial directives. Requests for new technology are submitted for funding approval on an annual basis and are assessed, prioritized, and approved based on the IWK's business strategy and the provincial IT strategy.

Policies and Procedures

3.91 Due to the sensitive nature of much of the information health organizations maintain, employees need to know what they can do with computer resources and the personal health information contained within them. The documentation and communication of up-to-date policies and procedures is imperative to protecting such information.

Without such measures, there is greater risk of unauthorized exposure of confidential information.

3.92 *Capital Health* – Executives at Capital Health communicate and reinforce the organization's control culture, ethics and values to staff through policies. There is also a policy requiring regular review and updating of policies. We found that Capital Health was in the process of updating their policies and subsequently published those policies during our audit.

3.93 At Capital Health, the process to provide users with access to the network includes both a documented acknowledgement by users of policies reflecting confidentiality, and the submission of the results of a criminal record check. After hire, however, an employee is not required to acknowledge new or changed IT policies.

Recommendation 3.50
Capital Health should require employees to periodically refresh their acknowledgement of confidentiality policies, especially when there are significant changes.

Capital Health Response:
CH accepts this recommendation and will be using CH's online learning system (LMS) to implement a mandatory annual review for all employees. This system will track completion of the session by employee.

3.94 Capital Health has a policy that requires employees to follow specific procedures upon identification of a policy breach or when an exception to policy is necessary. Required communication includes notifying the Policy Office, as well as identifying related risks and mitigation strategies. The policy also identifies who can approve such exceptions. However, the policy does not define the types of exceptions it is meant to address; therefore, it could be interpreted to include clinical, information technology and other policy exceptions.

3.95 Through our IT configuration testing, we found a policy breach that did not follow the protocols. While performing routine monitoring, management discovered changes to a system's password settings that did not comply with Capital Health's password policies. No risk assessment was completed and the individual who approved the changes did not have appropriate authorization.

Recommendation 3.51
Capital Health should ensure the requirements of its policy exception policy are being met.

Capital Health Response:
CH acknowledges this recommendation. The intention of the Policy Exception Policy was primarily for direct clinical care cases. In the administration/support areas, exceptions may be approved by the Manager/Director. CH will ensure clarity of its policies on this topic.

3.96 *IWK* – IWK does not have a current set of policies covering all areas of IT. This includes the important area of IT security. The organization is in the process of updating all of its policies, but there is no process to update policies on an ongoing basis.

Recommendation 3.52
IWK Health Centre should develop a current, comprehensive set of policies to guide its use and control of information technology.

IWK Response:
IWK agrees with the recommendation. The IWK will work in concert with other DHA's and HITS-NS to develop comprehensive IT policies. As we move along with Merged Services Nova Scotia, these polices will be developed at the provincial level and will be incorporated within the Provincial OP3 Initiative (One Province – One Process – One Policy). In light of new legislative changes and the provincial joint initiative in policy development, IWK is working along with other provincial DHA's in the development and revision of privacy policies. This is also in alignment with the Shared Services model.

Recommendation 3.53
IWK Health Centre should develop a process to keep its policies up-to-date.

IWK Response:
IWK agrees with the recommendation. The IT Department has several policies that have been updated; however they are currently in draft format. A formal mechanism for reviewing, updating and submission for approval will be developed and implemented for current policies by March 31, 2013.

3.97 The IWK has human resource procedures that communicate privacy and confidentiality policies to system users prior to users gaining access to confidential information. However, documented acknowledgement of such policies by system users is not required.

Recommendation 3.54
IWK Health Centre should require employees to provide documented acknowledgement of their understanding of confidentiality and IT security policies at the time of hire and periodically during their employment term.

IWK Response:
IWK agrees with the recommendation. The IWK is compliant with this recommendation for all new hires; this practice has been in place for many years. The IWK will require all users at hire and regularly thereafter to read and sign the revised confidentiality pledge form.

The IWK Privacy Manager is currently a member of a provincial working group, along with privacy representatives from all nine DHAs, that is developing a Privacy E-learning

module. The IWK plans to implement the E-Leaning module in early 2013, as a requirement for all current and new employees upon hire and annually thereafter. Employees will be required to refresh and re-sign their confidentiality pledge annually, upon completion of the Privacy E-Learning module.

Monitoring of IT Controls

3.98 To ensure business processes designed to protect confidential information are working as intended, an organization needs to assess processes on a periodic basis. Significant weakness need to be fixed promptly.

3.99 *Capital Health* – There is no internal audit group at Capital Health to assess IT controls and there have not been any external reviews to provide assurance on the organization's overall IT control framework.

Recommendation 3.55
Capital Health's IT control framework should include a process for monitoring and assessing IT controls.

Capital Health Response:
CH accepts this recommendation and will work on reviewing and updating its IT control framework.

3.100 *IWK* – There is no internal audit group at IWK to assess IT controls and we did not see evidence of any external reviews of overall IT controls. Various committees and processes exist within the organization that act as a mechanism to detect and track control deficiencies. The identification of risks based on the annual enterprise risk management process may also identify gaps in internal controls, but the exercise does not provide assurance that controls are designed properly and operating effectively.

Recommendation 3.56
IWK Health Centre's IT control framework should include a process for monitoring and assessing IT controls.

IWK Response:
The IWK agrees with the recommendation. Through Service Level Agreements (SLA) with our clients, we establish clear ownership and responsibilities for IT control, support and general acceptability of system and processes. There is a need to improve current processes and to provide better alignment based upon a clinical focus; and improve upon our shared understanding amongst all stake holders. Adoption of SLA is built into the implementation of all new systems over the past 12 months. Development of a process to review and develop SLA's for existing systems is currently underway and acknowledge this will require additional resources and time to coordinate with all of the stakeholders involved with clinical systems. As we move forward with Merged Services Nova Scotia the IT control framework will be identified and implemented with a provincial lens rather than an individual DHA/IWK.

Risk Management

3.101 Risks include any events that would adversely affect an organization's operations. Best practices in risk management include having a process that documents identified IT risks, related mitigation strategies and leftover residual risks. Analysis and assessment of IT risks should align with the organization's overall risk identification processes. Adoption of risk mitigation strategies should minimize residual risk to an accepted level. Failure to assess and mitigate IT risk within health organizations can result in events that affect the confidentiality, integrity and availability of personal health information.

3.102 *Capital Health* – Capital Health does not have an IT risk framework. The eHealth department manages risk on a project-by-project basis; however, this only addresses the specific risks of implementing new technology or changes to existing technology. eHealth does not perform a periodic assessment to document IT-related risks that could affect the entire organization. There is no central registry to document risks identified through other means, nor has a risk tolerance level for the organization been defined. There are no action plans developed to mitigate known risks.

Recommendation 3.57
Capital Health should implement an IT risk assessment framework that includes determining and documenting IT risks, related mitigation strategies and the acceptability of its residual risks.

Capital Health Response:
CH accepts this recommendation and will work on reviewing and updating the IT risk assessment framework.

3.103 *IWK* – Technology, Programs and Services has an IT risk management framework that includes an annual process to identify and update risks in a document referred to as a risk register. A dedicated staff member works closely with the Health Centre's Risk Management Office to ensure IT risks are managed in concert with overall organizational risks. The Risk Management Office defines the context for applying the risk assessment framework during the annual enterprise risk management process.

3.104 We observed that assessments of threats in the risk register were performed in a consistent manner and linked to documented mitigation strategies and action plans. However, the risk management process does not document the levels and acceptance of the residual risks remaining after mitigation strategies have been implemented.

Recommendation 3.58
IWK Health Centre should include residual risks as part of the maintenance of its risk register.

IWK Response:
IWK accepts the recommendation and will enhance our current risk register to document the residual risk following the implementation of the identified resolution or mitigation strategy. This enhancement will be implemented through our regular review process.