CIS Audit Service Model

Outline for CIS Security and Compliance Audits

4/3/2017

Updated Nov 1, 2018/RL

Contents

Service Background 3

Service Definition 3

Goal and Objectives 3

Core Activities 4

Target Population(s) 4

Key Outcomes and Measures 4

Staffing Model 4

Policy Requirements 5

Business Process 5

Security Audits 5

Compliance Audits 5

Investigative Audit Tools 5

Space, Equipment and Supplies 6

Financial Model/Budget 6

Implementation Plan and Potential Impacts 6

Implementation Plan 6

Impacts 6

Evaluation, Monitoring and Reporting 6

Appendix A: CIS Security Audit Process 7

CIS Security Audit – By Request 8

CIS Security Audits – Routine 10

CIS Security Audits – Scheduled 12

Appendix B: CIS Compliance Audit Process 14

Compliance Audits: 15

Appendix C: CIS Audit Service Implementation Work plan 17

Appendix D: Evaluation Framework 18

Service Background

Health PEI's Clinical Information System (CIS) has been operational since 2008. Since that same time, a *Security and Access* policy has been in place that outlines the CIS auditing requirements. While security audits are currently in practice, there is a need to build a more robust audit service to improve the breadth and access of auditing activities within CIS, that will not only meet the monitoring needs of today but those in the future (as the use of the CIS system expands in volume and form). This service model confirms and expands existing work to formalize a more comprehensive CIS audit service.

Service Definition

The CIS Audit Service provides a coordinated and structured approach to auditing activities within CIS.

Goal and Objectives

The main goal of the CIS Audit Service is to monitor the use of the clinical information system to promote the appropriate accessing of clinical data and personal information, as well as the compliance with provincial legislation (e.g., *Freedom of Information and Protection of Privacy Act*), organizational policy and standards (clinical, professional and Accreditation Canada) as well as HPEI training practices by assessing, monitoring and reporting on CIS user activity.

There are two categories of audits conducted for CIS; security and compliance.

- Security – monitor and promote the appropriate accessing of patient personal information within the CIS and compliance with the *Freedom of Information and Protection of Privacy Act* and the Health Information Act
- Compliance – monitor the use of the CIS in accordance with applicable provincial legislation and organizational policy, standards (clinical, professional and Accreditation Canada) and training practices.

Security Audits:

There are three types of security audits: requested audits, routine audits and scheduled audits.

- Requested audits are driven internally by a supervisor, manager or director, or they can be driven externally by a member of the public requesting an audit of access to his/her own CIS chart[1].
- Routine audits are regularly performed audits (conducted monthly) in which CIS users are randomly selected and audited to ensure their accessing of patient's charts (within a given time period) is appropriate from a security perspective. It does not address the quality of the file, such as whether the file content is in accordance with clinical guidelines. The purpose is solely security focused.
- Scheduled audits are regularly performed audits at a discipline level (frequency depends on the audit) and results are shared with the appropriate manager who is then required to review the audit findings in relation to staff activity to ensure no breach has occurred.

Compliance Audits:

[1] If Health PEI staff requests an audit of their file, this is treated as a request from a member of the public.

Compliance audits will look at whether the Clinical Information System is being utilized in accordance with applicable provincial legislation and organizational policy, standards (clinical, professional and Accreditation Canada) and training practices among the various professional or occupational groups. Requirements are to be identified and prioritized by the various discipline. Compliance audits can be requested by directors or leadership committees (e.g., Director of Nursing Committees) and need to be provincially monitored.

Core Activities

In terms of auditing, the following are the activity areas of the CIS Auditing services:

- Management and coordination of the audit framework and schedule.
- Design, produce and report audits
- Work with the various HPEI program areas and disciplines to identify audit requirements.
- Provide education and communication about the audit service, its methodology, and interpretation as well as how it relates to clinical operations
- Support quality improvement through technical advice and data in collaboration with the different program areas.

Compliance audits may occur at multiple levels within the organization: system, program/service, unit or individual level (client or clinician). The CIS Audit Services is responsible for providing the tools and framework required to perform the audits, while the managers or directors of the appropriate disciplines are responsible for identifying any compliance issues and acting on them accordingly

Target Population(s)

Clients of the CIS Auditing Services can be members of the public or HPEI managers, directors or leadership committees.

Key Outcomes and Measures

Overall it is expected that there will be a number of longer term outcomes for this service:

- Structured and transparent approach to audits CIS system use complies with guidelines, policy, legislation and standards.
- Reduce the risk of privacy breach.
- Accurate, timely and meaningful data can be yielded from CIS
- CEO Compliance Indicator measurement and annual reporting:
    - #1. Number of CIS user based audits completed/120 = % completed of expected for fiscal year 2016/17. Target = establishment of baseline (year 2016/17)
    - #2. Number of Privacy Breaches found by user based audit/120 = % of user audits that revealed a privacy breach. Target = establishment of baseline (year 2016/17)

Staffing Model

Staffing for the CIS Audit Service is drawn from two government service areas: Health PEI's Health Information Management and PEI Department of Finance, Information Technology Shared Services (ITSS). Currently one staff member from ITSS performs the role of Security Analyst and is assigned to Health PEI for a range of supports, of which approximately 30% of their time is allotted to CIS security auditing (0.3 FTE). For the audits, staff from Health Information Management division and the CIS

Reporting group, provide the tools and the framework for the audits while the appropriate business areas are responsible for investigating and actioning the audit results. There will be a need to monitor the demand audits place on staff time. Initially this will be monitored through a program evaluation.

Policy Requirements

Currently expectations related to CIS auditing are outlined in the Security and Access – Clinical Information System policy (created in 2008). This policy outlines that Health PEI is responsible to ensure acceptable and appropriate security and access safeguards are in place to protect personal information. As well, compliance with the guidelines, policy, legislation and standards are monitored and actioned.

Business Process

Processes for both the security and compliance audits are outlined in Appendix A and B respectively.

Security Audits

Security audits can be by request, part of routine or scheduled audits. Requests for the former are submitted to the CIS Security Analyst through a manager/director.

Security audits can be at an individual patient level (e.g., high profile, suspected breach), an individual staff member level (e.g., potential breach by a staff member) or at a unit or service level. Routine audits are focused at the individual staff member level, whereas scheduled audits are at the patient level. Currently, 10-20 random audits are conducted per month. Scheduled audits frequency will vary depending on the audit – but should be done at least on a quarterly basis.

Compliance Audits

Compliance audits can be conducted at the system level and broken down to a unit or service level. These audits are largely driven by organizational policy and standards (clinical, professional and Accreditation Canada) and so are most relevant to monitor clinical activities.

Investigative Audit Tools

There are several types of audit reports available to the Security Analyst to use when an audit requires additional investigation, or a Manager/Director requests a specific audit outside of the ones run on a regular basis. They are:

- **User Chart and Tab Access** - Identifies all patient charts a specified user has opened and which tabs they navigated to. Reflects when each patients chart has been opened in PowerChart and when each tab was clicked on.
- **Documentation Charted by User** - Identifies what charting a user has performed on a patients chart (power forms, progress notes etc). Reflects if the user opened the chart during the reports date range, when the documentation was performed and what type of documentation was charted.
- **Orders Placed by User** - Identifies what orders were placed by a specific user (either Entered by or Ordered by). Reflects when the order was placed, who the order was entered by, who the ordering provider was and a description of the order (order catalogue type, activity type and catalogue).

- **Patient List Audit** - Identifies all patients lists that a user has available to them. Reflects the name of the list, a description of the list, when they added the list and when the list last became active.
- **Users Logged into Applications Audit** - Identifies users who have logged into Cerner applications. Reflects the day they logged in, the number of times they logged in and how long they were in the application for. Note: The length of time is only calculated when the user closes the application, if they are timed out the length of time is set to zero.

Space, Equipment and Supplies

An application was designed to track and monitor the number and stage/status of audits being performed (CIS Audit Tracking System - CATS). No additional space, equipment or supplies are expected for this service to be implemented.

Financial Model/Budget

The costs associated with this service are in-kind compensation for the 30% of the ITSS CIS Security Analyst role. The additional time required for compliance audits will be tracked over the first year(s) of implementation to determine the in-kind costs associated.

Implementation Plan and Potential Impacts

Implementation Plan

The implementation plan is outlined in greater detail in Appendix C. A staged implementation of the expanded audit service began in April 2016 with routine security audits for nursing. A more complete service model was developed in the fall of 2016 to outline the parameters of both security and compliance audits. An implementation work plan is presented in Appendix A and outlines the implementation of CIS Audit Service through to December 2017.

Impacts

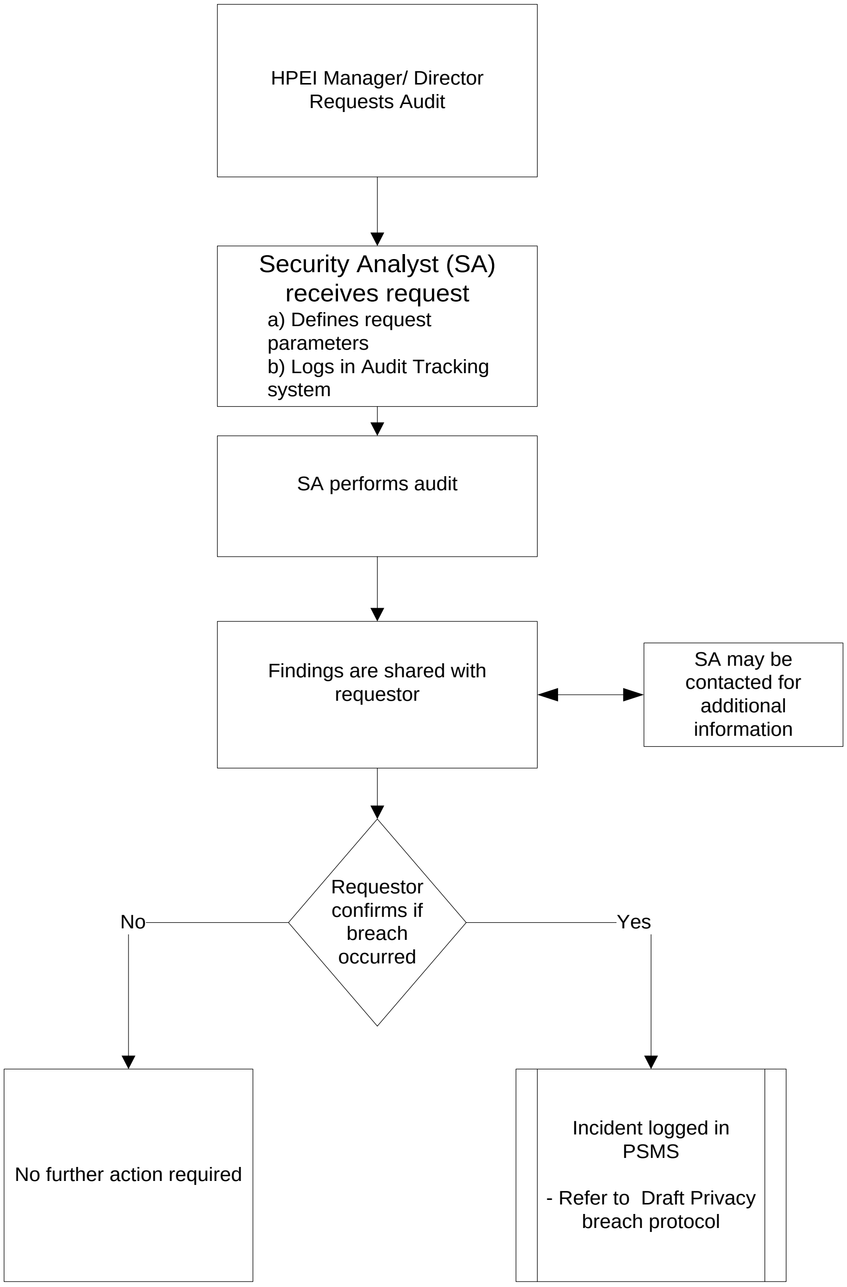
It should be noted that a more comprehensive auditing service as well as more awareness of this service may have additional impacts on the CIS Reporting Group and the ITSS Security Analyst. As the CIS user base continues to expand, as well as the different types of system access grows (ie. Non-Government access), the CIS Audit program must continue to be reviewed, modified and expanded to meet the monitoring requirements of the CIS. Since the specific implications are unknown at this time; impacts should be monitored as the schedule is implemented.

Evaluation, Monitoring and Reporting

The implementation and operationalization of this service will be monitored and reported regularly. This service is under the management of the Director of E-Health, Clinical Operations. The evaluation outcomes and progress of the service will also be reported to OMC (Operational Management Committee) for information and advice (refer to Appendix D). As well, the Compliance Indicator measurement will be reported as part of the CEO annual reporting. Responsibility and authority of this service rests with the Director of E-Health, Clinical Operations.

Appendix A: CIS Security Audit Process

CIS Security Audits – By Request


HPEI Manager/ Director Requests Audit
Security Analyst (SA) receives request
a) Defines request parameters
b) Logs in Audit Tracking system
SA performs audit
Findings are shared with requestor
SA may be contacted for additional information
Requestor confirms if breach occurred
No
Yes
No further action required
Incident logged in PSMS
- Refer to Draft Privacy breach protocol

CIS Security Audit – By Request

- A Health PEI Manager or Director can request a CIS Security Audit through the Security Analyst (SA) when:
    - they suspect that a user has inappropriately accessed a patient's or;
    - a person of interest has visited an acute care facility and they would like to confirm no inappropriate access has occurred.

  Requests should be emailed to: **CIS Security Audits** (CIS Security Audits@gov.pe.ca)

- Upon receiving the request, the SA works with the requestor to define the parameters of the request.
    - Example parameters would be: Time Frame, Facility/Unit, specific patient or employee.

- Once finalized, the SA will record the request in the Audit Tracking System.

- SA performs the security audit as per the agreed upon parameters.

- Findings are shared with the requestor.

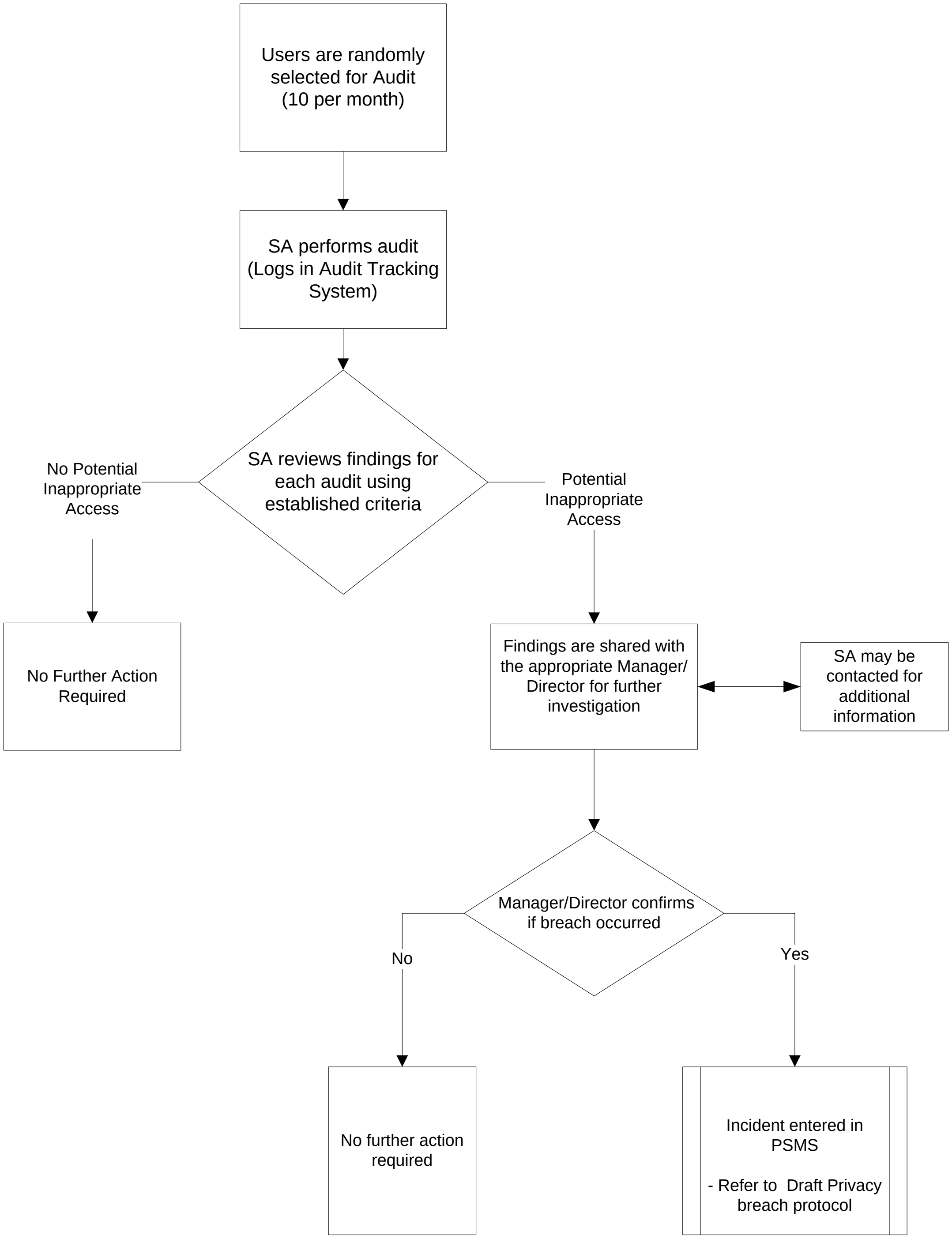
- The requestor is to review the findings and perform any additional investigation required to confirm if a security breach has occurred. The SA may use additional audit investigative tools as required.

- If a security breach has been confirmed, it is the responsibility of the requestor to log an incident in the Provincial Safety Management System (PSMS) as a "Privacy Breach" and follow the appropriate procedure. Refer to Draft Privacy Breach Protocol.

  Note: If over the course of the audit, other areas of suspicion or interest are identified, this would trigger additional audits (referred to as Trigger Audits).

CIS Security Audits – Routine

User Based Audits – applicable to all CIS User Groups/Disciplines


Users are randomly selected for Audit (10 per month)
SA performs audit (Logs in Audit Tracking System)
SA reviews findings for each audit using established criteria
No Potential Inappropriate Access
Potential Inappropriate Access
No Further Action Required
Findings are shared with the appropriate Manager/ Director for further investigation
SA may be contacted for additional information
Manager/Director confirms if breach occurred
No
Yes
No further action required
Incident entered in PSMS
- Refer to Draft Privacy breach protocol

CIS Security Audits – Routine

- CIS users will be randomly selected on a monthly basis for auditing.

- The Security Analyst (SA) will record each audit performed in the Audit Tracking System.

- The SA performs the security audit and highlights any questionable activity or potential inappropriate accesses.
    - Routine audits will examine a user's chart accesses over a one week period.
    - Examples of items that would flag further investigation:
        - User accessing a patient's charts outside of their area of responsibility;
        - Dormant charts accesses;
        - Patient Lists that may have been established outside of the user's area of responsibility.
        - Same Last Name as Patient
        - User's own chart has been accessed.

    - If no questionable or suspicious activity is identified, the SA records that the audit was conducted and no further action is required.
    - If questionable or suspicious activity is identified, the SA will send the audit findings along to the appropriate Manager/Director.

- The Manager or Director is responsible to then review the findings and perform any additional investigation required to confirm if a security breach has occurred.

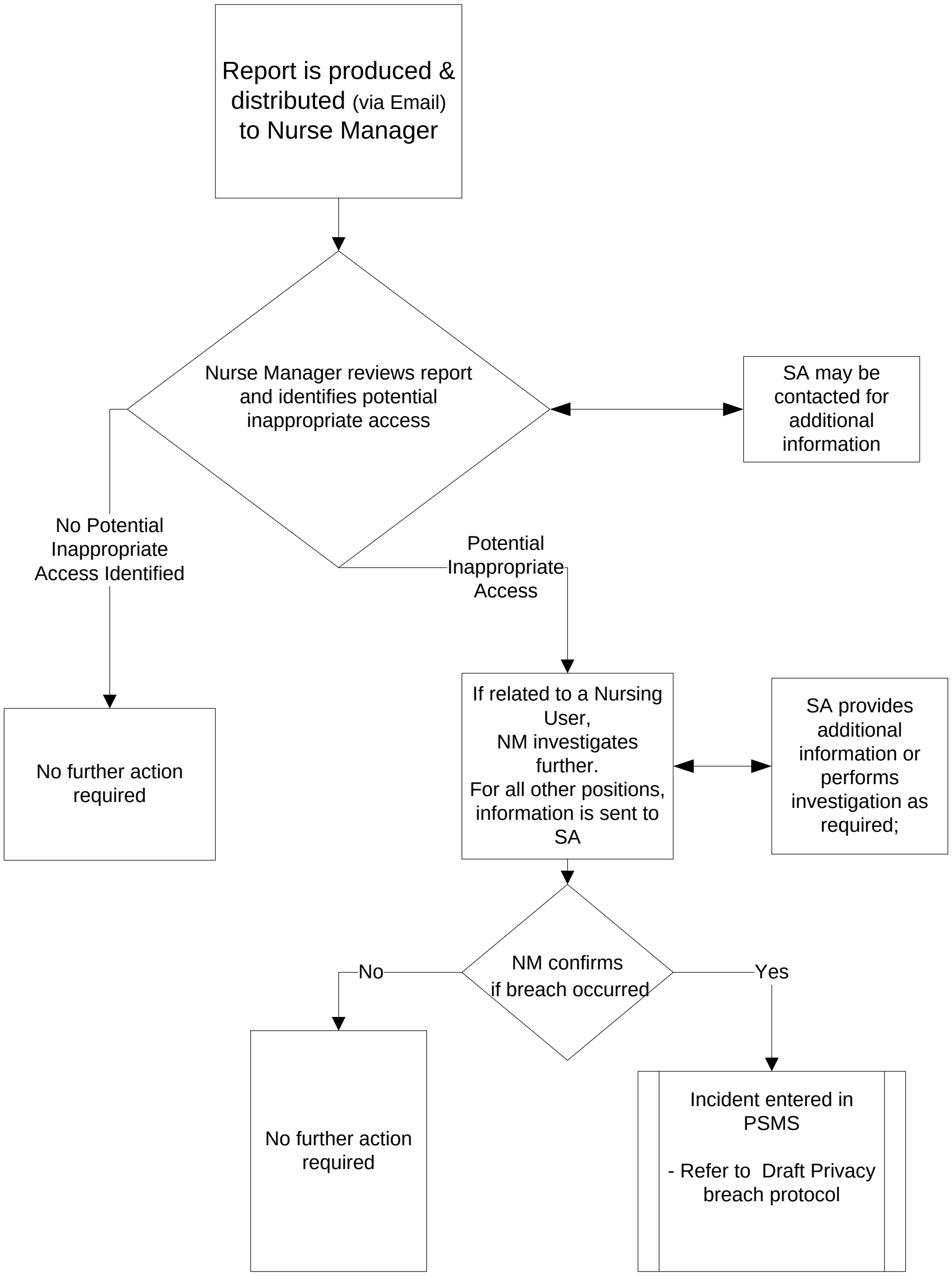
- If additional information is required from the SA, the Manager/Director can request additional information. The SA may use additional audit investigative tools as required.

- If the Manager or Director confirms that no security breach has occurred, no further action is required.

- If a security breach has been confirmed, it is the responsibility of the manager to log an incident in the Provincial Safety Management System (PSMS) as a "Privacy Breach" and follow the appropriate procedure (refer to Draft Privacy Breach Protocol).

  Note: If over the course of the Routine audit, other areas of suspicion or interest are identified, this may trigger additional audits (referred to as Trigger Audits).

CIS Security Audits – Scheduled Nursing Audit by Facility/Unit


Report is produced & distributed (via Email) to Nurse Manager
Nurse Manager reviews report and identifies potential inappropriate access
SA may be contacted for additional information
No Potential Inappropriate Access Identified
Potential Inappropriate Access
No further action required
If related to a Nursing User, NM investigates further. For all other positions, information is sent to SA
SA provides additional information or performs investigation as required;
NM confirms if breach occurred
No
Yes
No further action required
Incident entered in PSMS
- Refer to Draft Privacy breach protocol

CIS Security Audits – Scheduled

Nursing Audit by Facility/Unit

- Unit specific audit reports are automatically generated and emailed to the appropriate Nurse Manager.
  The report:
  - Will be specific to the facility and unit in which the nurse manager is responsible.
  - It will list all of the patients admitted to that particular unit at that point in time (when the report is run).
  - It will identify for each patient, all CIS users (and their credentials) who accessed the patient's chart within the last 2 days.

- The Nurse Manager is expected to review the information within one week of receiving it and identify any potential inappropriate access.

  Inappropriate access may include:
  - CIS Users that, to the Nurse Manager's knowledge, have no legitimate reason for accessing the patient's chart.
  - Any CIS Users with the same last name as the patient and that are not directly involved in the patient's care.

- If additional information is required, the Manager can request additional information from the Security Analysis who may use additional audit investigative tools as required.

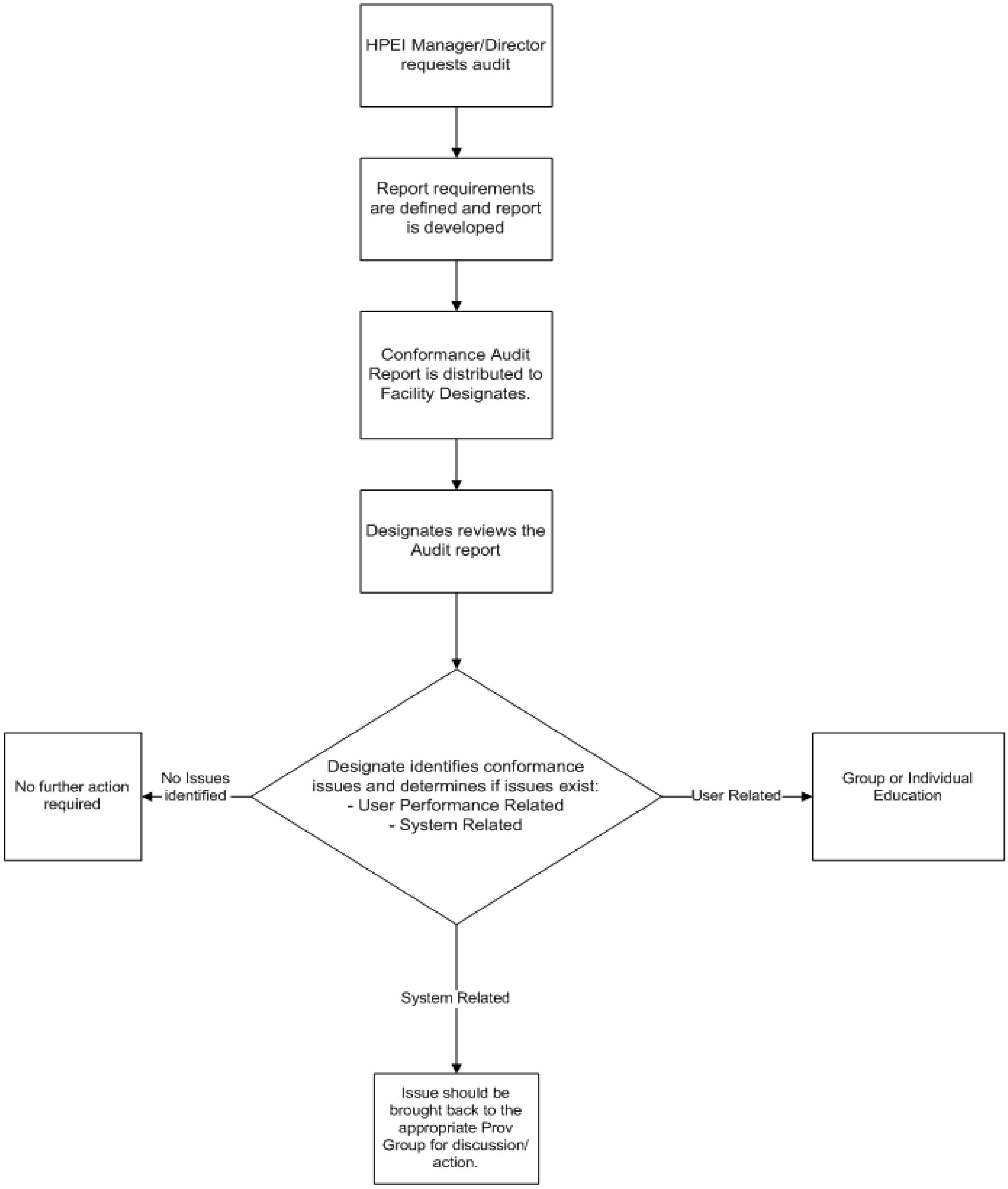
- For any Nursing related positions, the Nurse Manager or supervisor is to perform any additional investigation required to confirm if a security breach has occurred.
  If user's accesses have been flagged outside of "Nursing", this information will be provided to the SA for further investigation/follow up.

- If no security breach has occurred, no additional action is required by the Nurse Manager. The Nurse Manager should notify the Security Analyst that the audit was performed and required no further action.

- If a security breach has been confirmed, it is the responsibility of the Nurse Manager to log an incident in the Provincial Safety Management System (PSMS) as a “Privacy Breach” and follow the appropriate procedure. (Refer to Draft Privacy Breach Protocol)

Appendix B: CIS Compliance Audit Process

CIS Conformance Audit


HPEI Manager/Director requests audit
Report requirements are defined and report is developed
Conformance Audit Report is distributed to Facility Designates.
Designates reviews the Audit report
Designate identifies conformance issues and determines if issues exist:
- User Performance Related
- System Related
No Issues identified
No further action required
User Related
Group or Individual Education
System Related
Issue should be brought back to the appropriate Prov Group for discussion/ action.

Compliance Audits:

- A Health PEI Manager or Director can request a compliance audit if the request meets the following criteria:
    - Must be provincial in nature;
    - Must be sponsored by a provincial group and endorsed by the leadership of the discipline(s) being audited. Request must support a policy, procedure, training guidelines, accreditation standard, project/initiative evaluation or information required to proactively work to avoid high risk patient safety issues.

- Requests should be emailed to Service Centre and directed to the CIS Reporting Group.

- Upon receiving the request, the CIS team will work with the requestor to define the parameters of the request :
    - Purpose/Objective of report
    - Policy/Procedure/Accreditation Standard etc the request will support.
    - Determine how long each indicator is to be monitored (ongoing – or until a benchmark is reached)
    - Identify the provincial group that is responsible for monitoring and the facility designates that will be receiving the report/information for review & action.
    - Identify who will be validating the reports.

- Once the requirements are finalized, the request will be prioritized against the existing list of report needs.
    - Priority will be given as follows:
        - High Risk Patient Safety Issues (QIA)
        - Accreditation Standard
        - Policy/Procedure
        - Training Standard
        - Project/ Initiative Evaluation

- The CIS Reporting Team will develop the report and the identified business lead will work with the team to validate. Once validated, the report will be scheduled and distributed to the agreed upon facility designates.

- Facility Designates will review the information and identify any compliance issues.
    - If there are no issues identified, no further action is required.
    - If compliance issues are identified:
        - User Related (specific to how users are capturing or handling information in the system): will need to be sent to the appropriate group for education.

- System Related (issues with system build i.e. missing orderables, multiple locations to chart information etc) will need to be sent back to the sponsoring provincial group for discussion/action.

Appendix C: CIS Audit Service Implementation Work plan

Project Area	Task	Further Details	Timelines	Status
Planning	Re-design/development of Audit Reports	Redevelopment of CIS Audit Reports in Business Objects: - 2 User Specific Audit Report (Random selection and Selected Users) - Patient Specific Audit Report - Unit Level (Patient) Audit Reports - Patient List Audit Report	Jan 2016 - April 2016	Complete
	Develop of Audit Tracking Application		Jan 2016 – April 2016	Complete
	Development of Implementation Plan & Audit Calendar		April 2016	Complete
Program Communication	Memorandums to Health PEI staff	Reminding Staff that Audits are currently performed and the number of audits being performed will expand.	April 2016	Complete
	Develop and approve communications plan	Approval from CIS Director	Dec2016-Jan2017	Complete
	Develop communication tools	1 Page Hand Out	Dec2016	Complete
	Develop presentation and meeting schedule	Directors of Nursing		Complete
		Allied Health Group (PCH & Community Hospitals)		Complete
		Medical Directors		Complete
		IT/CIS Internal	Dec2016	Complete
		QEH allied health - January (including Pharmacy)	Jan 2017	Complete
		Clerks - Registration	Feb-Mar 2017	Complete
		View Only Users	Mar-August 2017	
Program Model Definition/ Development	Finalize program model		March 2017	Completed
	Approval of program model	OMG meeting in March 2017	May 2017	Completed
	Evaluation and monitoring plan		March 2017	In Progress
Implement Service	**Security Audits:**			

	Security by request	Currently operational		Complete
	Security routine random	Staggered Implementation by Discipline: Nursing - April 2016 Allied health - Physicians - All Other Groups - January 2017		Complete
	Scheduled Security Audits	Develop a process – Nursing Pilot	Jan - Mar2017	Complete
		Implement process - Nursing	May2017 – June 2017	Completed
		Identify other potential discipline scheduled audits	October 2017	
	Compliance Audits:			
	Compliance	Complete Compliance related requests in the CIS Reporting queue	April – June 2017	In Progress
	Compliance nursing	Engage with DONs to identify areas where compliance reports are required, generate a list and prioritize the work.	TBD	
	Compliance doctors	Engage with Medical Directors to identify areas where compliance reports are required, generate a list and prioritize the work.	TBD	
	Compliance Future - allied health and other groups	Engage with AH Managers and other HPEIDONs to identify areas where compliance reports are required, generate a list and prioritize the work.	TBD	
	Communication	Educate to request process and appropriate time to be looking at monitoring requirements (when standards, policies are being drafted etc). Target groups: DONs, HPEI Policy Group, Medical Directors, Allied Health Managers etc		Ongoing

Appendix D: Evaluation Framework

Evaluation Question	Indicator	Method	Data Collection	Data Reporting	Timelines	Responsibility
What is the productivity of the service	# audits, types of audits	counts	data collected ongoing in Y1	reported quarterly to CIS Director and OMC	Ongoing	CIS Security Analyst and CIS Team
Is the service providing information in a manner and time that facilitates appropriate action by the service area	opinion of the utility and timeliness	Survey	data collected at a point in time Y1 (Dec 2017)	reported annually to CIS Director and OMC	March-18	CIS HI Specialist
Is the process for requesting and/or prioritizing audits working well?	opinion of the process	Survey	data collected at a point in time Y1 (Dec 2017)	reported annually to CIS Director and OMC	March-18	CIS HI Specialist
Overall how is the audit service operating? Are there lessons to learn that require the service to adapt in future?	opinion of the quality of operation and lessons learned	Survey	data collected at a point in time Y1 (Dec 2017)	reported annually to CIS Director and OMC	March-18	CIS HI Specialist