eHealth Ontario
It's working for you

Business Continuity Standard

Version: 1.5

Document ID: 3536

Ontario
eHealth Ontario

Document Control

Next Review Date : Annually or otherwise established by the Connecting Security Committee.

Approval History

APPROVER(S)	APPROVED DATE
Connecting Security Committee	2014-12-11
Connecting Security Committee	2018-03-26

Revision History

VERSION NO.	DATE	SUMMARY OF CHANGE	CHANGED BY
1.0	2013-12-20	Nov 2013 version adopted from the cGTA PSWG	Mark Carter
1.1	2014-12-05	Updated policy based on feedback from CSC members. Added definition for Agent, Data Contribution Endpoint and Identity Provider Services. Added requirement to validate business requirements in 1.13; Added necessary stakeholder contact information and communication plan to 1.10.9	Mark Carter
1.2	2014-12-11	Updated based on Dec 11th CSC meeting. 2.12 updated to note that testing of the BCP must include at least one of the three and all must be executed within a three year period. Policy was approved by the membership	Mark Carter
1.3	2015-10-19	Updated policies to note the change in governance. The Steering Committee was replaced by the Applicable Oversight Body. The regional privacy and security committee has been removed from the exemption decision process.	Mark Carter
1.4	2017-03-20	Updated Standard to align with ITSM. The document title was changed from Policy to Standard. EHR Solution definition was updated. Revised controls based on feedback.	Raviteja Addepalli
1.5	March 16, 2018	Updated standard to include Patient access to the EHR.	Geovanny Diaz

Business Continuity Standard

Purpose

To define the requirements and recommendations for creating and implementing business continuity plans to help ensure that:

- Access to [the EHR Solution] remains available or can be restored in the event of a disruption, and
- The flow of personal health information (PHI) to the [the EHR Solution] is not disrupted.

Scope

This standard applies to [the EHR Solution] and all [the EHR Solution] Services, including all Patient Portals/Applications.

For HICs that view, handle, contribute or otherwise deal with PHI to [the EHR Solution] Clinical Data Repository (CDR) or provide identity provider services this standard also applies to:

- The HIC's local access control and identity management infrastructure ("identity provider services") that manages the authentication and authorization used to provision access to [the EHR Solution] (e.g., [the EHR Solution] Security Token Service Solution, Microsoft Active Directory Federation Services 2.0, etc.)
- Direct network connectivity to [the EHR Solution] Provider Portal and administrative functionality, including components in the connection path (firewalls, proxies, etc.)
- The integration of [the EHR Solution] Provider Portal with the HIC's local health information system (HIS) or electronic medical record (EMR) application(s)
- The data contribution endpoints that provide PHI to [the EHR Solution]'s Clinical Data Repository
- The information technology and processes that ensure the quality of the data submitted (e.g., terminology mapping)

This standard does not apply to any HIC, their agents or their Electronic Service Providers who do not create, contribute, view or have access to [the EHR Solution].

Definitions

[The EHR Solution]: [The EHR Solution] and supporting systems designed to store and make available specified electronic PHI from the electronic health information systems of HICs.

[The EHR Solution] includes Patient Portals/Applications (HIC or non-HIC affiliated) that facilitate Patient access to the EHR. These applications may be:

- Provider-Gated (Provider facilitates communication with Patient)
- Direct-to-Patients (Patient has direct access to EHR)
- Patient-Gated (Patient delegates access to a Substitute Decision Maker/additional delegates (i.e., family member, physician)

[The EHR Solution] Program: Also known as the Program Office; consists of Agents and Electronic Service Providers who support [the EHR Solution] including privacy and security-related activities, initiatives and processes.

Applicable Oversight Body: The Applicable Oversight Body is comprised of senior-level executives who oversee all aspects of [the EHR Solution]. See Policy Governance Structure section within the Information Security Policy.

Agent: In relation to a health information custodian, means a person that, with the authorization of the custodian, acts for or on behalf of the custodian in respect of personal health information for the purposes of the custodian, and not the agent's own purposes, whether or not the agent has the authority to bind the custodian, whether or not the agent is employed by the custodian and whether or not the agency is being remunerated. For example, an agent may be an organization, employee or contractor that validates identities of the EHR users on behalf of a HIC; an Agent may perform data correction services for a HIC on their data contribution endpoint.

Electronic Service Provider: A person that provides goods or services for the purpose of enabling a HIC to use electronic means to collect, use, modify, disclose, retain or dispose of PHI, and includes a health information network provider.

Information system: A discrete set of information technology organized for the retention, collection, processing, maintenance, use, disclosure or disposition of information.

Information Technology: Any asset (physical or logical) that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. It includes, but is not limited to, hardware, software, firmware, ancillary equipment, and related resources.

Data Contribution End Point(s): Technology and related processes that provide data to the Clinical Data Repository or are queried to provide data to a Clinical Viewer. Typically, these systems are the Information System (e.g., Hospital Information System, Laboratory Information System, Clinical Information System, HL7 Interface Engine, etc.) that directly connects to [the EHR Solution] to provide clinical data.

Identity Provider Services: Technology and related supporting services, policies, processes, and procedures that are used to create, maintain, secure, validate, assert and manage electronic identities to [the EHR Solution].

Business continuity: The set of activities to maintain access to [the EHR Solution] or tolerate disruption related to its access. These activities may include non-technical elements such as paper-based processes, workflow changes, and resource allocation. These activities may also include the execution of a disaster recovery plan.

Disaster recovery: The set of activities that determine the necessary actions to recover information systems that support the access to [the EHR Solution].

Shall/Must: Used for absolute requirements, i.e., they are not optional.

Should: Used when valid reasons exist in certain circumstances not to implement the requirement; however, the implementer must understand the implications before choosing a different course and must consider implementing compensating controls.

May: The requirement is only a recommendation, or provided as an implementation example and is not intended on being exhaustive.

Standard Requirements

1. Requirements for Health Information Custodians

1.1. HICs must ensure that [the EHR Solution] related identity provider services and data contribution endpoint requirements are embedded in their business continuity strategy and should address the following:

1.1.1. Developing a resilient technical infrastructure including disaster recovery plans.

1.1.2. Coordinating and maintaining business continuity plans and arrangements.

1.1.3. Validating business continuity plans to ensure requirements can be met.

1.2. HICs should ensure that the business continuity strategy identifies the identity provider services and data contribution endpoints to be supported by business continuity plans and arrangements, and records relevant details (e.g., in a business continuity risk register) about:

1.2.1. The business processes they support, and

1.2.2. Key internal and external stakeholders.

Resilience

1.3. HICs should implement methods to reduce the likelihood of their identity provider services and data contribution endpoints malfunctioning, which may include:

1.3.1. Employing up-to-date makes/models of hardware and software that are easily maintained and can meet the requirements of critical business processes.

1.3.2. Giving high priority to reliability, compatibility and capacity during the acquisition process.

1.3.3. Ensuring compliance with common or industry security standards for hardware and software.

1.3.4. Using telecommunication network links and services that are robust and resilient.

1.4. HICs should implement methods to ensure that the availability of their identity provider services and data contribution endpoints are maintained, which may include:

1.4.1. Running the critical information systems simultaneously at multiple locations (e.g., by using hot stand-by or virtualization).

1.4.2. Providing alternative locations from which information systems can be run and administered.

1.4.3. Automatically identifying and recovering transactions following an information system failure.

1.5. HICs should reduce single points of failure in their network, which may include:

1.5.1. Rerouting network traffic automatically when critical network equipment or links fail.

1.5.2. Installing duplicate or alternative network components (e.g., assets, hubs, bridges, concentrators, switches, firewalls and network traffic filters) to critical communications equipment.

1.5.3. Arranging fall-back to alternative points of connecting and links with external service providers.

1.6. HICs should develop a method for dealing with faults on their identity provider services and data contribution endpoints, which may include:

1.6.1. Recording all actual or suspected faults.

1.6.2. Notifying affected parties of faults in a timely manner.

1.6.3. Disabling the systems and services with suspected faults until adequately remedied.

1.6.4. Ensuring that they are repaired or replaced within critical timescales.

Planning

1.7. HICs should have a business continuity plan for each of their identity provider services or data contribution endpoints that are part of the wider business continuity strategy to support their participation in [the EHR Solution].

1.8. HICs should appoint an owner for their identity provider services and data contribution endpoints (or group of related identity provider services and data contribution endpoints) who is responsible for developing, testing, and executing business continuity plans and arrangements for their identity provider services and data contribution endpoints.

1.9. HICs should base their business continuity plan on the results of a risk assessment, which may include:

1.9.1. Assessing the potential business impacts associated with the disruption of critical information systems.

1.9.2. Evaluating the likelihood of critical information systems being disputed by performing a threat risk assessment based on a set of scenarios of possible disasters or disruptions.

1.9.3. Obtaining senior management sign-off for selective suitable business continuity plans and arrangements to treat the risks identified.

1.10. A HIC's business continuity plan for their identity provider services and data contribution endpoints should include:

1.10.1. Conditions for their invocation.

1.10.2. Arrangements for the secure storage of plans (e.g., offsite) and their retrieval in case of emergency.

1.10.3. The maximum tolerable period of disruption, i.e., the maximum period of time the organization can withstand a disruption the information system(s).

1.10.4. A schedule of recovery tasks and activities to be carried out, including emergency fall back and resumption procedures (in priority order).

1.10.5. The roles and responsibilities for carrying out each task and activity.

1.10.6. Information security controls to be applied following invocation of the business continuity plan (e.g., to protect the confidentiality and integrity of PHI).

1.10.7. Tasks to be undertaken following a recovery and restoration (e.g., checking that systems and information are restored to the same state they were in before the business continuity plan was invoked).

1.10.8. Ownership of the specific plan and a record of the most recent review for the adequacy of the plan.

1.10.9. Necessary stakeholder and responsible party contact information and communications plan.

Testing

1.11. HICs should review and test their business continuity plans for their identity provider services and data contribution endpoints annually, which may include:

1.11.1. Simple tests, which involve structured walk-through tests where stakeholders meet to rehearse the business continuity plan using different scenarios.

1.11.2. Medium tests, which involve simulation tests where staff test the business continuity plan using a specific scenarios and parallel tests where alternative facilities are used to avoid disrupting production information systems.

1.11.3. Complex tests, which involve full-interruption tests where the original site is shut down and a complete test is performed at an alternative facility.

1.12. HICs should maintain a record of the execution of the tests with the date, the results, and sign-off from one of their senior level executive (e.g., CIO).

2. Requirements for [the EHR Solution] Program

2.1. [The EHR Solution] Program must ensure that information security and information technology requirements are embedded in their business continuity strategy, and address the following:

2.1.1. Developing a resilient technical infrastructure including disaster recovery plans.

2.1.2. Coordinating and maintaining business continuity plans and arrangements.

2.1.3. Validating business continuity plans to ensure requirements can be met.

2.2. [The EHR Solution] Program must ensure that the business continuity strategy identifies the information systems to be supported by business continuity plans and arrangements, and records relevant details (e.g., in a business continuity risk register) about:

2.2.1. Critical information systems (ranked in order of priority) and the business processes they support, and

2.2.2. Key internal and external stakeholders.

Resilience

2.3. [The EHR Solution] Program should ensure that [the EHR Solution] is robust, reliable and supported by alternate or duplicate facilities.

2.4. [The EHR Solution] Program must implement methods to reduce the likelihood of critical information systems malfunctioning, which must include:

2.4.1. Employing up-to-date makes/models of hardware and software that are easily maintained and can meet the requirements of critical business processes.

2.4.2. Giving high priority to reliability, compatibility and capacity during the acquisition process.

2.4.3. Ensuring compliance with common or industry security standards for hardware and software.

2.4.4. Using telecommunication network links and services that are robust and resilient.

2.5. [The EHR Solution] Program must implement methods to ensure that the availability of critical information systems is maintained, which may include:

2.5.1. Running the critical information systems simultaneously at multiple locations (e.g., by using hot stand-by or virtualization).

2.5.2. Providing alternative locations from which information systems can be run and administered.

2.5.3. Automatically identifying and recovering transactions following an information system failure.

2.6. [The EHR Solution] Program must reduce single points of failure in their network, which may include:

2.6.1. Rerouting network traffic automatically when critical network equipment or links fail.

2.6.2. Installing duplicate or alternative network components (e.g., assets, hubs, bridges, concentrators, switches, firewalls and network traffic filters) to critical communications equipment.

2.6.3. Arranging fall-back to alternative points of connecting and links with external service providers.

2.7. [The EHR Solution] Program should develop a method for dealing with faults, which may include:

2.7.1. Recording all actual or suspected faults.

2.7.2. Notifying affected parties of faults in a timely manner.

2.7.3. Disabling information systems and services with suspected faults until adequately remedied.

2.7.4. Ensuring that critical information systems are repaired or replaced within critical timescales.

Planning

2.8. [The EHR Solution] Program must ensure that a business continuity plan is created for each information system (or group of related information systems) as part of the wider business continuity strategy.

2.9. [The EHR Solution] Program must appoint an owner for each information system (or group of related information systems) who is responsible for developing, testing, and executing business continuity plans and arrangements for their information systems.

2.10. [The EHR Solution] Program must base the business continuity plan on the results of a risk assessment, which must include:

2.10.1. Assessing the potential business impacts associated with the disruption of critical information systems.

2.10.2. Evaluating the likelihood of critical information systems being disputed based on a set of scenarios of possible disasters or disruptions.

2.10.3. Obtaining sign-off from a senior-level executive (e.g., a Chief Information Officer) for selective suitable business continuity plans and arrangements to treat the risks identified.

2.11. The business continuity plan for each critical information system (or group of related critical information systems) must include:

2.11.1. Conditions for their invocation.

2.11.2. Arrangements for the secure storage of plans (e.g., offsite) and their retrieval in case of emergency.

2.11.3. The maximum tolerable period of disruption, i.e., the maximum period of time the organization can withstand a disruption the information system(s).

2.11.4. A schedule of recovery tasks and activities to be carried out including, emergency fall back and resumption procedures (in priority order).

2.11.5. The roles and responsibilities for carrying out each task and activity.

2.11.6. Information security controls to be applied following invocation of the business continuity plan (e.g., to protect the confidentiality and integrity of the information).

2.11.7. Tasks to be undertaken following a recovery and restoration (e.g., checking that systems and information are restored to the same state they were in before the business continuity plan was invoked).

2.11.8. Ownership of the specific plan and a record of the most recent review for the adequacy of the plan.

2.11.9. Necessary stakeholder and responsible party contact information and communications plan.

Testing

2.12. At a minimum, [the EHR Solution] Program must review and test their business continuity plans annually, which must include at least one of the following, with each scenario being tested within a period of three years:

2.12.1. Simple tests, which involve structured walk-through tests where stakeholders meet to rehearse the business continuity plan using different scenarios.

2.12.2. Medium tests, which involve simulation tests where staff test the business continuity plan using a specific scenarios and parallel tests where alternative facilities are used to avoid disrupting production information systems.

2.12.3. Complex tests, which involve full-interruption tests where the original site is shut down and a complete test is performed at an alternative facility.

2.13. [The EHR Solution] Program must maintain a record of the execution of the tests with the date, the results, and sign-off from a senior level executive (e.g., CIO).

Exemptions Any exemptions to this Standard must be approved by the Applicable Oversight Body, who will authorize exemptions only where there is clear justification to do so and only to the minimum extent necessary to meet the justified need.

Enforcement All instances of non-compliance will be reviewed by the Applicable Oversight Body.

The Applicable Oversight Body has the authority to impose appropriate penalties, up to and including termination of the Agreements with the HIC, Electronic Service Providers or termination of the access privileges of agents, and to require the implementation of remedial actions.

References **Legislative**

- PHIPA, ss. 12, 13 and Part V.1
- O. Reg. 329/04, s. 6

International Standards

- ISO/IEC 27001:2005, Information Technology – Security Techniques – Information Security Management Systems – Requirements.
- ISO/IEC 27002:2005, Information Technology – Security Techniques – Code of Practice for Information Security Management
- ISO/IEC 27005: 2008 Information Technology – Security Techniques – Information Security Risk Management
- ISO 27799:2008(E), Health Informatics – Information security management in health using ISO/IEC 27002

eHealth Ontario EHR Policy Documents

- Information Security Policy
- Acceptable Use of Information and Information Technology
- Access Control and Identity Management Standard for System Level Access
- Local Registration Authority Procedures
- Identity Federation Standard
- Business Continuity Standard
- Cryptography Standard
- Electronic Service Providers Standard
- Information Security Incident Management Standard
- Information and Asset Management Standard
- Network and Operations Standard
- Security Logging and Monitoring Standard
- Systems Development Lifecycle Standard
- Physical Security Standard
- Threat Risk Management Standard
- Harmonized Privacy Protection Policies

Canada Health Infoway Reference

- Canada Health Infoway Electronic Health Record Privacy and Security Requirements (Version 1.1 Revised February 7, 2005)

Other

- Information and Privacy Commissioner of Ontario's Guidelines on Facsimile Transmission Security (January 2003)