CPQR
Canadian Partnership for Quality Radiotherapy
PCQR
Partenariat canadien pour la qualité en radiothérapie

Pan-Canadian Emergency Preparedness Framework for Radiotherapy Downtime

---

Developed by the Canadian Partnership for Quality Radiotherapy (CPQR),

a standing committee of the Canadian Association of Provincial Cancer Agencies (CAPCA)

(v1.0 March 31, 2026)

CAPCA
Canadian Association of Provincial Cancer Agencies

Preface

The ***Pan-Canadian Emergency Preparedness Framework for Radiotherapy Downtime*** was developed to support the assessment and enhancement of emergency preparedness and cybersecurity in radiotherapy centres in Canada. Because radiotherapy services depend heavily on interconnected digital systems, they are particularly sensitive to cyberattacks, system failures, and infrastructure disruptions, which can jeopardize continuity of care and treatment outcomes. By establishing pan-Canadian guidelines, practical tools, and coordination mechanisms, this framework aims to address critical gaps in radiotherapy resilience, helping to ensure that radiotherapy centres across Canada can sustain life-saving treatments even during crisis scenarios involving structural failures.

This work is led by the Canadian Partnership for Quality Radiotherapy (CPQR), a standing committee of the Canadian Association of Provincial Cancer Agencies (CAPCA). The development of this framework has been made possible through collaboration and financial support from the Canadian Partnership Against Cancer Corporation and Health Canada.

CAPCA is the only organization representing Canada's provincial cancer agencies and programs involved in cancer control. CAPCA provides a forum for the leaders of Canada's cancer control systems to discuss, learn from and collaboratively address issues that affect the delivery of cancer care in Canada. By focusing on important operational issues, CAPCA works efficiently and responds quickly to urgent and emergent cancer control issues.

CPQR promotes a culture of quality and safety in radiotherapy through national standard-setting, quality improvement initiatives, and data-driven system learning. It stewards the Accreditation Canada radiation treatment program standards and oversees quality improvement efforts of the National System for Incident Reporting – Radiation Treatment (NSIR-RT). CPQR works closely with professional associations, including the Canadian Association of Medical Radiation Technologists (CAMRT), the Canadian Association of Nurses in Oncology (CANO), the Canadian Organization of Medical Physicists (COMP), the Canadian Association of Radiation Oncology (CARO), and other partners to strengthen radiotherapy services through collaboration, innovation, and continuous improvement.

This framework summarizes best practices for emergency preparedness and cybersecurity in the delivery of radiation therapy. It outlines detailed action measures organized by lifecycle domains, and the corresponding resource manual provides tools and templates to support practical implementation tailored to local needs. By adopting this framework, radiotherapy centres can strengthen their emergency readiness and cybersecurity position, protect sensitive patient data, and ensure the continuity of life-saving radiotherapy treatments during disruptive events.

Acknowledgements

A *Radiotherapy Emergency Preparedness Advisory Group* was established, comprising radiotherapy clinical leaders, hospital IT professionals, quality and risk managers, and cybersecurity officers nominated by their respective provincial cancer programs. This approach ensured broad geographic and professional representation across Canada. The Advisory Group supported the development of the framework through structured engagement activities, including a national survey assessing emergency preparedness readiness, scenario-based discussions to identify institutional vulnerabilities, refinement of priority domains for inclusion in the framework, and deliberation on potential pan-Canadian coordination tools and resources.

In parallel, the *Canadian Partnership for Quality Radiotherapy (CPQR) Steering Committee* provided strategic oversight by validating emerging findings, identifying areas requiring pan-Canadian standardization, and ensuring alignment with broader strategic priorities. Their contributions emphasized patient-centred planning, low-tech fallback solutions, and alignment with regulatory requirements. The framework was further strengthened through review and feedback from national and international subject matter experts and stakeholders across disciplines, helping ensure it is practical, relevant, and reflective of real-world clinical and operational environments.

We would like to sincerely thank the following individuals for their time, expertise, and contributions:

Advisory Group Members

Lisa Barbera - Alberta Health Services

Jason Berry - CancerCare Manitoba

Jean-Pierre Bissonnette - University Health Network, Ontario

Dan Bond - Newfoundland and Labrador Health Services

Nick Chng - BC Cancer, British Columbia

Gavin Cranmer-Sargison - Saskatchewan Cancer Agency

Carol-Anne Davis - Nova Scotia Health

Jon Dysart - Horizon Health Network, New Brunswick

Scott Gallant - Vitalité Health Network, New Brunswick

George Hajdok - Alberta Health Services

Gina Henneberg - Saskatchewan Cancer Agency

Joe Ho - Provincial Health Services Authority, British Columbia

Louis-Martin Girouard - CHU de Québec-Université Laval, Québec

Brian Liszewski - Ontario Health (Cancer Care Ontario)

Eshwar Kumar - New Brunswick Cancer Network

Kristi MacKenzie - Canadian Association of Provincial Cancer Agencies

Krista MacLeod - Horizon Health Network, New Brunswick

Donia MacDonald - Newfoundland and Labrador Health Services

Boyd McCurdy - CancerCare Manitoba

Kathryn Moran - Nova Scotia Health

Andrew Moull - Hamilton Health Sciences, Ontario

Natalie Pomerleau Dalcourt - Vitalité Health Network, New Brunswick

Gregory Salomons - Kingston Health Sciences Centre, Ontario

Devin Schellenberg - BC Cancer, British Columbia

Brad Warkentin - Alberta Health Services

Yalda Zarif Zargarian Talasaz - Michener Practicum Student, Digital Health Data Analytics

Reviewers

Marie Ambrosio - Waterloo Regional Health Network, Ontario

Jean-Pierre Bissonnette - University Health Network, Ontario

Stephen Breen - Sunnybrook Health Sciences Centre, Ontario

Renata Chmielewski - Ontario Health (Cancer Care Ontario)

Tim Craig - Niagara Health, Ontario

Louis-Martin Girouard - CHU de Québec-Université Laval, Québec City, Québec

Eric Gutierrez - Ontario Health (Cancer Care Ontario)

Nareesa Ishmail - Ontario Health (Cancer Care Ontario)

Robyn Kraft - Waterloo Regional Health Network, Ontario

Christopher Kwong - Royal Victoria Regional Health Centre, Ontario

Marie-Christine Lapointe - CHU de Québec-Université Laval, Québec

Donia MacDonald - Newfoundland Health Services

Kathryn Moran - Nova Scotia Health

Samuel Peters - European Society for Radiotherapy and Oncology (ESTRO), Switzerland

Nadia Petseva - The Canadian Nuclear Safety Commission, Government of Canada

Petra Reijnders - Maastricht Radiation Oncology Clinic (Maastro), Netherlands

Leah Shuparski-Miller - The Canadian Nuclear Safety Commission, Government of Canada

Jen Smith - Waterloo Regional Health Network, Ontario

Laurie Stillwaugh - Shirley & Jim Fielding Northeast Cancer Centre, Ontario

Tynan Stevens - Nova Scotia Health

Chris Thomas - Nova Scotia Health

Christine Tompkins - Nova Scotia Health

Steven Waytowich - Health Sciences North, Ontario

Shawn Wilson - Nova Scotia Health

Leah Wolfe - Waterloo Regional Health Network, Ontario

Lixin Zhan - Waterloo Regional Health Network, Ontario

Mike Oliver- Health Sciences North, Sudbury, Ontario

Table of Contents

1. Glossary of Abbreviations (Reference)

Abbreviation	Full Term
ADS	Anomaly Detection System
AI	Artificial Intelligence
BCP	Business Continuity Plan
CADRA	Canadian Artificial Intelligence and Data in Radiotherapy Alliance
CD	Compact Disc
CIS	Center for Internet Security
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CNSC	Canadian Nuclear Safety Commission
CPPA	Consumer Privacy Protection Act
CPQR	Canadian Partnership for Quality Radiotherapy
CSF	Cybersecurity Framework
CSA	Canadian Standards Association
CT	Computed Tomography
DC	Downtime Continuous Improvement (Post-Incident Actions)
DICOM-RT	Digital Imaging and Communications in Medicine – Radiation Therapy
DVD	Digital Versatile Disc
ECHO	Enhancing Cybersecurity in Healthcare Organizations
EDR	Endpoint Detection and Response
EHR	Electronic Health Record
EMR	Electronic Medical Record
ESTRO	European Society for Radiotherapy and Oncology
HDD	Hard Disk Drive
HDR	High Dose Rate
HIMSS	Healthcare Information and Management Systems Society
HITRUST	Health Information Trust Alliance
IAP	Incident Action Plan
IDS	Intrusion Detection System
IMS	Incident Management System
IRT	Incident Response Team

Abbreviation	Full Term
ISO	International Organization for Standardization
IT	Information Technology
LAN	Local Area Network
LINAC	Linear Accelerator
LIS	Laboratory Information System
LOA	Letter of Agreement
MFA	Multi-Factor Authentication
MoU	Memorandum of Understanding
MPE	Medical Physics Expert
NHS	National Health Service
NSIR-RT	National Systemic Incident Reporting – Radiotherapy
OIS	Oncology Information System
ORMS	Organizational Resilience Management System
OT	Overarching Enabler (System-Level Support)
PACS	Picture Archiving and Communication System
PDCA	Plan-Do-Check-Act
PHIA	Personal Health Information Act
PHIPA	Personal Health Information Protection Act
PIPEDA	Personal Information Protection and Electronic Documents Act
QA	Quality Assurance
RBAC	Role-Based Access Control
RO	Radiation Oncology
ROIS	Radiation Oncology Information System
RT	Radiotherapy
RTT	Radiation Therapist
R&V	Record and Verify
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SOC	Security Operations Centre
TPS	Treatment Planning System
USB	Universal Serial Bus

Abbreviation	Full Term
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WHO	World Health Organization

2. Introduction

2.1 Radiotherapy Centres Face Growing Operational Risks

Radiotherapy centres operate in complex technical and physical environments and may face a range of risks that can lead to unplanned or extended downtime, affecting critical treatment services.

For the purposes of this framework, *unplanned downtime* is defined as an unexpected interruption to radiotherapy services caused by technical failures, infrastructure disruptions, environmental hazards, cyber incidents, or workforce limitations that prevent the normal delivery of radiation treatment or supporting clinical operations.

Extended downtime is defined as a prolonged disruption to radiotherapy services—typically lasting beyond the timeframe manageable through routine operational workarounds—that significantly impacts the ability to deliver scheduled treatments, maintain clinical workflows, or access critical systems, and may require service modifications, patient triage, or coordination with external partners.

For example, in August 2023, a ruptured pipe at the London Regional Cancer Program in Ontario forced the cancellation of all clinic appointments, significantly affecting patient care.[1] Likewise, in November 2021, severe flooding in Abbotsford, British Columbia, led to the cancellation or delay of approximately 70 patient appointments over a three-day period, while also impacting access to dialysis and other essential healthcare services.[2]

In addition to environmental and technical risks, the rise of cyber threats poses a serious and growing concern for healthcare institutions. High-profile international incidents, such as the 2021 ransomware attack on Ireland's Health Service Executive and the 2018 data breach involving Singapore's SingHealth system, have exposed the potential for widespread service disruption.[3] [4] Similar incidents have occurred in Canada, including the 2023 extended downtime at Windsor Regional Hospital in Ontario, the 2021 cyberattacks on Eastern Health in Newfoundland and Labrador, as well as the 2019 cyber incident at Health Sciences North in Sudbury, Ontario.[5] [6]

Workforce disruptions also represent a significant operational risk to radiotherapy services. The COVID-19 pandemic demonstrated how staffing capacity can be affected by illness, quarantine requirements, burnout, and redeployment, potentially limiting centres' ability to maintain normal operations. In such circumstances, centres may need to triage patients, adjust treatment schedules, or transfer care to partner institutions with available capacity. These challenges highlight the importance of coordinated approaches to workforce planning and mutual support across radiotherapy centres, including mechanisms to share expertise, provide remote support, or temporarily redistribute workload during periods of disruption.

These events underscore the need for a coordinated and resilient approach to emergency preparedness and cybersecurity within the radiotherapy community. In Canada, where healthcare delivery falls under provincial jurisdiction and serves a geographically dispersed population, radiotherapy centres often operate at significant distances from one another. This geographic dispersion and jurisdictional structure can limit the availability of immediate external support during disruptions, reinforcing the need for a national framework to promote consistency, shared standards, and support across centres.

2.2 Development of the Pan-Canadian Framework

The *Pan-Canadian Emergency Preparedness Framework for Radiotherapy Downtime* was developed in 2025 by CPQR and was identified as a key priority in CPQR's 2025–2027 Multi-Year Strategic Work Plan.

The framework provides clear, actionable guidance for managing extended, unplanned downtimes in radiotherapy centres across Canada. It draws on lessons from both local and international incidents and incorporates learnings from global best practices and standards. It equips radiotherapy centres to prepare for, prevent, detect, respond, recover and learn from a wide range of incidents.

Ultimately, the framework aims to:

- Support the uninterrupted delivery of life-saving radiotherapy treatments;
- Strengthen the cybersecurity and operational resilience of radiotherapy services in collaboration with hospital IT departments, health system partners, and external service providers;
- Contribute to safeguarding sensitive patient health data through alignment with institutional cybersecurity governance and best practices.

2.3 Intended Audience

This framework is intended for radiotherapy department leadership (e.g., radiation oncologists, medical physics experts (MPEs), radiation therapists, and departmental administrators), as well as hospital and regional partners, including information technology (IT) services, cybersecurity teams, enterprise risk management, and hospital-wide incident response teams. While radiotherapy programs are central stakeholders, effective implementation requires coordinated action across institutional and system levels. The specific responsibilities for each measure will depend on local governance structures, available resources, and whether functions such as IT security and emergency response are managed within the department, hospital-wide, or at a regional/provincial level.

2.4 Objectives

The following key objectives were identified to inform the development of the framework:

I. **Enhance Resilience:** Improve the ability of radiotherapy centres across Canada to maintain safe and continuous operations during, and recover efficiently after, disruptive events such as natural disasters, equipment failures, and cyberattacks.
II. **Standardize Emergency Preparedness Guidelines:** Provide a consistent, scalable framework that radiotherapy centres of all sizes and technological maturity levels can adopt, ensuring clear, actionable guidelines for managing unexpected extended downtimes.
III. **Promote Secure Data Management and Sharing:** Plan for secure data protection, access control, and inter-institutional sharing that comply with national and provincial regulations.
IV. **Foster Inter-Institutional Collaboration:** Encourage radiotherapy centres to share best practices, coordinate during disruptions, and support one another through standardized communication protocols and mutual support agreements.
V. **Enhance Knowledge Transfer and Awareness:** Provide knowledge transfer opportunities and reference materials to ensure clinical, technical, and administrative staff are prepared to respond effectively to emergencies.
VI. **Facilitate Feedback Collection for Continuous Improvement:** Support a culture of continuous learning by gathering feedback from radiotherapy centres and the broader health system, analyzing incident data, and updating the framework based on lessons learned.

2.5 Flexible and Scalable Across Diverse Clinical Environments

Recognizing the diversity of radiotherapy settings across Canada, from large academic institutions to smaller community clinics, the framework is designed to be flexible and adaptable. Centres operate within varying governance structures, where decision-making authority may reside at the department, hospital, regional, or provincial level, influencing how resources are allocated and how changes are implemented. In addition, centres differ in radiotherapy vendors, IT infrastructures, and levels of technological maturity. As such, the framework supports a range of implementation approaches, from foundational cybersecurity hygiene practices to more advanced threat detection and incident response capabilities, allowing adaptation to local operational realities and organizational constraints.

2.6 Promoting Collaboration

The framework emphasizes the importance of coordinated collaboration within institutions (e.g., radiotherapy programs, hospital IT, cybersecurity teams, clinical engineering, communications, and leadership), across institutions, and across provincial and territorial jurisdictions. Effective

preparation and response to unplanned or extended downtime require clear role definition, shared situational awareness, and aligned decision-making at multiple levels of the health system.

By fostering structured collaboration, shared emergency preparedness practices, and appropriate information exchange, including lessons learned from downtime events, organizations can support coordinated and timely responses to service disruptions. A pan-Canadian learning environment, where experiences, mitigation strategies, and recovery approaches are shared across jurisdictions, strengthens collective resilience and reduces duplication of effort.

Importantly, efforts to preserve continuity of care must be balanced with patient safety, regulatory obligations, and clinical risk management. Alternative workflows or contingency measures implemented during downtime should be formally assessed and governed to avoid introducing unintended clinical or operational risks.

Through integrated collaboration and shared learning, the Canadian radiotherapy community can enhance preparedness, safeguard patient data, and support the safe and resilient delivery of care nationwide.

3. Methodology

The methodology used to develop the *Pan-Canadian Emergency Preparedness Framework for Radiotherapy Downtime* followed a comprehensive, multi-phase approach that integrated international best practices and literature, pan-Canadian data collection, and extensive stakeholder engagement. This approach ensured the framework is both evidence-informed and aligned with the operational realities of Canadian radiotherapy centres. Where appropriate, insights from real-world tool use, such as Security Information and Event Management (SIEM) systems, were mapped to specific action items.[7]

3.1. Environmental Scan

3.1.1. Literature Review

A detailed environmental scan was conducted to evaluate global standards and best practices in emergency preparedness and cybersecurity, and their relevance to radiotherapy. Key references included:

- **ESTRO Cybersecurity Framework**: Developed by the European Society for Radiotherapy and Oncology (ESTRO),[8] this framework presents a six-step lifecycle model tailored to radiation oncology departments. It emphasizes business continuity planning, critical systems identification, technical safeguards, staff training, and continuous post-incident

learning. It specifically addresses cyber threats in radiation therapy, with recommendations for pre-incident resilience to post-incident recovery workflows.[9]

- **ECHO Clinical Cybersecurity Recommendations**: Created by Imperial College London's Institute of Global Health Innovation, the ECHO guidelines aim to enhance cybersecurity maturity in healthcare settings. They include a structured maturity model and practical checklists covering governance, threat detection, incident response planning, and staff awareness. The guidelines highlight multidisciplinary engagement and prioritize patient safety in cybersecurity planning.[10]
- **NIST Cybersecurity Framework (CSF)**: Developed by the U.S. National Institute of Standards and Technology, the CSF is a voluntary, risk-based approach to cybersecurity built around five core functions: Identify, Protect, Detect, Respond, and Recover. It includes detailed categories and subcategories for desired cybersecurity outcomes and maps to a wide range of international standards. CSF is especially valued for its scalability and adaptability across diverse sectors, including healthcare.[11]
- **The World Health Organization's (WHO) Guidance for Business Continuity Planning:** Developed by the WHO Health Emergency Programme Country Health Emergency Preparedness and the International Health Regulations department, it provides a structured, organization-wide lifecycle framework designed to strengthen resilience and continuity of operations across all hazards. It emphasizes key phases, risk assessment, critical-function identification, plan development, simulation/exercise, monitoring and review, with the goal of enabling headquarters, regional and country offices to maintain or restore essential services and respond effectively during emergencies. The guidance aligns with WHO's Corporate Risk Management policy, the United Nations Organizational Resilience Management System (ORMS), and obligations under the International Health Regulations**.**[12]

- **The NHS England and Business Continuity Management Toolkit:** Developed by a Task Group convened by NHS England, it lays out a comprehensive, healthcare-specific toolkit designed to support NHS organizations and providers in maintaining continuity of key services in the face of disruption. The toolkit is structured around the Plan-Do-Check-Act (PDCA) cycle, aligned with ISO 22301 principles and the Business Continuity Good Practice Guidelines 2018.[13]

- **The ISO 22301 – Business Continuity Management System:** Developed by the International Organization for Standardization (ISO), it provides an international standardized framework for organizations to plan, establish, implement, operate, monitor, review, maintain, and continually improve a documented management system

to protect against, reduce the likelihood of, and ensure recovery from disruptive incidents. The standard is applicable to all organizations, regardless of type, size, or nature, and is designed to ensure that organizations can continue to deliver products and services at an acceptable predefined capacity during a disruption**.** [14]

- **The Z1600 Standard, The Canadian Standards Association (CSA Group):** Developed by the CSA Group, a recognized Standards Development Organization accredited by the Standards Council of Canada. The Z1600 series provides comprehensive criteria for organizations to establish, implement, evaluate, and maintain emergency and continuity management programs that address prevention, mitigation, preparedness, response, and recovery. The 2017 edition (Z1600-17) supersedes the previous editions published in 2014 and 2008**.**[15]

3.1.2. Pan-Canadian Emergency Preparedness & Cybersecurity Survey

To understand current Canadian radiotherapy emergency preparedness and cybersecurity practices, a survey was developed and distributed to radiotherapy centres in Canada.

- **Survey Design**: The final survey included 30 mixed-format questions aligned with the six lifecycle domains defined by ESTRO's Radiation Oncology Cybersecurity Framework. Topics covered included legislative compliance, system redundancy, cybersecurity hygiene practices, patient safety protocols, incident response, and real-world recovery strategies.

- **Survey Distribution**: The survey was distributed in collaboration with the Advisory Group to radiotherapy centres in Canada, with targeted outreach to radiotherapy leads, medical physicists, hospital IT teams, and operational directors, depending on each province's organizational structure. In larger jurisdictions, at least two to three responses were sought to capture intra-provincial variation, and at least one detailed response was expected from smaller jurisdictions.

- **Real-World Practice**: Survey respondents were also encouraged to submit existing institutional policies, tools, and procedures to support framework development. Several tools and protocols shared by radiotherapy centres and regional cancer programs provided valuable insight into emergency preparedness practices.

- **Response Rate**: Feedback was received representing 32 radiotherapy centres across all 10 provinces. In some cases, a single submission reflected consolidated input from multiple centres. Overall, this represents over half of Canada's 49 radiotherapy centres, including

two single-LINAC satellite sites in Ontario affiliated with larger regional centres. With participation from every province, the dataset reflects a diverse and pan-Canadian perspective.

3.1.3. Emergency Preparedness Plans and Resources

A number of resources and tools were shared by surveyed Canadian radiotherapy centres, informing the complementary ***Pan-Canadian Radiotherapy Emergency Preparedness & Resource Manual*** and supporting cross-jurisdictional knowledge sharing and opportunities for broader adaptation and scaling. Examples of resources include:

1. **Waterloo Regional Health Network Downtime Process Policy (2025):** This policy outlines a detailed Radiation Oncology Information System (ROIS) downtime response for radiotherapy departments. It includes the activation of a printed downtime protocol, transitioning to offline treatment delivery via USB plan retrieval, manual charting using downtime binders, and reintegrating treatment data post-recovery. The procedure is proactively tested and scheduled for annual training.[16]

   In the framework, this policy supports the Response and Recovery domains by offering a tested operational workflow for ROIS outages, with tools for ensuring treatment continuity, manual documentation, and post-downtime data integrity restoration.

2. **CHU de Québec-Université Laval (UL) Treatment Interruption Guide (2024):** This guide categorizes radiotherapy patients based on the urgency and sensitivity of their condition to treatment delays (Categories 1 to 3). It defines thresholds beyond which compensatory actions, such as dose adjustment or accelerated fractionation, should be implemented. The guide also includes sample workflows and triage strategies, including prioritization algorithms and reallocation of treatment slots, used during past clinical interruptions.[17]

   Within this framework, this guide supports the Preparation and Response domains by offering standardized patient triage workflows and providing clinical rationale for care deferral or adjustment during resource-limited scenarios.

3. **Ontario Health (Cancer Care Ontario) - Emergency Preparedness MoU Checklist (2023):** This provincial tool supports Ontario radiation treatment centres in formalizing emergency partnerships through Memorandums of Understanding (MoUs). It outlines technical and clinical prerequisites for transferring patient care between paired centres during extended service disruptions while supporting specialized programs. The checklist covers financial reimbursement, staffing deployment, medico-legal agreements, DICOM-RT data sharing, and communication protocols.[18]
   Within the Framework, this tool supports the Preparation and Response domains by identifying complex areas of focus when exploring transfer of care between two centres.

4. **Hamilton Niagara Haldimand Brant Regional Cancer Program Letter of Agreement (LOA) – Radiotherapy Redeployment (2021):** This Letter of Agreement (LOA) establishes a legal and operational framework for the temporary redeployment of clinical staff between two healthcare institutions in the event of a service disruption or emergency. It was proactively developed to enable rapid cross-institutional staffing support if required. The LOA outlines key provisions including dual accountability to both the sending and receiving organizations, defined supervision structures, legal indemnification, wage and benefit arrangements, and termination clauses. Although the agreement has not been activated to date, its development reflects advanced preparedness planning. Having such an agreement in place significantly reduces the time and administrative burden required to mobilize personnel during a crisis.
   Within the Framework, this LOA supports the Preparation domain and serves as an example of how formal personnel redeployment agreements can strengthen emergency preparedness, particularly in regions where radiotherapy programs may need to share staffing resources during extended downtimes.[19]

5. **Hamilton Niagara Haldimand Brant Regional Cancer Program Radiation Therapy Consolidation Guidance Document (2020):** This document outlines planning protocols for consolidating radiotherapy services across sites during significant service disruptions, specifically addressing the transfer of activity across centres. It includes logistics planning, transportation coordination, supply transfer, and documentation for patient funding (i.e. billing codes).
   Within this Framework, the protocol supports the Preparation and Response domains by offering surge planning and capacity reallocation protocols, especially for regional service suspension scenarios.[20]

6. **Hamilton Niagara Haldimand Brant Regional Cancer Program Process to Re-Direct Patient Care in Emergency Situations (2021):** This process was developed during the COVID-19 pandemic to address the risk of critical staffing shortages that could compromise the ability of the cancer program to deliver radiotherapy services. It provides an operational framework for safely transferring oncology patients between institutions when local service capacity is significantly reduced. The process map outlines the steps required to identify receiving ("host") facilities, manage clinical role transitions, coordinate radiation treatment delivery, align diagnostic and documentation workflows, reconcile financial considerations, and define communication responsibilities between organizations.
   Within the Framework, the structure and principles of this process informed the Preparation and Response domains by informing continuity of care and regional rerouting strategies during emergency or extended downtime events.[21]

7. **Hamilton Niagara Haldimand Brant Regional Cancer Program Functional Exercise Manual (2021):** This includes a scenario-based tabletop exercise designed to prepare radiation departments for large-scale staff shortages during the COVID-19 pandemic. The exercise outlines structured modules for setting incident objectives, activating command centres, triaging patients, and coordinating communication across partner hospitals. It evaluates institutional readiness, capacity decanting strategies, and the use of consolidated support tools such as prioritization grids and lessons-learned reports Within the Framework, this exercise supports the Preparation and Response domains through simulation-based testing.[22] [23]

8. **Hamilton Niagara Haldimand Brant Regional Cancer Program Incident Management System Manual (2022):** This manual outlines the process for triggering a regional or multi-institutional command centre. It defines roles for key stakeholders (e.g., Medical Leads, Logistics, and Communications) and includes standardized incident management tools such as Incident Briefings and Incident Action Plans (IAPs).[24]

   Within this Framework, this manual supports the Preparation and Response domains through structured tools commonly used in incident management response.

9. **Juravinski Cancer Centre Incident Management System Overview and Incident Action Plan Process Presentation (2021):** This document describes the operational flow and decision-making process for escalating issues to a central coordinating body. It specifies when and how hospitals should engage partners for coordinated response.

   Within the Framework, these workflows inform the Preparation, Response and Recovery domains by sharing standardized communication and escalation levels.[25] [26]

10. **Hamilton Niagara Haldimand Brant Regional Cancer Program Regional Fan-Out List (2021):** A communications escalation tool that maintains an up-to-date contact tree across regional cancer centres to ensure rapid mobilization during emergencies. [19]

Within the framework, this template informs the Preparation and Response domains by offering a standardized tool for documenting key roles and contact information of value during unplanned and extended downtime.

3.1.4. Cybersecurity Tool Integration

Hospital IT departments typically implement cybersecurity tools as part of enterprise-wide security strategies. Radiotherapy programs should be engaged to ensure that these tools do not disrupt critical clinical systems, including treatment planning, R&V systems, imaging, and oncology information systems. The categories of tools described below represent common approaches used in healthcare to enhance cyber resilience. They are provided as illustrative

examples and do not constitute a prescriptive or endorsed list. Selection should be based on local IT policies, clinical requirements, and compatibility with radiotherapy workflows.

1. **Phishing Simulation Platforms:** These platforms educate staff on recognizing and responding to social engineering attacks, particularly email-based phishing threats. Simulations mimic realistic attack scenarios, allowing organizations to assess staff awareness and track improvements over time. Regular phishing simulations have been shown to reduce the success rate of actual phishing attacks.[27]
2. **Security Information and Event Management (SIEM) Systems:** SIEM systems act as centralized platforms for collecting, normalizing, and analyzing log data across IT infrastructure—including network devices, servers, applications, and user endpoints. They provide real-time monitoring and generate alerts based on known threat signatures or anomalous activity.[28]
3. **Endpoint Detection and Response (EDR) Tools:** EDR solutions focus on endpoint-level monitoring (e.g., workstations, laptops, mobile devices). These tools detect and respond to malicious behaviours such as unauthorized access attempts, suspicious software execution, or lateral movement across the environment. Many include automated responses, such as isolating compromised endpoints from the network. EDR is especially valuable in decentralized clinical environments with multiple access points.[29]

4. Framework Design and Development

4.1 Framework Structure

The development of the *Pan-Canadian Emergency Preparedness Framework Radiotherapy Downtime* was guided by a multi-source approach that included an extensive literature review, international benchmarking, and a structured pan-Canadian consultation process. The intent was to ground the framework in global best practices while ensuring its adaptability to the operational and regulatory context of Canadian radiotherapy centres.

A primary reference point for the structural design was ESTRO's Cybersecurity Framework, [9] which offers a lifecycle-based model for enhancing digital resilience in cancer care. Drawing on this model, the Canadian framework was adapted to include six functional domains spanning the full spectrum of cybersecurity and emergency preparedness, from pre-incident prevention through post-incident recovery. These domains anchor a set of targeted action measures that reflect the unique workflow, infrastructure, and inter-organizational challenges of Canadian cancer centres.

The Canadian adaptation integrates clinical, operational, and technical considerations, emphasizing a multidisciplinary approach to resilience building. Key informants across the

country noted that the framework must address not only low- frequency, high-impact events (e.g., ransomware attacks or natural disasters) and complete system outages (e.g., server and system failure), but also system degradation, such as significantly slowed performance or partial feature failures. These degradations occur more frequently than full outages and can be nearly as disruptive to clinical workflow, care continuity, and patient safety. The resulting framework is therefore designed to be scalable, evidence-informed, and grounded in real-world operational vulnerabilities and practice gaps.

4.2 ESTRO's Cybersecurity Framework

ESTRO's framework for radiation oncology departments to mitigate against cyberattacks has six core domains.[9] It presents a six-step model tailored to radiation oncology departments, reflecting a comprehensive lifecycle approach:

1. **Preparation**: Design and prepare emergency and business continuity processes
2. **Prevention**: Implementing technical and organizational safeguards
3. **Detection**: Monitoring systems for signs of disruption or cyber incidents
4. **Response**: Activating incident response protocols, managing communications, and maintaining continuity of patient care
5. **Recovery**: Restoring systems, validating data, and resuming normal operations
6. **Continuous Improvement**: Conducting post-incident reviews and updating plans based on lessons learned

The six domains of cyber and operational resilience in radiotherapy are supported by three complementary categories of action measures. These categories provide a structured way to plan, implement, and evaluate safeguards across technology, organization, and people.

I. **Technological (T):** Hardware, software, and network security solutions
II. **Organizational (O):** Policies, governance structures, and coordination mechanisms
III. **Human-Centred (H):** Staff training, awareness, and attention to human factors

4.3 Pan-Canadian Survey Findings

A survey conducted in 2025 provided a pan-Canadian snapshot of emergency preparedness and cybersecurity practices in radiotherapy centres. While detailed methodology and response rates are described in Section 3, the high-level findings reveal patterns and gaps that directly informed the framework.

Key insights include:

- **Governance and Responsibility:** Cybersecurity and technical system management were generally handled by hospital or health authority IT departments, while clinical preparedness and patient continuity were overseen by radiotherapy program leadership. This highlighted the need for clearer cross-functional coordination and integrated incident response models.
- **Redundancy and Recovery Capacity:** Larger or more centralized centres often had redundancy for critical systems, whereas smaller or rural sites relied on vendor-hosted solutions or had limited backup capabilities.
- **Simulation and Training:** Formal downtime drills, tabletop exercises, and testing of offline workflows were inconsistently conducted, emphasizing the importance of routine simulation to ensure readiness.
- **Inter-Institutional Coordination:** Agreements for patient transfer or staff redeployment during extended downtime were uncommon, underscoring the need for pre-established regional collaboration mechanisms.
- **Common Challenges:** Recurring issues included legacy infrastructure, workforce limitations (IT and clinical physics), funding constraints, and variable vendor engagement to create feasible contingency workflows.

These findings shaped the framework's recommendations on governance, redundancy, training, cross-department and cross-institution collaboration, and structured recovery processes.

4.4 Action Measure Categorization

A total of **194 action measures** were identified and categorized across the six core domains of the *Pan-Canadian Emergency Preparedness Framework for Unplanned & Extended Downtime for Radiotherapy Centres*. These domains (Prevention, Preparation, Detection, Response, Recovery, and Continuous Improvement) mirror the incident lifecycle model adopted from ESTRO, ensuring consistency with international best practices while allowing for local adaptation.

Each action measure was reviewed and assigned to the domain that best reflected its primary operational function within radiotherapy system resilience. While many measures intersected with multiple lifecycle phases, only their most critical alignment was used for classification purposes to avoid duplication and ensure implementation clarity.

To further support interdisciplinary engagement and resource allocation, each action measure was also assigned one of three categorical tags:

- **Technological (T)** – Actions that involve infrastructure, digital systems, software tools, redundancy planning, and cybersecurity infrastructure.

- **Organizational (O)** – Actions focused on governance, policy development, escalation pathways, inter-departmental and inter-institutional coordination, and vendor agreements. *It is important to note that the "Organizational" category includes responsibilities that may extend beyond the radiotherapy program's direct control or influence, encompassing hospital-level leadership, IT departments, provincial authorities, or contracted service providers.*
- **Human-centred (H)** – Actions that prioritize staff training, awareness campaigns, triage simulations, communication workflows, and role clarity.

This dual-level classification (by domain and by type) ensures a balanced approach, enabling institutions to assess their strengths and gaps across technical capacity, organizational readiness, and human resources. By explicitly acknowledging that some organizational actions fall outside the direct sphere of the radiotherapy program, the framework clarifies which measures require collaboration with broader institutional or provincial stakeholders. This approach allows IT teams, radiation program leaders, and policymakers to clearly identify responsibilities and coordinate implementation of specific components of the framework.

4.5 Distribution of Measures by Domain

The action measures were distributed across the framework's six core lifecycle domains, with a small subset categorized as cross-cutting or unassigned due to their broad or foundational nature.

This distribution reflects stakeholder-identified priorities, international best practices, and common points of failure observed during real-world incidents. The allocation also highlights the need for balance across proactive business continuity planning, technical safeguards, real-time incident response, and long-term system learning.

Domain	Number of Measures	Examples
Preparation	40	Risk inventory templates, role mapping, legal agreements, tabletop drills
Prevention	37	MFA[1], patch management, staff phishing training
Detection	17	SIEM[2], anomaly alerting, endpoint monitoring

[1] Multi-Factor Authentication.
[2] Security Information and Event Management

Response	48	Activation of incident command, manual treatment workflows, patient triage
Recovery	22	Restoration protocols, system revalidation, chart reintegration
Continuous Improvement	22	Post-incident debriefs, framework revisions, staff feedback mechanisms
Other	8	Framework dissemination, national oversight coordination, funding advocacy

This breakdown reinforces the need to invest not only in cybersecurity infrastructure but also in governance, training, and post-incident learning. The strong presence of prevention and preparation measures reflects the emphasis placed by both Canadian and international frameworks on proactive risk mitigation.

5. The Framework

5.1. Preparation Domain

Preparation establishes the foundational elements required for coordinated, rapid, and effective responses to downtime events, whether caused by cyberattacks, infrastructure failure, or external emergencies. This domain focuses on building organizational readiness through formalized business continuity planning, governance structures, baseline risk assessments, and stakeholder alignment. It includes developing inventory systems for critical assets, clarifying roles and responsibilities across IT, clinical, and vendor partners, and ensuring familiarity with established frameworks. Preparation also addresses legislative awareness and regulatory compliance by prompting institutions to map their obligations under privacy laws. Canadian radiotherapy centres participating in the pan-Canadian survey consistently identified the lack of formal planning, role clarity, and policy awareness as key barriers to preparedness. As such, this domain integrates real-world insights from across the country, emphasizing pragmatic readiness measures such as system mapping, baseline capability assessments, and integration of cybersecurity into broader emergency planning structures. The actions outlined in this domain serve as preconditions for all subsequent phases in the framework and are essential to embedding cybersecurity and emergency preparedness into the operational culture of radiotherapy programs.

No.	**Action measure**	Cat
PP0 – Preparation in General		
PP0.1	**Understanding of the Vulnerability of Radiotherapy and Healthcare Systems and the Threat from Extended Downtimes**	Organization

	• Build awareness that Canadian cancer centres are at risk from a range of threats, including cyberattacks, hardware or software failures, and environmental emergencies. • Build awareness of the vulnerabilities created by untrained or unaware users and gaps in preparedness. • Build awareness of the need for a constant state of readiness to respond quickly and maintain continuity of care during any extended downtime event. • Build awareness of the value, sensitivity, and regulatory protection requirements of oncology patient data.	
PP0.2	**Understand the Implications of an Unexpected Extended Downtime** • Build understanding of the clinical risks caused by interruptions to radiotherapy treatment, including delayed or missed fractions. • Build understanding of patient safety impacts, including treatment errors from manual workarounds and potential harm from deferred care. • Build understanding of the risks of data loss or breach, including impacts on privacy, compliance, and trust. • Build understanding of reputational risks for cancer programs and partner institutions when services are disrupted.	Organization
PP0.3	**Understanding of the Involved Parts** • Build understanding of who and what can be affected when radiotherapy services are disrupted, including patients, clinical teams, technical staff, IT support, vendors, and administrative functions. • Ensure that employee behaviours, the technologies in use, and all business and clinical processes align with established operational continuity and IT security requirements. • Include consideration of external partners such as regional cancer programs, hospital IT departments, and contracted service providers to ensure coordinated readiness.	Organization
PP0.4	**Understanding the Cost of Preparedness Measures** • Be aware of the resource (human and financial) costs of implementing countermeasures and preventive measures for both cybersecurity and operational downtime readiness (e.g., redundant systems, surge agreements, staff training). • Ensure that a budgeting process is in place to sustain preparedness measures, including regular upgrades, maintenance, and exercises. • When planning budgets, consider the costs associated with recovery from an extended downtime, including system restoration, productivity loss, patient redirection, and reputational repair. • Consider, at the institutional or health system level, whether cybersecurity insurance is appropriate to help offset the financial impact of a major cyber incident. Coverage scope, exclusions (e.g., ransom payments, regulatory fines), reporting obligations, and insurer-mandated security controls should be clearly understood in advance. Decisions regarding procurement and coverage limits typically reside with hospital or regional leadership rather than individual radiotherapy programs, but radiotherapy	Organization

	leadership should understand the implications for downtime recovery and claims processes.	
PP0.5	**Understanding Applicable Canadian Legal, Regulatory, and Policy Requirements** • Identify and document all applicable federal and provincial health information laws and regulations, such as: *PHIPA (Ontario), PIPEDA (federal)*, and equivalent legislation across provinces (HIA in Alberta, PHIA in Manitoba, etc.), and relevant *federal initiatives* (e.g., CNSC regulations, Bill C-27: CPPA & AIDA, pending). • Align downtime, cybersecurity, and recovery measures with recognized regulatory and professional standards, such as Canadian Nuclear Safety Commission (CNSC) licensing requirements and CPQR guidance, to ensure radiotherapy practices meet legal and safety expectations within each jurisdiction. • Integrate legal and regulatory obligations into downtime manuals, MoU agreements, and BCPs (e.g., data sharing under PHIPA/PIPEDA, privacy safeguards for manual documentation). • Ensure staff are aware of these requirements through orientation, refresher training, and annual downtime drills, reinforcing compliance and safe operational practices within the centre.	Organization
PP0.6	**Understanding of the Partner and Stakeholder Landscape** • Radiotherapy programs to identify all internal and external stakeholders essential to maintaining radiotherapy services during disruptions. • Map relationships, roles, and dependencies between cancer programs, hospital IT, provincial networks, and vendors. • Ensure mutual awareness of downtime protocols and escalation pathways.	Organization
PP0.7	**Understanding Communication Requirements During Downtime** • Define who must be informed, by whom, and through which channels during service disruptions. • Ensure communication plans address internal staff, external partners, patients, and the public. • Integrate communication requirements into downtime drills.	Organization + Human-related
PP0.8	**Understanding Recovery Time Objectives and Acceptable Service Interruption Thresholds** • Identify and define the maximum allowable downtime for critical systems before patient care is significantly affected. Recognize that these thresholds may vary by institution depending on local infrastructure, available support from neighbouring clinics, and prior experience with similar incidents. • Establish prioritization criteria for restoring services, considering which systems and processes are most critical to patient safety and treatment continuity. • Document these recovery objectives and acceptable interruption thresholds in business continuity and disaster recovery plans, noting the assumptions, constraints, and rationale that inform them.	Organization + Technical

	• Review and update these thresholds periodically, using lessons learned from actual downtime events, simulations, or system upgrades to ensure they remain realistic and achievable.	
PP1 – Identification of Systems, Tools, Processes and stakeholders and its Weakness		
PP1.1	**Inventory of Hardware, Software, and Network Dependencies** • Maintain a detailed inventory of all hardware and software used in radiotherapy operations, including treatment planning systems, oncology information systems (e.g., ARIA, OPIS), imaging devices, and supporting IT infrastructure. • Describe all devices that communicate with each other, including data flows, defined interfaces, and the network architecture. • Check and update the inventory regularly, ideally through an automated asset management system, and verify accuracy during audits or downtime drills. • Have readily accessible (e.g. printed hard copies) of vendor contacts and other support contacts.	Technical
PP1.2	**System and Process Categorisation** • Identify and broadly classify radiotherapy systems, data, and operational processes according to their relative risk of downtime, data loss, or disruption to patient care, recognizing that a fully comprehensive or highly granular categorization may not be feasible. • Focus primarily on systems under the direct control or influence of the radiotherapy program, such as treatment planning systems, oncology information systems, imaging, and other department-specific operational tools (e.g., scheduling, communication platforms). • Note that hospital-wide systems, such as the EMR, are generally outside the scope and direct control of the RT department, though awareness of their dependencies is important for coordination with hospital IT teams during downtime or recovery planning. • Map major interfaces, dependencies, and potential single points of failure at a high level, to inform prioritization and recovery planning without implying that detailed enterprise-wide system inventories are the responsibility of the RT program.	Technical
PP1.3	**Priorities of Systems** • Set clear priorities for radiotherapy and supporting systems by identifying which are essential for daily clinical operations and which can be temporarily suspended without compromising patient safety. • Define the sequence for restoring systems following an outage, informed by clinical urgency, dependency mapping, operational impact, and applicable regulatory requirements, including Canadian Nuclear Safety Commission (CNSC) compliance obligations for radiotherapy delivery and safety systems. • Ensure that prioritization decisions account for both patient care continuity and regulatory compliance, particularly where downtime could affect licensable equipment or treatment safety thresholds.	Technical

	• Review and update system priorities regularly to reflect changes in workflows, technologies, treatment delivery models, and any updated regulatory guidance.	
PP1.4	**Documentation of Configuration and Integration Points** • Maintain detailed documentation of system configurations, interface settings, and network integration points. • Ensure this documentation is stored securely offline for use during downtime recovery. • Maintain records of major service account passwords for both on-premises and online systems in a safe and secured area.	Technical
PP1.5	**Risk Analysis/Risk Assessment** • Conduct comprehensive risk analyses to identify threats and weaknesses in radiotherapy systems, workflows, and data management processes. These should cover cybersecurity, hardware and software failures, vendor dependencies, and environmental hazards. • Implement the assessment collaboratively, with the Radiotherapy department working closely with hospital IT, clinical engineering, and relevant administrative teams to ensure all technical, clinical, and operational perspectives are captured. The assessment should also account for the **time and resources required** to complete it. • Risk analyses should be conducted at least once annually, and whenever there are changing environments, such as system changes, software upgrades, or workflow changes. • Perform gap analysis to identify major challenges, impacts, and feasible mitigation strategies. • Engage highly qualified personnel (e.g., IT security specialists, medical physicists, clinical engineers etc.) in the assessment process. • Assess feasibility of treatment without critical systems, such as R&V systems, and document risks and mitigation approaches. • Reassess risks regularly, using self-assessment tools where available, and consider consulting third-party risk management services or tools where specialized expertise is needed. Document all findings, mitigation strategies, and roles/responsibilities across RT and hospital IT teams clearly in business continuity or disaster recovery plans.	Technical + Human-related
PP1.6	**Proactive Identification of Vulnerabilities** • Assess the risk and vulnerability of all radiotherapy-related hardware, software (including in-house or custom-developed applications), and vendor-provided services, considering both cybersecurity and operational resilience. This should be performed through a collaborative working group of multi-disciplinary subject matter experts, including radiation oncology staff, medical physicists, IT specialists, clinical engineers, and system vendors. • For in-house or locally developed software, ensure that design, coding, and deployment practices meet security and reliability requirements, including access control, logging, testing, and validation. Document these design considerations as part of the risk assessment process.	Technical

	• Review or perform vendor security audits and third-party risk management assessments, ensuring that service-level agreements (SLAs) address downtime preparedness as well as cybersecurity. • Identify single points of failure and ensure mitigation strategies are in place, such as redundancy, failover systems, or alternative workflows.	
PP1.7	**Stakeholder Management** • Understand the objectives, responsibilities, and roles of all stakeholders, including patients, the healthcare workforce, leadership, vendors, and the full radiotherapy supply chain. • Recognize human factor vulnerabilities (e.g., lack of training, procedural non-compliance) and define strategies to address them through education, drills, and clearly documented protocols. • Establish communication, privacy, and security policies for all stakeholders that apply during both normal operations and extended downtimes.	Organization + Human-related
PP1.8	**Regional Cooperation** • Establish and maintain mechanisms to organize and facilitate regional cooperation for radiotherapy preparedness and downtime response. • Engage both professional and non-governmental organizations, as appropriate, including provincial cancer agencies, hospital networks, and emergency management partners. • Support agreements for mutual aid, resource sharing, and coordinated patient transfers across jurisdictions during extended downtime events.	Organization
PP1.9	**Leverage Past Incident Learnings** • Integrate lessons learned from prior incidents (e.g., COVID-19 staffing gaps, ransomware attacks) into immediate response protocols. Maintain a knowledge base or post-event review archive as part of your continuous improvement processes.	Organization + Human-related
PP2 – Define a Business Continuity Plan (BCP)		
PP2.1	**Business Continuity Plan (BCP)** • Maintain a formal Business Continuity Plan (BCP) as part of overall quality assurance, with accessible hard copies available at workstations for all modalities. • Include predefined procedures for incident response, defined continuity phases, restoration processes, authority involvement, and escalation pathways. These should ensure frontline staff are aware of their roles and escalation responsibilities rather than managing complex or high-risk situations independently. The BCP should also incorporate technical workarounds for systems downtime, with clear guidance on safety assessment and approval processes to ensure that temporary procedures do not compromise patient care or clinical safety. • Where feasible, the BCP should outline provisions for a pre-configured emergency or virtual network (e.g., to connect the OIS, linacs, TPS, and CT systems) that could be activated in the event of a system disruption. This network should be designed to operate independently of the compromised environment and be clearly documented within the BCP. Some Canadian centres have explored or tested isolated ROIS environments or virtual LANs as potential fallback approaches.	Organization + Technical

	• Include communication continuity measures within the BCP, such as dedicated telephone lines or a centralized hotline or call station for patients and referring providers to obtain real-time updates regarding service disruptions. The plan should also define urgent communication pathways to support clinical escalations and triage during downtime, including fallback options such as fax, emergency phone lines, or secure email channels. • Plan for proactive staff support during prolonged disruptions, recognizing the operational and emotional strain associated with extended downtime events. The BCP should outline strategies to support workforce well-being, such as rotating duties to manage workload, conducting regular team debriefs, and implementing leadership or wellness rounds to provide support and maintain situational awareness among staff. • Ensure the BCP also addresses governance for system resilience, recovery processes, and clearly identifies responsible IT, management, and security teams for oversight and decision-making.	
PP2.2	**Communication Plan** • Define communication processes for employees, patients, vendors, management, and external stakeholders. • Include alternate communication means (private email, mobile devices, secure messaging apps). • Identify key personnel, timing, and escalation procedures for internal/external notifications, including legal counsel, law enforcement, and media. • Create communication templates that can be filled in with relevant information and emailed to patients, media, etc. • Develop scripts for staff engaged in direct communication with patients, including responses to commonly anticipated questions. Staff should practice delivering these communications through mock scenarios.	Organization
PP2.3	**Gap Compensation in Treatment** • Maintain radiobiological guidelines, formulae, and tools to compensate for treatment interruptions. • Provide standard documents and calculators to guide dose adjustments.	Technical
PP2.4	**Written Documentation** • Create paper templates for essential radiotherapy-specific records including treatment prescriptions, diagnosis lists, treatment regimens, session notes, admission forms, imaging references and progress tracking etc. • Disseminate concise “how-to” guides and other resources to support accurate handwritten documentation of essential radiotherapy processes, ensuring continuity of care during downtime. • Focus on radiotherapy-relevant clinical and administrative records.	Organization + Technical
PP2.4.1	**Material and Resources** • Ensure all materials and devices needed for continuity are available, such as backup computers, USB-sticks, fax machines, DVD readers, photocopiers, printers, toner, paper, pen/pencil, folders, phone	Organization + Technical

	directories, protocols, downtime checklists, and an extended downtime manual.	
PP2.5	**Treatment without Record and Verify System (R&V)** • Delivering radiotherapy without an R&V system is generally unsafe and not recommended for contemporary treatment, except potentially for very simple palliative cases where risks are minimal. • Any consideration of treating without R&V should be explicitly addressed in CNSC contingency plans and must include strict QA measures, robust verification protocols, and regulatory approval. • The primary focus should remain on maintaining access to R&V systems through redundancy, downtime procedures, and vendor support, rather than attempting full treatment delivery without them.	Technical
PP2.6	**Comprehensive Backup Strategy** • Implement automated, encrypted backup systems for all critical infrastructure. • Follow the 3-2-1-1-0 backup principle: maintain three copies of data, on two different media, with one copy offsite, one offline/immutable, and zero errors upon verification. • Ensure scheduled backup routines include configuration files, patient data, treatment schedules, and QA logs, and are aligned with provincial regulations and vendor specifications.	Technical
PP2.7	**Leadership** • Define senior leadership roles and responsibilities for decision-making and oversight during downtime.	Organizational
PP2.8	**Paying Cyberattack Ransom** • Define in the BCP how ransom demands will be managed, including negotiation protocols and decision criteria. **Important note:** It is not advisable to pay a ransom after a cyberattack for several reasons, including the lack of guarantee that data will be recovered, the risk of encouraging further attacks, potential legal and regulatory consequences, financial loss and hidden costs, and concerns about data privacy.	Organization + Human-related
PP2.9	**Agreement with Neighbouring Hospitals** • Maintain up-to-date key contact lists in electronic and hard copy for neighbouring/partnering cancer centres, including administrative leaders and other essential personnel. • Formalize agreements with other centres to accept patients during outages, and/or redeploy staff across centres, where feasible. Within agreements, ensure data transfer feasibility and risk mitigation for incomplete records are captured. • Define and document, in advance, the minimum clinical dataset required for patient transfer and acceptance at receiving centres. This dataset should be standardized across partner institutions where possible and incorporated into the Business Continuity Plan (BCP), including both electronic and paper-accessible formats for use during extended downtimes.	Organization + Human-related

PP2.10	**Triaging Patients** • Define patient prioritization criteria for treatment during downtime, differentiating between new and ongoing cases and determining referral triggers.	Organization + Human-related
PP2.11	**BCP Simulation and Test Drills** • Define schedules and methods for BCP testing (tabletop, functional, full-scale drills) and update plans based on lessons learned.	Organization
PP2.12	**Vendor Involvement** • Based on local approach, detail the role distinction between that of system vendor and local IT during downtime, backup and service restoration. • Clearly define vendor support roles, such as IT security, backup, and restoration timelines, as well as vendor checks and modification oncer service is restored. • Clarify vendor requirements in advance.	Organization
PP2.13	**Cooperation and Alignment** • As defined by the hospitals BCP, ensure the radiotherapy BCP is integrated with the hospital's overall BCP and security strategy, with leadership and IT teams collaborating.	Organization
PP2.14	**External Experts** • Define processes for engaging external specialists (cybersecurity consultants, digital forensics experts, disaster recovery providers) when internal resources are insufficient. • Identify relevant law enforcement agencies and establish appropriate points of contact in advance (e.g., local police services, cybercrime units). Proactively defining these relationships supports timely notification, coordinated response, and access to security-related expertise or intervention when required.	Organization
PP3 – Specific Roles and Responsibilities /Incident Response Team (IRT)		
PP3.1	**Incident Response Team (IRT)** • Establish a multidisciplinary Incident Response Team with representation from all relevant areas of the radiotherapy program, including radiation oncologists, medical physicists, radiation therapists (RTTs), nursing staff, administrative staff, IT, and medical technology departments. • Ensure the team is trained to respond to both cyber-related and operational downtime events.	Organization + Human-related
PP3.2	**Roles and Responsibilities** • Use a governance framework to clearly define and assign responsibility, authority, and accountability for each Incident Response Team member. • Recognize that roles, responsibilities, and activities during downtime events may differ from normal operations and must be adapted to local conditions and resources.	Organization + Human-related
PP3.3	**Key Personnel** • Identify key personnel within the radiotherapy department and IT who have the education, authority, and formal responsibility to coordinate response actions.	Organization + Human-related

	• Define procedures with the IT security team or Chief Information Security Officer to ensure effective knowledge transfer, continuity, and communication during incidents. • Focus on documented roles, responsibilities, and escalation pathways rather than relying on individual situational awareness, which can fluctuate during high-stress events.	
PP3.4	**External IT Security Partners** • Radiotherapy departments may liaise with hospital or health authority IT and cybersecurity teams to ensure timely escalation and coordination during incidents affecting RT systems. • Establish clear procedures for communication and information sharing with these teams, including what details to provide and who to contact.	Organization
PP4 – Awareness of Legal and Regulatory Requirements		
PP4.1	**Knowledge of Recognised Frameworks** • Radiotherapy programs and associated hospital IT or operational leads should be aware of internationally recognized cybersecurity and business continuity frameworks relevant to healthcare, such as NIST CSF, ISO 27001, HIMSS cybersecurity guidelines, Center for Internet Security (CIS) Controls, and HITRUST CSF.	Organization
PP4.2	**Knowledge of Legal Aspects** • Radiotherapy program leadership, in collaboration with hospital privacy, legal, and IT departments, should ensure that operational, cybersecurity, and emergency preparedness policies reflect applicable Canadian privacy and health data protection laws (e.g., PHIPA, provincial equivalents, PIPEDA), including mandatory breach and incident reporting requirements. • Operational procedures should incorporate CNSC requirements for radiation safety, physical protection of sealed sources, and associated cybersecurity considerations, particularly for high-activity sources used in HDR brachytherapy, Gamma Knife, or Cobalt teletherapy. • Incident response plans must include clear processes for timely regulatory notification when security-related events, system compromises, or breaches affecting sealed source security occur.	Organization
PP4.3	**Access to Cybersecurity Experts** • Ensure the radiotherapy program has ongoing access to cybersecurity governance expertise, such as a Chief Information Security Officer or equivalent hospital-level function. • Establish formal advisory pathways for clinical leaders to consult with cybersecurity and business continuity experts when planning, testing, or updating the BCP. • Document escalation procedures to external specialists when internal expertise is insufficient (cross-reference PP2.14 External Experts, PP3.3 Key Personnel, and PP3.4 External IT Security Partners).	Organization
PP4.4	**Accreditation/Certification** • The radiotherapy program should liaise with the hospital IT department and relevant vendor partners to understand their compliance with recognized IT security standards, such as ISO/IEC 27001.	Organization + Technical

	• Where feasible, incorporate insights from external IT audits and vendor certifications into radiotherapy downtime and cybersecurity planning. • Consider accreditation and certification status as one factor in vendor selection or engagement discussions, in collaboration with procurement and IT teams (see PP2.12 Vendor Involvement).	

5.2. Prevention Domain

Prevention refers to a comprehensive set of proactive safeguards designed to reduce vulnerabilities, strengthen system defences, and minimize the likelihood and impact of service disruptions in radiotherapy operations. These disruptions may stem from cybersecurity incidents, infrastructure failure, vendor outages, or environmental hazards. The Prevention domain emphasizes implementing layered technical, organizational, and procedural controls across radiotherapy-specific and enterprise IT systems. Key strategies include promoting cybersecurity awareness, conducting role-based training, enforcing strong user access and identity management, ensuring timely system patching, maintaining endpoint protection, and segmenting networks to contain potential threats. It also incorporates encryption protocols, secure data storage and archival processes, physical and remote access controls, and robust backup systems, such as immutable/air-gapped/isolated off-site storage strategies, such as cloud. To ensure resilience, these measures are reinforced through regular testing of contingency workflows, including downtime simulations and restore procedures.

No.	**Action measure**	Cat
PR0 – Prevention in General		
PR0.1	**Understanding the Mechanism of System Disruption** • Develop a practical understanding of how technical, cyber, and infrastructure failures propagate through radiotherapy systems and workflows in order to map dependencies between clinical applications, treatment planning systems, oncology information systems, imaging platforms, network services, and external interfaces to identify single points of failure. • Recognize how disruptions, whether malicious (e.g., ransomware encryption, denial-of-service activity) or non-malicious (e.g., misconfigurations, failed updates, hardware degradation), can impair functionality, degrade performance, or interrupt data integrity. • Understand how partial system degradations (e.g., latency, limited feature availability) differ operationally from complete outages and may require distinct mitigation strategies.	Human-related
PR0.2	**Governance** • Establish a formal governance structure that oversees all preventive measures related to system resilience. This structure should define clear responsibilities between hospital/health system IT and radiotherapy department personnel, especially for patching, user access controls, software updates, staff training,	Organization

	and backup verification. Prevention governance should be periodically reviewed and informed by legal obligations, and organizational cybersecurity strategies. Leadership should also foster a clinical culture where preventive actions are prioritized even under high workload conditions**.**	
PR0.3	**Security Oversight and Response Coordination** • Establish or connect to a formal security operations structure, such as a Chief Information Security Officer (CISO), security operations centre (SOC), or a hospital IT unit with defined cybersecurity escalation protocols. For smaller centres or those without in-house cybersecurity analysts, a designated liaison should be identified to coordinate with external IT support and provincial cyber response teams. This ensures real-time threat visibility and unified response when downtime risks emerge.	Organization + Human-related
PR0.4	**External Support and Risk Transfer Mechanisms** • Define, in advance, the processes and contractual arrangements required to access external expertise during major disruptions, including cybersecurity response firms, disaster recovery vendors, legal counsel, and digital forensic specialists. • Ensure that service-level agreements (SLAs) with critical technology vendors (e.g., treatment planning systems, record-and-verify systems, oncology information systems, EMR providers) clearly outline responsibilities, response timelines, escalation pathways, and recovery support during cybersecurity incidents or prolonged outages. • Clarify roles and accountability between the radiotherapy (RO) department, hospital leadership, and hospital or regional IT services. In most settings, enterprise cybersecurity response, infrastructure restoration, and external vendor engagement will be led by hospital IT or regional authorities, while the RO department is responsible for defining clinical requirements, workflow contingencies, and patient safety priorities during recovery. Responsibilities should be documented to avoid ambiguity during an incident. • Where appropriate and determined at the organizational level, consider mechanisms for financial risk transfer (e.g., cyber insurance) to mitigate recovery costs and support continuity of operations. Decisions regarding insurance procurement and coverage scope typically reside with hospital or health system leadership rather than individual RO programs. • Recognize that the structure and implementation of these mechanisms will depend on local governance models, internal capacity, and whether IT and cybersecurity functions are managed at the hospital, regional, or provincial level.	Organization + Human-related
PR1 – Awareness and Training		
PR1.1	**Cybersecurity and Downtime Awareness Culture**	Organization + Human- related

	• Establish and sustain a culture of cybersecurity and downtime preparedness across all staff levels, including clinical, IT, and administrative personnel. • Implement regular staff training programs that build awareness and readiness for all types of downtime scenarios, including cyber incidents, EMR outages, and infrastructure disruptions. • Training should include practical components such as phishing awareness, secure digital practices, offline workflow procedures, and familiarity with local Business Continuity Plans (BCPs) and escalation pathways. • Reinforce awareness through regular dissemination of internal alerts, lessons learned from past cyber and non-cyber downtime events, and organization-wide messaging that clarifies individual roles and responsibilities during outages. • Integrate these efforts into existing institutional quality, safety, and risk management programs to ensure ongoing oversight, accountability, and continuous improvement.	
PR1.2	**Role-Specific Training Programs** • Implement structured, role-specific education for different professional groups (e.g., radiation therapists, radiation oncologists, medical physicists, administrative staff) addressing cybersecurity hygiene, incident reporting pathways, and downtime procedures relevant to their responsibilities. • Ensure training is delivered during onboarding and at least annually thereafter, with updates reflecting evolving threats, technologies, and regulatory requirements. • Include instruction on applicable legal and regulatory obligations (e.g., PHIPA, PIPEDA, provincial equivalents), as well as clear expectations regarding documentation, communication, and recovery processes during an incident. • Focus on building individual knowledge, awareness, and role clarity to ensure staff understand *what to do* and *who to notify* in the event of a disruption.	Organization
PR1.3	**Phishing Simulations and Social Engineering Exercises** • Radiotherapy programs should coordinate with the hospital IT department to ensure staff participate in periodic phishing simulations and social engineering awareness initiatives. • Focus on understanding key lessons and escalation pathways rather than tracking performance over time within the radiotherapy program itself. • Emphasize awareness of suspicious communications and proper reporting procedures to maintain cybersecurity hygiene.	Organization + Human- related
PR1.4	**Vendors and Manufacturers' Awareness** • Include cybersecurity requirements in vendor procurement and contract evaluation processes. Radiotherapy centres should verify that vendors have cybersecurity certifications (e.g., ISO 27001), adequate incident response support, and secure default	Technical

	configurations for medical devices and software. This is especially critical for cloud-based TPS and R&V platforms.	
PR2 – System Patching		
PR2.1	**Update Patches** • Ensure that appropriate systems essential to radiotherapy service delivery are regularly updated with security patches and system updates. • Patching schedules should be coordinated between institutional IT and the radiotherapy program, with consideration of clinical operations and patient safety. • Because many critical radiation oncology applications (e.g., treatment planning systems, record-and-verify systems, delivery consoles) are regulated medical devices and sensitive to their software environment, all patches, operating system upgrades, and configuration changes must be reviewed in consultation with the vendor to confirm compatibility, validated configurations, and regulatory compliance. • Patch deployments must be logged, validated, and tested to ensure continued functionality of clinical software before full production release.	Technical
PR2.2	**Update Procedure** • Establish and document a formal governance procedure for managing system updates and security patches. This procedure should define approval workflows, risk assessment processes, prioritization criteria (including handling of urgent or zero-day vulnerabilities), change management requirements, and documentation standards. • Define clear accountability for decision-making and oversight, specifying which responsibilities reside with institutional IT, hospital cybersecurity teams, and radiotherapy (RT) program leadership. This includes clarifying authority to defer, expedite, or stage updates based on clinical risk, vendor guidance, and operational impact. • Require documented vendor consultation and validation for updates affecting regulated medical device software or systems operating within vendor-supported configurations. • Outline communication and notification protocols to ensure affected clinical and technical stakeholders are informed in advance of planned updates and promptly notified of urgent patching actions. • Incorporate requirements for auditability, including periodic review of patch management performance, exception tracking, vendor advisories, and documentation of risk-based decisions.	Organization
PR2.3	**Control of Changes** • Implement strict change control policies for all radiotherapy systems. Any system modification, whether a patch, configuration change, or upgrade, should follow a structured process that	Organization

	includes testing, approval, validation steps and documentation of what has taken place. • Ensure continued compliance with vendor specifications and safety standards and retire outdated or unsupported systems that pose risks to operational continuity or patient safety.	
PR3 – Endpoint Protection (Anti-virus-software)		
PR3.1	**Protection Software** • Ensure endpoint devices used within the radiotherapy environment, including clinical workstations, treatment consoles, and mobile devices, are protected by appropriate security controls (e.g., antivirus, anti-malware, endpoint detection and response (EDR), and web filtering), in coordination with the hospital IT department. • Recognize that general-purpose systems commonly used within radiotherapy departments (e.g., email access, office workstations, and shared network devices) may present greater exposure to cyber threats than specialized treatment equipment and should therefore be included in protection strategies. • Ensure protection solutions deployed on regulated medical devices or vendor-managed systems are approved by the respective vendors and compatible with supported system configurations. • Deployment or configuration changes to protection software on regulated medical devices should involve consultation and agreement with system vendors, to avoid unintended interference with clinical performance or regulatory compliance. • Where possible, monitor the use of administrative privileges and ensure unusual behaviour is escalated to hospital IT or security teams for review	Technical
PR3.2	**Regular Updates** • All protection software must be updated regularly to defend against evolving threats and minimize the risk of system corruption or failure. • Updates should be centrally managed, with subscription-based definitions, and include automated alerts for outdated or non-compliant endpoints.	Technical
PR3.3	**Protection of Medical Devices and Systems** • Implement and maintain cybersecurity protections on radiation oncology medical devices only in close collaboration with, and with explicit approval from, the system vendor to ensure continued functionality, validated configurations, and regulatory compliance. • Recognize that many radiotherapy systems (e.g., linear accelerator consoles, imaging systems, treatment planning and record-and-verify platforms) are regulated medical devices that operate within tightly controlled software environments. Any security controls, configuration changes, operating system updates, or protection	Organization + Technical

	software deployments must therefore be reviewed and validated with the vendor. • Maintain appropriate separation between general IT asset management and radiation oncology clinical systems, while ensuring coordinated oversight between hospital IT, cybersecurity teams, and the radiotherapy program. • Ensure endpoint and security software does not interfere with system performance, safety controls, or regulatory compliance. Where supported by the vendor, segment these devices within the network to further isolate risks and limit lateral threat movement.	
PR4 – Network Architecture		
PR4.1	**Firewalls** • Ensure enterprise-grade firewalls are deployed and centrally managed to enforce strict traffic control between radiotherapy systems and external or non-clinical networks. • Configure firewall rules according to the principle of least privilege, permitting only explicitly authorized inbound and outbound communications required for clinical operations (e.g., vendor support connections, approved system interfaces). • Regularly review and document firewall rules to remove unnecessary open ports or legacy access pathways that may increase risk exposure. • Ensure firewall configurations are coordinated with hospital IT and cybersecurity teams and aligned with broader institutional security architecture.	Technical
PR4.2	**Network segmentation** • Design network architecture to reduce exposure of radiotherapy systems to broader hospital or public networks, using segmentation strategies appropriate to the local infrastructure and governance model. • Where feasible, logically isolate key systems (e.g., LINACs, imaging servers, treatment planning systems, record-and-verify platforms) through VLANs, subnetworks, or equivalent controls. Recognize that the degree and structure of segmentation will depend on local network architecture and enterprise IT constraints. • Consider implementing micro-segmentation within the radiotherapy environment to further limit lateral movement between systems or functional components. This approach, increasingly regarded as state of the art, enables more granular traffic control and containment. • Segmentation strategies should support malware containment, limit internal propagation of threats, and enable prioritized system restoration during extended downtimes. • Segmentation design and implementation should be coordinated with institutional IT and cybersecurity teams and validated with vendors where regulated medical devices are involved.	Technical
PR5 – User and Access Management		

PR5.1	**Role-Based Access Control (RBAC)** • Define and enforce access privileges based on clinical and operational roles (e.g., Radiation Oncologist, Medical Physicist, Therapist, IT Admin, etc). • Apply the principle of least privilege to limit access to only those systems and datasets essential for role-specific functions. • RBAC policies should support secure fallback workflows during downtime, ensuring that critical users retain access to essential systems or offline tools.	Organization
PR5.2	**Password Policy Enforcement** • Implement robust password policies that include minimum length, complexity requirements, and expiration cycles. • Configure login timeout and auto-lock protocols for unattended terminals in treatment rooms and planning stations. • Ensure password reset options remain operational during system downtime or network isolation (e.g., offline IT helpdesk protocols).	Technical
PR5.3	**Multi-Factor Authentication (MFA)** • The implementation and governance of MFA are typically managed by the hospital or health authority IT department and fall outside the direct scope of the radiotherapy program. • Radiotherapy departments should liaise with hospital IT teams to understand how MFA is applied to systems commonly used within radiotherapy workflows, particularly for remote access or high-privilege accounts. • Where MFA policies affect clinical operations (e.g., access to R&V systems, imaging archives, or other critical systems), radiotherapy staff should be aware of relevant procedures and escalation pathways, including any approved contingency processes during network outages.	Technical
PR5.4	**Access Logging and Monitoring** • Implement real-time logging and monitoring of user activities, especially for elevated accounts (e.g., domain admins, PACS admins). • Establish alert systems for abnormal login behaviour or access to sensitive datasets outside of standard workflows. • Ensure logs are retained and backed up securely, with provisions for manual log reviews if SIEM systems are unavailable during downtime.	Organization + Technical
PR6 – Data Protection		
PR6.1	**Data Encryption** • Encryption of radiotherapy-related data, both in transit and at rest, is typically implemented through hospital IT infrastructure and vendor-supported system configurations. • Radiotherapy programs should work with hospital IT and system vendors to understand what encryption capabilities are supported by clinical systems (e.g., treatment planning systems, oncology	Technical

	information systems, imaging platforms) and how these protections are applied in practice. • Ensure that encryption approaches used for critical treatment data remain compatible with vendor-supported configurations and regulatory requirements. • When planning for downtime or system recovery, consider how encryption controls may affect data access, retrieval, and interoperability during emergencies, and coordinate with IT and vendors to ensure continuity of care.	
PR6.2	**Data Storage and Retention** • Establish and document retention schedules for treatment-related datasets in accordance with provincial health privacy laws and institutional policies. • Ensure that critical data is redundantly stored across systems (e.g., treatment planning servers, vendor-neutral archives), and fallback access pathways are defined to maintain continuity during network outages, vendor service interruptions, or hardware failures. • Develop a clear, actionable data recovery strategy in collaboration with institutional IT and relevant vendors, specifying how data can be restored quickly and safely under different disruption scenarios. • Regularly test backup and restoration procedures to validate accessibility, system compatibility, and recovery times, ensuring that recovery can be achieved even if primary networks are unavailable. • Document all backup, restoration, and testing activities to support operational readiness, auditability, and continuous improvement.	Technical
PR6.3	**Portable Storage Devices Policy** • Develop a standardized protocol for handling portable storage devices (e.g., USBs, external HDDs) used to import/export patient data, including virus scanning and approval workflows. • Limit usage to predefined, monitored endpoints and restrict clinical system access to authorized devices only. • During emergencies, authorized use of encrypted USB keys may support offline patient transfers or manual treatment continuation.	Technical + Human-related
PR6.4	**Secure Archives and Retrieval Systems** • Establish archives for critical treatment and operational data, with metadata tagging and searchability. • Ensure that retrieval workflows support both digital and non-digital formats, allowing radiotherapy teams to locate key information even during extended outages. • Offline archive access protocols (e.g., printed schedules, mirrored drives) should be tested and documented.	Technical
PR7 – Physical and Remote Access Restrictions		

PR7.1	**Secure Remote Access Architecture** • Ensure all remote access to radiotherapy systems is routed through secure VPNs or encrypted tunnels with endpoint verification and access logging. • Access to critical systems should be role-based and time-limited, especially during emergencies or vendor support sessions. • Remote workflows for off-site planning or inter-centre collaboration must meet provincial privacy regulations (e.g., PHIPA, PIPEDA) and include protocols for emergency access without compromising system integrity.	Technical + Organizational
PR7.2	**Access Policy** • Implement formalized policies governing third-party access, including software vendors, IT contractors, and affiliated clinicians. • All external access should be pre-approved, logged, and subject to real-time monitoring. • Emergency service-level agreements (SLAs) should define remote support procedures for extended outages, including backup credentialing and downtime service escalation protocols.	Organization + Technical
PR7.3	**Physical Access** • Restrict physical access to sensitive equipment and workstations through badge authentication or locked clinical areas. • Ensure that servers, R&V systems, and networking hardware are housed in secured rooms with environmental controls and surveillance. • Introduce protocols for rapid lockdown of physical spaces during cybersecurity events, natural disasters or other emergency scenarios. • During downtime, safeguard access to printed backups, offline workstations, and USB devices used for manual treatment delivery. • Conduct regular walkthrough inspections of clinical and server areas to verify that equipment is properly stored, environmental controls are functioning, and physical security measures are maintained.	Organization + Human-related + Technical
PR8 – Backups and Hard Copies		
PR8.1	**Redundant Network and Server Infrastructure** • Develop fallback server and/or isolated local network environments capable of temporarily supporting essential operations during central system or cloud service outages. • For cloud-hosted systems, define contractual and technical mechanisms for rapid failover or local cache access when connectivity is lost.	Technical
PR8.2	**Offline Data Copies** • Identify critical radiotherapy data required to support continuity of care during extended system outages (e.g., patient schedules, contact details, treatment prescriptions, relevant imaging references, and key planning parameters).	Technical

	• Strategies for maintaining access to these data should be developed in coordination with hospital IT policies and security requirements. In some institutions, maintaining data outside the primary network (e.g., on USB drives or standalone systems) may not be permitted, and alternative secure approaches should be considered. • If offline or isolated copies are permitted, ensure they follow institutional security and encryption policies and are limited to the minimum dataset required to support safe clinical decision-making during downtime. • Clearly define procedures for accessing and using these data when primary systems are unavailable, including how staff retrieve and review the information without normal electronic system interfaces (e.g., viewing stored records or printed documentation when network-based systems are inaccessible). • Where applicable, ensure the predefined minimum transfer dataset required for potential patient redirection to another centre is maintained and periodically reviewed with relevant stakeholders.	
PR8.3	**Cloud Storage Resilience** • Ensure cloud-hosted systems (e.g., ROIS, EMRs) have documented contingency plans for no-internet scenarios. Plans should address local access (e.g., cached databases, offline copies), backup connectivity (e.g., 5G), and vendor-supported fallback options. All measures must comply with Canadian privacy laws (e.g.PHIPA, PIPEDA)**.**	Organization + Technical
PR8.4	**Paper Copies** • Have paper copies of critical treatment-related information necessary for continuity of care during system outages. This may include paper schedules, treatment regimens, fractionation details, and contact information. Determine the feasibility of providing patients with simplified or summary hard copies of relevant treatment information (e.g., appointment schedules, treatment instructions) to support continuity of care during downtime, while ensuring privacy and regulatory compliance. • Regularly review which information is essential for manual workflows and ensure printed copies are updated consistently (daily, weekly, or as appropriate).	Organization + Technical
PR8.5	**Data Restore and Validation Procedure** • Define clear, step-by-step procedures for restoring data for each critical radiotherapy system, including the order of restoration, system dependencies, and validation checkpoints after recovery. • Establish formal validation processes to confirm that restored data is complete, consistent, and correctly synchronized with live systems, and to prevent duplication, corruption, or loss.	Technical

	• Schedule and conduct routine restore drills to verify that the documented procedures are effective and that staff can execute them accurately under simulated downtime scenarios. • Record all restoration activities, validation results, and lessons learned to support auditability, continuous improvement, and operational readiness.	
PR9 – Testing of Reaction, Response and Recovery Plans		
PR9.1	**Testing Business Continuity Plan** • Conduct annual or biannual tabletop exercises simulating extended downtime scenarios (e.g., cyberattack, EMR failure, flood). Exercises should include clinical leads, IT teams, and regional partners. Debriefings must feed into BCP updates. • Schedule regularly testing of the recovery procedures and update recovery plans accordingly.	Organization + Technical
PR9.2	**Downtime Simulation Drills** • Conduct simulation drills involving real-world downtime scenarios, such as IT system failure, clinical software outage, or cybersecurity incident. • Involve interdisciplinary teams (e.g. radiation therapist, oncologist, medical physicists, IT support, and administrative staff) to test response workflows, communication protocols, patient continuity strategies, and patient transfer processes, including transfer of patient data, where applicable. • Use dummy patients, offline documentation, and non-production systems whenever possible to safely simulate clinical operations. • Perform tabletop or low-fidelity drills at least annually, and conduct full-scale functional simulations every 1-2 years, or more frequently if major system changes, new technology, or staffing changes occur. • Document lessons learned from each drill and update downtime procedures accordingly to continuously improve readiness.	Organization
PR9.3	**Analog Workflow Testing** • Periodically test complete treatment workflows using paper-based records and offline protocols in a controlled, simulated environment rather than with real patients, to validate that staff can execute downtime procedures safely. • Ensure simulations are conducted in parallel with normal processes, using dummy patients or test datasets to avoid compromising clinical safety or regulatory compliance. • Focus on identifying potential gaps, human errors, or workflow inefficiencies that could occur during an actual downtime event, without relying on paper-based workflows for real patient care when safe electronic systems are available. • Document lessons learned and update downtime procedures to strengthen readiness, minimize risk, and support training for clinical staff.	Organization
PR9.4	**Audits**	Organization

	• Engage certified vendors to assess infrastructure vulnerabilities through external audits. Ensure audit recommendations are tracked and integrated into BCP updates.	
PR9.5	**Penetration Tests** • Penetration testing of hospital networks and clinical systems is typically conducted at the institutional or health authority level by hospital IT or cybersecurity teams and may require organizational authorization. • Radiotherapy programs may liaise with these teams to understand whether radiotherapy-related systems are included in such assessments and to identify any findings that could affect treatment continuity or patient safety. • Where relevant findings are identified, radiotherapy leadership should coordinate with IT and vendors to understand potential operational impacts and support appropriate mitigation planning.	Technical

5.3. Detection Domain

The Detection domain focuses on the early identification of threats, anomalies, and infrastructure failures that may compromise the safe and continuous delivery of radiotherapy services. In the Pan-Canadian context, this domain is not limited to cyber threats but also encompasses broader sources of system downtime, such as software failures, vendor disruptions, or infrastructure outages. Proactive monitoring, staff vigilance, and clear communication channels are essential for early recognition and containment. Canadian centres reported varied capacity in leveraging tools such as SIEM (Security Information and Event Management), anomaly detection systems, and internal escalation protocols. The following table outlines actionable measures customized to the Canadian context, supporting timely detection, threat visibility, and rapid situational assessment across all forms of digital disruption.

No.	**Action measure**	Cat
DE1 – Real Time Detection		
DE1.1	**Surveillance of Networks** • Ensure monitoring tools and continuous surveillance, detection and response tools are utilized by all networks accessed by the department	Technical
DE1.2	**Surveillance Systems Awareness** • Radiotherapy programs should document the institutional IT or cybersecurity contacts responsible for monitoring intrusion detection systems (IDS) and anomaly detection or monitoring systems (ADS) that may impact radiotherapy infrastructure. • Define clear escalation pathways between the radiotherapy department and hospital IT/security teams in the event that suspicious activity affecting radiotherapy systems is identified.	Technical

	• Where relevant, ensure radiotherapy-specific systems or networks are included in institutional monitoring programs, in coordination with hospital IT and vendors.	
DE1.3	**Recognition of Suspicious Activity** • Learn to recognise what is suspicious activity and may represent the harbinger of a cyberattack. • These include slow network performance, increased network traffic, receipt of emails from known fraudulent sources, unexpected changes in key files on network drives, unusual activity in privileged accounts, tampered file and registry configurations, large amounts of compressed data in unused system areas. executable email attachments, unexpected changes in key files on network-attached drives, unknown processes encrypting files, or significant increases in network traffic on unexpected ports	Technical + Human-related
DE1.4	**Having the Correct Tools for Surveillance** • Ensure that appropriate monitoring and detection tools are in place to maintain situational awareness across all critical radiotherapy systems. This includes tools for network traffic analysis, endpoint monitoring, event logging, and anomaly detection. • Surveillance tools should support early identification of system disruptions, cybersecurity incidents, or operational failures, enabling timely intervention and mitigation. • Select tools that are compatible with the clinical environment and do not interfere with treatment delivery or regulatory compliance requirements. • Integrate surveillance tools into the broader incident detection and response strategy, with clearly defined roles for monitoring, alert escalation, and remediation. • Regularly review and update the tools, configurations, and alert thresholds to adapt to evolving threats and changes in the IT and clinical environment.	Technical
DE1.5	**Review of Detection Systems** • Detection systems are typically maintained and reviewed by hospital IT or cybersecurity teams in response to evolving threats, including zero-day vulnerabilities. • Radiotherapy programs should maintain communication with institutional IT/security teams to understand how updates or changes to detection systems may affect radiotherapy infrastructure or workflows. • Ensure clear escalation pathways are in place so potential threats impacting radiotherapy systems can be promptly communicated to the appropriate IT/security teams.	Technical
DE1.6	**Testing Detection Systems** • Ensure that detection systems are tested in your organisation on a regular basis.	Technical, Organization
DE1.7	**Security Operations Centres**	Organization

	• Radiotherapy departments should have access to cybersecurity experts or Security Operations Centers (SOCs), either internally or through third-party arrangements, to support threat detection and initiate response protocols during or outside of business hours	
DE1.8	**Staff Vigilance and Reporting** • Promote a culture of vigilance by encouraging staff to report unusual system behaviour or suspicious communications. • Use awareness campaigns to frame staff as "human firewalls" and include reporting pathways in downtime training	Organization
DE1.9	**Incident Feedback and Learning Loop** • Ensure all reported suspicious activities, whether they result in actual incidents, are reviewed and used as learning opportunities. Lessons should be documented and fed back into training, system configuration, or policy updates.	Organization
DE1.10	**Cross-Institutional Threat Sharing** • Foster relationships with provincial cancer agencies, hospital partners, and national bodies (e.g., ISMP Canada for NSIR-RT, CPQR) to enable timely sharing of threat intelligence and downtime triggers. Use existing networks (for alerts and case sharing.	Organization
DE1.11	**The Role of Artificial Intelligence (AI) in the Early Detection of Cyberattacks** • Recognize that AI is increasingly being incorporated into cybersecurity tools to support early and comprehensive detection of suspicious activity. • Emerging AI algorithms can analyze patterns across networks, endpoints, and applications to identify anomalies or potential threats more quickly than traditional rule-based systems. • While AI tools are still evolving, awareness of their capabilities can help radiotherapy programs plan for future integration, enhance monitoring strategies, and improve response times to potential cyber incidents. • Stay informed about vendor offerings and industry best practices to evaluate how AI-enabled security solutions can complement existing cybersecurity measures without disrupting clinical workflows.	Technical
DE2 – Communication Process		
DE2.1	**Rapid Communication During Downtime** • Establish structured, rapid communication protocols to be activated immediately upon detection of any significant downtime event. • Communication should follow predefined escalation pathways involving radiation oncology leadership, clinical operations teams, IT/cybersecurity units, hospital command centres, and regional cancer program stakeholders. Ensure multi-channel options are pre-configured, accessible offline, and tested regularly.	Organization

	• Define clear roles, responsibilities, and timing for each escalation step to minimize confusion and delay during critical events.	
DE2.2	**Proactive Integration with IT and Operations** • Foster continuous collaboration between radiotherapy teams and institutional IT/operations departments to ensure mutual understanding of system interdependencies and clinical priorities during interruptions. • Incorporate radiotherapy-specific workflows and safety-critical systems into broader institutional continuity plans. • Identify designated IT and operational liaisons with knowledge of RT infrastructure to ensure prompt alignment in response actions, decision-making, and communication flow during an emergency.	Organization
DE3 – Understanding Service Impact (Operational Awareness)		
DE3.1	**Loss of Access to Electronic Health Records (EHRs)** • Have predefined contingency workflows to reinstate paper records, ensuring continuity of patient identification, treatment tracking, and communication with referring providers.	Technical
DE3.2	**Loss of Access to Imaging System** • Establish alternative strategies for accessing essential imaging data during system outages in coordination with hospital IT and privacy policies. • Approaches such as transferring imaging data via portable media (e.g., CD-ROM/DVD) should only be considered where permitted under institutional policies and must comply with applicable privacy and security requirements for personal health information. • Where possible, prioritize secure, institutionally approved methods of image sharing or retrieval to support continuity of care when coordinating treatment across institutions or during patient transfers.	Technical + Organization
DE3.3	**Lack of Access to Laboratory Information Systems (LIS)** • Access to laboratory information systems is typically managed at the hospital or institutional level and is generally outside the direct scope of the radiotherapy program. • In situations where laboratory results are required to support radiotherapy care (e.g., treatment eligibility or concurrent systemic therapy coordination), radiotherapy staff should follow institutional procedures for obtaining critical results during system outages, in coordination with the relevant clinical services and hospital IT teams.	Technical + Organization
DE3.4	**Overall Impact on Radiotherapy Service** • Assess the potential impact of system downtime on radiotherapy operations, including access to patient records, diagnostic and planning tools (e.g., OIS, TPS), scheduling systems, and linear accelerator configuration. • Plan and document response strategies that account for varying impact levels, including staged restoration of services, safe patient	Technical

	rerouting, or use of validated manual workflows where clinically feasible. • Assign responsibilities for monitoring affected systems and coordinating recovery efforts in collaboration with hospital IT and other relevant departments.	

5.4. Response Domain

The Response domain focuses on immediate actions required to contain, stabilize, and manage the impact of an unplanned downtime incident, whether caused by cyberattacks, infrastructure failure, or natural disasters. This section outlines pragmatic and jurisdictionally relevant measures to activate response teams, maintain patient safety, engage IT and clinical leadership, and restore partial or full treatment operations under constrained conditions. It emphasizes regulatory reporting requirements (e.g., OIPC), inter-institutional mutual aid strategies, and patient-centred communication, particularly in the context of health data privacy laws such as PHIPA. It also acknowledges the importance of local governance structures, surge staffing, analogue workflows, and treatment continuity strategies tailored to both large urban centres and rural facilities. The following table summarizes the action measures associated with the Response phase, grouped across general actions, incident team coordination, system isolation, vulnerability remediation, and continuity of care.

No.	Action measure	Cat
RS0 – Initial Assessment and Impact Identification		
RS0.1	**Immediate Assessment of the Situation** • Obtain a rapid overview of the incident and assess its scope, including affected systems, potential patient impact, and possible vectors of compromise. • Initial containment measures should focus on segmented isolation of affected systems rather than shutting down the entire hospital network. Complete network shutdown should be considered only as a last resort, for example if there is no segmentation or insufficient detection capability. • Any decision to disconnect or shut down network segments must be made in close coordination with the hospital IT and cybersecurity teams, and servers, PCs, and other clients should remain powered on to preserve forensic evidence for investigation. • As a general precaution, temporarily restricting internet access may help limit external propagation of malware, but procedures must allow unaffected systems or network segments to be restored quickly to maintain clinical operations. All containment steps, escalation criteria, and coordination responsibilities should be predefined in the Business Continuity Plan	Technical

	(BCP) and tested during simulation drills to ensure rapid, safe, and legally compliant response.	
RS0.2	**Mitigation** • Assess the situation to identify potential ways to limit harm, contain disruptions, or prevent escalation. • Evaluate immediate and feasible mitigation actions, such as isolating affected systems, switching to offline workflows, or activating backup procedures. • Prioritize mitigation actions based on patient safety, data protection, and continuity of care. • Document all mitigation steps taken, including rationale and outcomes, to support post-incident review and continuous improvement.	Technical
RS0.3	**Network Segmentation** • Assess whether critical systems can be isolated or segmented to maintain partial service continuity during an incident. For example, treatment planning and oncology information systems (ROIS) may be operated on a secure, “clean” network segment while affected systems are contained. • Consider both macro-segmentation (separating the radiotherapy network from the broader hospital network) and micro-segmentation (isolating smaller clusters or individual devices) to limit exposure and contain threats. • Confirm that segmentation strategies are compatible with clinical workflows and do not introduce safety risks or violate regulatory requirements. • Document segmentation configurations, dependencies, and procedures for activating isolated networks as part of the BCP. • Coordinate with IT and vendors to ensure that isolated segments maintain connectivity to essential data and that restoration to full service is smooth once the incident is resolved.	Technical
RS0.4	**Identify Unaffected Systems** • Review all radiotherapy systems (e.g., TPS, CT scanners, LINACs, ROIS) to determine which remain operational and unaffected by the incident. • Assess whether these systems can safely continue providing partial services while affected systems are isolated or under maintenance. • Prioritize continuity for urgent patient treatments, ensuring that using unaffected systems does not compromise safety, quality, or regulatory compliance. • Document which systems are available, their operational status, and any limitations on their use during the incident. • Coordinate with clinical, physics, and IT teams to implement temporary workflows that leverage unaffected systems while maintaining accurate records and minimizing patient impact.	Technical
RS1– Operational Response Foundations		

RS1.1	**Patient Safety as Central Principle** • Patient safety must guide all decisions during downtime. Evaluate risks of fallback methods such as file mode delivery or use of analogue workflows without Record & Verify (R&V) systems. Document rationale for using non-standard techniques and consult clinical leadership before resuming modified treatments.	Organization
RS1.2	**Redeployment of Personnel and Risk Mitigation** • Define internal redeployment strategies for staffing, as required. • Assess skill gaps when assigning alternate duties and apply buddy systems, supervision protocols, or reduced workload expectations to manage clinical risk.	Organization
RS1.3	**Leadership Mobilization** • Mobilize leadership teams immediately, including Radiation Oncology (RO) department heads, program managers, and IT security leads. • Activate established leadership structures to support timely operational decision-making, with higher-risk or system-level decisions escalated through the institutional command centre.	Organization
RS1.4	**Radiotherapy Prioritization in IT Recovery** • Work with hospital IT teams during recovery to prioritize restoration of radiotherapy systems, recognizing their dependence on specialized digital infrastructure. • Ensure radiotherapy needs are actively represented in institutional IT recovery prioritization, particularly where multiple critical services are competing for restoration.	Organization
RS1.5	**Surge Staffing Provisions** • Incorporate feasible surge staffing models into the BCP, such as extending shifts, offering overtime, temporarily increasing hours for part-time staff, and reallocating qualified personnel from lower-priority or non-urgent activities. These measures should represent the first-line surge response. • Define clear activation triggers for surge measures (e.g., downtime exceeding 24 hours, significant treatment backlog, reduced system capacity) and outline approval and escalation pathways consistent with institutional labour agreements and fatigue-management policies. • Depending on the anticipated or confirmed duration of downtime, progressively activate more complex surge strategies. For extended disruptions, this may include leveraging regional mutual aid agreements, cross-training personnel for essential functions, or engaging retired or former staff who maintain active licensure and credentials. Such measures should only be relied upon if credentialing, occupational health clearance, and HR onboarding processes have been addressed. • Coordinate all surge staffing decisions with hospital leadership and human resources to ensure compliance with regulatory	Organization

	requirements, collective agreements, and occupational health standards. • Communicate expectations transparently to staff, including anticipated duration, workload redistribution, and available supports to reduce fatigue and maintain patient safety.	
RS1.6	**Incident Log keeping and Documentation** • Document all decisions and actions taken during downtime using a standardized Incident Action Plan (IAP) format or downtime-specific record-keeping toolkits. Include timestamps, responsible parties, decisions made under constrained conditions, and supporting rationale for later audits or medicolegal reviews.	Organization + Human-related
RS1.7	**Group-Based Decision Making** • Establish predefined multi-role decision teams (e.g., radiation oncologist, radiation therapist, IT representative, medical physicist) to coordinate actions during downtime. • Clearly define roles, responsibilities, and escalation pathways so that decisions are documented, accountable, and aligned with patient safety and institutional policies. • Ensure that the team has access to all relevant information and predefined protocols to guide decisions, rather than relying on ad hoc consensus.	Organization + Human-related
RS1.8	**Interdependencies with Other Departments** • Anticipate cascading effects of downtime in radiology, lab, pharmacy, and other services. Activate and/or define fallback protocols for essential imaging transfers (e.g., CD-ROM use for PACS outages), manual lab requisitions, and centralized medication tracking.	Organization + Human-related
RS2– Incident Response Team Meetings		
RS2.1	**Activate the Radiotherapy Incident Response Team (IRT)** • Initiate the RT-specific IRT promptly upon identifying significant downtime (cyberattack or other disruption). Follow roles and response steps defined in the BCP, mobilizing relevant clinical, technical, and admin leads.	Organization
RS2.2	**Incident Command Structure and Coordination** • Establish a structured meeting cadence for the Incident Response Team (IRT), scaled to the severity and phase of the incident. During the initial assessment and containment phase, meetings may occur multiple times per day; as the situation stabilizes, frequency may taper to daily or as required. • Document all meetings, decisions, action items, and assigned responsibilities to ensure accountability, regulatory traceability, and continuity across shifts. • Designate a formal Command Centre, either physical or virtual, to serve as the central coordination hub for incident management. This location should be predefined in the BCP and activated immediately upon escalation.	Organization

	• Ensure the Command Centre is equipped with essential resources, including communication tools (secure phones, alternate email access, radios if needed), hard copy contact lists, downtime manuals, system inventories, escalation pathways, and documentation templates. • If physical co-location is not feasible (e.g., infection control restrictions or infrastructure limitations), implement a secure virtual command structure with clearly defined access controls and backup communication methods.	
RS2.3	**Designate a Command Centre** • Use a designated space (physical or virtual) for Incident Response Team operations, equipped with essential tools, records, and communication systems.	Organization
RS3 – Activate Business Continuity Plan (BCP)		
RS3.1	**Activate the Business Continuity Plan** • Activate the business continuity plan (BCP). Analyse the actual situation and follow the according procedure defined in the BCP defined for this situation.	Organization
RS3.2	**BCP Adaptation** • As the predefined BCP may not cover the current situation or circumstance make sure to be able to adapt the plan accordingly – in the beginning after analysing the situation and during the crisis.	Organization
RS3.3	**Paying the Ransom** • Define in the BCP how ransom demands will be managed, including escalation pathways, decision-making authority, legal consultation requirements, involvement of cybersecurity insurers (if applicable), and coordination with law enforcement. • Decisions regarding ransom payment must be made at the highest institutional leadership level, in consultation with legal counsel, cybersecurity experts, insurers, and relevant authorities. • As a general principle, paying a ransom is discouraged because it does not guarantee data recovery, may expose the organization to repeat attacks, can create legal or regulatory risks (including sanctions violations), and may undermine broader cybersecurity deterrence efforts. The BCP should therefore prioritize prevention, containment, system restoration, and validated backup recovery as the primary recovery strategies. • If negotiation or communication with threat actors becomes necessary, this should be conducted only through qualified external experts (e.g., cyber incident response firms) and never by clinical or operational staff.	Organization + Human-related
RS4 – Isolate Infected Systems		
RS4.1	**Isolate Compromised Network Sections** • Disconnect the affected segments of the network and ensure unaffected areas can continue to function where possible. Internet access may also need to be temporarily suspended. This isolation	Technical

	supports containment and allows investigations to proceed in a secure manner.	
RS4.2	**Emergency or Virtual Network** • If feasible, activate a pre-configured emergency or virtual network (e.g., to connect the OIS, linacs, TPS, and CTs). This network should operate independently of the compromised system and be defined in your BCP. Some Canadian centres have tested isolated ROIS environments or virtual LANs as fallback solutions.	Technical
RS4.3	**Access Verification During Isolation** • During network isolation, verify what systems (e.g., linacs, CT, R&V systems) remain accessible, and what treatment data can still be retrieved locally. This informs decisions on whether to initiate on-site treatment continuity using offline processes.	Technical
RS4.4	**Cloud Access Workaround** • Activate available contingency access methods for cloud-hosted systems, such as mobile hotspots, local database mirrors, or hybrid cloud pathways, to support continued access to radiotherapy systems during downtime. • Coordinate with institutional IT and privacy teams when enabling emergency cloud access, ensuring actions remain aligned with applicable provincial and federal privacy and data protection requirements (e.g., PHIPA).	Technical + Organization
RS5 – Remediate the Vulnerabilities		
RS5.1	**Remediation of Vulnerabilities** • Once the root cause (attack vector or system failure) is identified, remediate the vulnerability swiftly. This may include installing missing patches, fixing misconfigurations, or replacing compromised components. If no definitive cause is identified, full system rebuilds may be required. • IT security officers and vendors must collaborate with clinical leadership to ensure restoration pathways are safe and compliant.	Technical
RS5.2	**Disinfect and Patch Devices** • Begin checking, cleaning, and patching all affected endpoints (PCs, servers, network devices). Clearly label “clean” systems and isolate them from others until the full environment is verified. This process must be documented thoroughly for internal audit and medico-legal protection.	Technical
RS6 – Implement Procedures Regarding Treatment Continuity		
RS6.0	**Collect Patient Information** • Gather critical treatment information from any available source (paper backups, patients, staff, previous communications, vendor-hosted systems). • This includes verifying demographic data, diagnosis, treatment regimen, fractionation schedule, and any paper records or printed reports. Coordination with Health Information Management (HIM) departments and compliance with PHIPA guidelines is essential.	Organization + Technical + Human-related

RS6.1 - Communication		
RS6.1.1	**Proactive Communication with Stakeholders** • Activate the communication plan from the BCP. Notify staff, vendors, leadership, partner institutions, and other stakeholders about the incident. Ensure updates are timely, consistent, and aligned with institutional messaging. Assign clear responsibilities (who communicates what, when, and to whom) to reduce confusion and misinformation. • Establish a dedicated patient communication strategy, recognizing that usual digital channels (e.g., patient portals, automated appointment systems, hospital email) may be unavailable. Implement alternate communication methods such as direct phone calls, secure mobile messaging, SMS notifications (if permitted), website banners, call centre scripts, or in-person briefings. • Provide patients with clear, practical information: appointment status, treatment continuity plans, triage decisions, safety assurances, expected timelines, and contact pathways for urgent concerns. • Ensure messaging is coordinated with privacy, legal, and leadership teams, particularly if personal health information may have been affected. • Document all major communications for governance, regulatory, and post-incident review purposes.	Organization + Human-related
RS6.1.2	**Internal information pathways** • Ensure team members are kept informed through huddles, email, or printed briefings. Share Incident Response Team meeting summaries. In Canadian institutions, this includes updating clinical and administrative leaders across disciplines (e.g., RO, RT, physics, nursing, booking and registration, oncology informatics).	Organization
RS6.1.3	**Alternative Communication Platforms** • Use secure alternatives when internal systems are down (e.g., personal phones, secure messaging apps, cloud-based tools). Ensure encryption when PHI is involved and log communications for legal review. In remote areas, consider paper-based logs or landlines. • Determine if pre-defined alternative communication methods identified during the Preparation phase (e.g., encrypted messaging apps, backup phone lines, radios) need to be activated. • Confirm functionality of backup communication channels in real time and note any deviations from expected performance for later review.	Technical + Organization
RS6.1.4	**Dedicated Telephone Lines** • Establish a centralized hotline or call station for patients and referring providers to obtain real-time updates about care disruptions, as noted in the BCP.	Technical + Organization

RS6.1.5	**Media Communication** • Engage with the hospital's communications or media team to provide radiotherapy-specific updates during an incident that may be captured in public messaging via websites, press releases, and social media. • The RO department's role is to supply accurate clinical and operational information relevant to radiotherapy services. Use previously approved communication templates if available.	Organization + Human-related
RS6.1.6	**Urgent Communication Pathways** • Ensure urgent matters (e.g., clinical escalations or triage) have direct channels, such as emergency phones, or encrypted email chains, as noted in the BCP.	Organization
RS6.2 – Treatment Continuity		
RS6.2.1	**Treatment Continuity Decision-Making** • Initiate treatment continuity planning. Decide whether to resume treatments onsite using offline workflows or transfer patients to partner institutions. The decision should account for patient priority, system availability, and inter-institutional agreements.	Organization + Human-related
RS6.2.2	**Prioritisation of Patient Management** • Use clinical triage protocols to prioritize urgent cases (e.g., head & neck, cervical, or other high-risk cancers) to minimize treatment delays that could affect outcomes. • Align prioritization with provincial or national guidance, such as oncology triage frameworks developed during the COVID-19 pandemic or other recognized standards for managing limited treatment capacity. • Ensure protocols are documented, communicated to staff, and integrated into the BCP, with flexibility to adapt to local patient volumes and resource	Organization + Human-related
RS6.3 – On-Site Treatment		
RS6.3.1	**Offline Treatment Assessment** • Conduct a safety and clinical risk assessment before initiating any offline treatment, including evaluation of the potential risk of mistreatment, available verification processes, and the ability to maintain safe treatment delivery without standard system connectivity. • If deemed safe and feasible following this assessment, initiate onsite treatment using available offline modes (e.g., vendor-enabled functionality such as file mode), supported by paper-based documentation, manual verification processes, and staff checklists. • Confirm that offline treatment is permitted within your licensing and regulatory framework, as some facilities may not be authorized to treat in offline modes. Where required, contingency approaches may need to be reviewed or approved by the Canadian Nuclear Safety Commission (CNSC).	Technical + Organization

RS6.3.2	**Manual Treatment Setup** • As directed by the BCP, use saved DICOM plans or create basic palliative setups (e.g., electrons) when treatment software is unavailable. Track each fraction and field manually.	Technical + Organization
RS6.3.3	**QA and Safety Checklists** • Deploy predefined QA checklists (e.g., double signature, time-stamped logs) to mitigate risk during offline treatment delivery.	Organization + Human-related
RS6.3.4	**Vendor Support for Offline Mode** • Coordinate with ROIS vendors to gain access to file mode or offline capabilities for treatment delivery. Include vendor contact protocols in the BCP.	Technical + Organization
RS6.4 – Redirecting of Patients		
RS6.4.1	**Transfer to Other Facilities** • If treatment cannot continue onsite, transfer patients to regional centres with capacity. Use interprovincial agreements where applicable.	Organization
RS6.4.2	**Engagement with Partner Hospitals** • Reach out to hospitals defined in pre-established MOUs (see PP2.9). If no agreement exists, rapidly formalize one. Arrange logistics and transfer protocols.	Organization
RS6.4.3	**Staff Redeployment to Support Transfers** • Redeployment of radiotherapy staff (RTTs, ROs, physicists) to support patient care at the receiving centre should be considered only where feasible and permitted by agreements, local policies, unions, and liability/insurance considerations, and when deemed safe to do so (see PP2.9 in the Preparation section). • If staff redeployment is possible, implement buddy systems, orientation, and safety briefings to minimize onboarding risks and ensure continuity of care.	Organization + Human-related
RS6.4.4	**Transfer of Treatment Data** • Ensure full clinical package accompanies each patient: diagnosis, treatment plan, current status, imaging, previous treatments and/or re-irradiation history, and any relevant reports.	Technical + Organization
RS6.5 – Non-Irradiation Processes		
RS6.5.1	**Continuity of Supporting Clinical Functions** • Determine which other clinical processes (e.g., consultations, imaging, simulation, planning) can proceed. This depends on system availability (e.g., PACS, Lab).	Organization
RS6.5.2	**Process Overview and Visualization** • Maintain an updated visual tracking system for patient status, visits, and tasks. Use whiteboards, spreadsheets, or cloud platforms (when available).	Technical + Organization
RS6.6 – Treatment Documentation		
RS6.6.1	**Paper Documentation of All Care**	Technical + Organization

	• In addition to paper charting of each treatment session (RS6.3.2) make sure to have each treatment step documented on paper; use predefined documentation templates (PP2.4) • Keep treatment record with all information as a printout, as well as any hand-written notes, (demographics, diagnosis, anamnesis, patient consent, prescription, planning, progress notes, general comments, reports printed scans, etc.)	
RS6.6.2	**Reports** • Define where to store medical information (reports hand- or machine written, images on CDs/DVDs, lab-results etc.) and how to transfer copies of it between facilities	Organization
RS6.6.3	**Printers and Copier Access** • Make sure to have printing devices and photocopiers available, which can print without a functioning network.	Technical
RS6.7 – Incident Documentation		
RS6.7.1	**Track All Incident Actions** • Maintain a transparent record of decisions, actions, and escalation steps taken by the Incident Response Team and operational staff throughout the event.	Organization
RS6.7.2	**Crisis Status Overview** • Use centralized visual tools (e.g., whiteboards, command centre dashboards) to track crisis phase and key challenges.	Organization

5.5. Recovery Domain

The Recovery domain outlines the systematic transition from emergency operations to the full restoration of clinical and digital systems. This phase is essential for ensuring continuity of patient care, preserving data integrity, and mitigating long-term impacts following a downtime event. Recovery activities are categorized across technical and organizational dimensions and emphasize collaboration among radiation oncology teams, IT departments, and external partners, such as vendors and insurers. Key actions include incremental resumption of services, quality assurance of restored systems, back-entering of offline data, effective communication, and managing clinical backlogs.

No.	**Action measure**	Cat
RC0 – Recovery in General		
RC0.1	**Recovery Function** • Implement the recovery process as defined in the BCP once containment and stabilization have been achieved. Ensure activation criteria, leadership oversight, and sequencing of recovery steps are clearly followed. • The recovery function encompasses all coordinated activities required to restore systems, validate data integrity, resume normal clinical operations, and strengthen resilience following a cybersecurity event or prolonged downtime.	Organization

	• Clearly define roles and timelines for back-entering information generated during downtime (e.g., paper documentation, manual treatment records) into electronic systems once they are restored. Establish validation steps to prevent data loss, duplication, or transcription errors. • Monitor recovery progress against predefined recovery time objectives (RTOs) and communicate status updates to clinical teams and leadership until full operational capacity is re-established. • Conduct a structured post-recovery review to identify system improvements, workflow refinements, and resilience enhancements.	
RC0.2	**Resume Incrementally Until Normal Business Activities** • Once the systems have been fully restored, regular treatment processes cannot be resumed in full immediately. An incremental restart with comprehensive safety checks must be carried out, which may take a long time.	Organization
RC0.3	**Collaboration** • The recovery coordination must involve Radiation Oncology program leadership, hospital IT departments, and ROIS vendors, as described in the BCP. In addition, local privacy officers, legal counsel, law enforcement, and cybersecurity vendors should be engaged to support forensic analysis, threat containment, and system restoration. • Where relevant, provincial health authorities may also assist with recovery support coordination and jurisdictional communications.	Organization + Human-related
RC0.4	**Access to Backups** • Access and restore system data from available backups in accordance with procedures defined in the Business Continuity Plan (BCP) and institutional recovery protocols, ensuring actions remain compliant with applicable privacy legislation, including PHIPA and PIPEDA. • Where possible, retrieve backup data through infrastructure that operates independently of the hospital's compromised core network, such as air-gapped or physically isolated systems, as outlined in the BCP to support secure system restoration.	Technical
RC0.5	**Communication of Expectation** • Clearly communicate to all stakeholders, including clinical teams, hospital leadership, patients, and provincial authorities, that full recovery and return to normal operations may take several weeks or even months. This timeline depends on the scope of the incident, IT capacity, and vendor support.	Organization + Human-related
RC1 – Activate Recovery Plan		
RC1.1	**Start Recovery Process** • As soon as the scope of the incident has been determined and the vulnerabilities or entry points have been rectified, the recovery process must be initiated.	Organization

RC2 – Recovery Method		
RC2.1	**Define Recovery Process to Be Used** • As defined in the BCP, the recovery method to be used should now be determined. This depends heavily on the extent of the incident and the backups available	Technical
RC2.2	**Setup New PCs** • If the situation requires it, setup new PCs and laptops or consider a complete reset of the existing ones and label them accordingly so that it is clear which PCs are new and secure which should not yet be used.	Technical
RC2.3	**Rebuild Entire IT Infrastructure** • Depending on the extent of the incident the whole IT infrastructure (Servers, Databases, Network etc) may need to be rebuilt	Technical
RC2.4	**Rebuilding ROIS** • Reinstallation of the ROIS system is completed, as required, in collaboration with the licensed Canadian vendor or third-party contractor supporting the system (e.g., ROIS vendors). • Systems are restored in alignment with previously validated configurations and tested using vendor-supplied verification protocols. Documentation must be compliant with PHIPA and institutional privacy guidelines.	Technical
RC2.5	**Data Restoration** • Restoring from offline, encrypted backups that were maintained as part of data backup plan	Organization
RC2.6	**Preparation for Re-entering Data** • Identify all clinical, operational, and treatment-related information generated during downtime (e.g., patient demographics, treatment parameters, progress notes, consent forms) that must be re-entered into digital systems. • Assign clear responsibility for each data stream, whether by clinical leads, medical physicists, or administrative staff, and define timelines, workflows, and verification procedures. • Ensure alignment with institutional policies, privacy regulations (e.g., PHIPA), and vendor system requirements to minimize risks of error and legal noncompliance during data back-entry.	Organization + Human-related
RC2.7	**Re-entering Data After Recovery** • When re-entering data collected during downtime (e.g., from paper charts or USB backups), institutions must follow hospital-defined validation workflows, double-check protocols, and medical QA review processes. This includes confirming dose and fractionation accuracy through oversight by both Medical Physicists and Radiation Oncologists. Additional privacy protections under PHIPA must be followed when handling temporary records.	Organization + Technical
RC2.8	**Security Check After Ransom Payment**	Technical

	• As previously noted, It is not advisable to pay a ransom after a cyberattack for several reasons, including the lack of guarantee that data will be recovered, the risk of encouraging further attacks, potential legal and regulatory consequences, financial loss and hidden costs, and concerns about data privacy; however, if the ransom has been paid, and the system is released by the hackers, they cannot yet be trusted even if they appear to be working. Comprehensive security checks must be carried out to remove any remaining malware.	
RC3 – Check Recovery Data		
RC3.1	**Quality assurance, data restoration and data consistency** • Data re-entry should follow organizational data integrity protocols, such as those defined by the hospital's Privacy Office or QA team. • Radiotherapy-specific QA review tools (e.g., comparison with original treatment plans, record-and-verify audits) should be used to minimize the risk of data loss or treatment error. Documentation should be stored securely per PHIPA guidelines.	Organization
RC3.2	**Checking processes** • Check whether the regular processes work, e.g. using a dummy run or end-to-end test.	Organization + Technical
RC3.3	**Treatment continuity** • Decide how to proceed with patients who are currently being treated under the emergency procedure. These patients can be transferred to the regular procedures or treatment can be continued in the emergency procedure. This applies in particular to patients who have been referred to other locations**.**	Organization + Technical
RC4 – Communication (Internal)		
RC4.1	**Regular Communication** • Inform employees regularly about the status of the recovery work, especially to provide a perspective on when regular processes can be resumed. • Inform other stakeholders (patients, providers, senior leaders, vendors) once certain steps have been taken. • Keep up regular (daily) crisis meetings during the recovery phase. • Communication through public channels should be coordinated through hospital Public Affairs/Communications departments. • Dedicated media lines or emergency updates could be published through hospital websites and trusted provincial portals, as required.	Organization
RC4.2	**Patient Contact** • Contact patients regularly to keep them updated with the recovery process.	Organization
RC5 – Define end of the Recovery and Resume Normal Business Activities		
RC5.1	**Statement** • As soon as the recovery processes have been completed, the data checked and the regular processes are working again, the incident	Organization + Human-related

	can be considered closed. Declare systems restoration and data recovery as complete and communicate it to all stakeholders.	
RC5.2	**Return to Normal** • Transition from emergency workflows to regular treatment processes using a phased, stepwise ramp-up approach, rather than a single fixed return date. • Gradually restore services based on system stability, validated data integrity, staffing capacity, and clinical prioritization. Clearly define criteria for moving between phases (e.g., partial system restoration, expanded scheduling, full-service capacity). • Communicate each phase transition and expected service levels to staff, patients, vendors, and leadership to ensure alignment and manage expectations. • Formally declare "full-service restoration" only once all critical systems are validated, backlogged treatments are addressed or actively managed, and emergency processes are no longer required. • Document the transition process and retain contingency readiness in case issues re-emerge during ramp-up.	Organization
RC5.3	**Gap Compensation** • If treatment interruptions have occurred, assess the potential clinical impact based on tumour type, total dose delivered, overall treatment time, and patient-specific factors. • Where clinically indicated, consider compensation strategies grounded in established radiobiological principles and professional guidance (e.g., schedule adjustments, additional fractions, or accelerated treatment), as determined by the treating radiation oncologist in collaboration with medical physics. • Decisions regarding compensation should be individualized and documented clearly in the patient record, including rationale and patient communication. • As no single national Canadian standard mandates specific compensation formulas, departments should maintain local clinical guidance to support consistent and evidence-informed decision-making.	Organization + Technical

5.6. Debriefing and Continuous Improvement Domain

The final domain of the framework focuses on post-incident evaluation and system strengthening through structured learning, accountability, and knowledge dissemination. This domain is critical for transforming crisis experiences into actionable insights that reduce future risk and enhance institutional resilience. The measures included in this category cover comprehensive debriefing processes, formal reviews of system performance, adaptation of response protocols, and strategic investment planning. Additionally, the domain emphasizes the importance of peer-to-peer learning across jurisdictions and national coordination led by CAPCA, CPQR, and provincial stakeholders. Continuous improvement actions also include evaluating vendor support, refining

offline workflows, strengthening communication practices, and ensuring long-term follow-up on patients affected by treatment disruptions. These actions collectively ensure that radiotherapy departments do not simply return to baseline after a downtime event but evolve to become more resilient and responsive.

No.	**Action measure**	Cat
DC0 – Debriefing and Continuous Improvement in General		
DC0.1	**Recommendation** • Use knowledge and "lessons learned" from previous events to develop recommendations to strengthen unplanned and extended downtime in radiotherapy	Organization
DC0.2	**Post-Incident Debrief and Lessons Learned** • Conduct a structured debrief following recovery, involving members of the Incident Response Team (IRT) and key personnel who were directly engaged in the command centre and operational response. • The purpose of the debrief is to review what occurred, assess what worked well, identify gaps or inefficiencies, and evaluate communication, governance, technical response, and clinical continuity measures. • Document lessons learned and translate them into concrete updates to the BCP, downtime manuals, communication templates, triage protocols, and technical safeguards. • Where appropriate, share high-level insights with institutional leadership, regional partners, or professional networks to support broader system learning, while respecting confidentiality and security considerations.	Organization + Human-Related
DC0.3	**Continuous Preparation** • Establish a procedure for regular testing and updates across all stages of unplanned/extended downtime, ensuring that detection, reaction, response, and recovery plans remain robust and aligned with evolving threats and continuous improvements are implemented.	Organization
DC0.4	**Staff Support** • Acknowledge and formally recognize staff contributions during the incident. Express appreciation for flexibility, professionalism, and teamwork shown under challenging circumstances. • Conduct supportive discussions to reflect on what worked well and highlight examples of effective collaboration, leadership, and problem-solving. Positive reinforcement strengthens resilience and organizational culture. • Recognize that team spirit may have been strained depending on the nature of the event and how it was managed. Provide opportunities for open dialogue, psychological safety, and constructive feedback.	Human-Related, Organizational

	• Monitor for signs of burnout or moral distress and ensure access to institutional wellness resources, peer support programs, or employee assistance services. • Use the post-incident period as an opportunity to strengthen team cohesion through continued engagement, learning, and shared improvement efforts.	
DC1 – Review Past Events		
DC1.1	**Overall Review** • Create a comprehensive list of all challenges and problems that occurred during the unplanned/extended downtime.	Technical
DC1.2	**Risk management and vulnerability** • Identify the weaknesses of the hospital and its cybersecurity concept. Analyse if the cybersecurity risk management worked.	Organization + Technical
DC1.3	**Communication** • Recap how the communication has worked with patients, staff, providers and vendors. Check how transparent the communication was and how well informed the stakeholders felt.	Human-Related
DC1.4	**Vendors** • Conduct a post-incident review of vendor involvement during the response and recovery phases, including the availability and effectiveness of vendor support, where applicable.	Organization + Technical
DC1.5	**Prevention Phase** • In collaboration with institutional IT, cybersecurity, and organizational leadership, identify measures that could have prevented or mitigated the incident, including actions within the radiotherapy program and broader enterprise-level controls.	Technical
DC1.6	**Respond Phase** • Analyse what actions need to be taken urgently versus a phased response.	Organization
DC1.7	**Available Offline Data** • Evaluate the availability, usability, completeness and quality of offline data as well as how well the prepared templates for paper-based processes worked.	Organization + Technical
DC1.8	**Patient Priority** • Analyse how triaging and prioritisation of patients worked, and if/how there was an impact to patient care.	Organization + Human-Related
DC1.9	**Offline Treatment** • Analyse how the RT delivery without OIS and R&V worked, how the QA worked and how safe the treatment could be applied.	Technical
DC1.10	**Referring Patients** • Analyse how the referring of patients to other hospitals worked, i.e., Patient logistics, data transfer and treatment continuity.	Organization + Technical
DC1.11	**Backups and Recovery** • Review the status and usefulness of offline backups and offline/ redundancy servers and network if available.	Technical

DC1.12	**Recovery Phase** • Analyse how the recovery worked, how the restored data and paper-based date has been merged and how return to normalcy went.	Organization + Technical
DC1.13	**Treatment Outcome** • Monitor patients who have received unusual treatment as a result of the incident (e.g. prolonged interruptions, missing sessions). • Document potential treatment outcome impact.	Organization
DC2 – Adaptation of the Incident Respond Plan		
DC2.1	**Disaster Protocol** • The results of the analysis and review of the past events and the associated procedures must be incorporated into an adaptation of the incident respond plans for detection, respond and recovery.	Organization + Technical
DC2.2	**Future Investment** • Derive from the analyses of the past events where financial, technical and personnel investments need to be made to be better prepared for future events.	Organization + Human-Related
DC3 – Disseminate Organizational Learnings from Each Phase of Incident Handling		
DC3.1	**Sharing Experience** • Encourage the sharing of incident experiences and practical solutions not only within departments and hospitals but also through pan-Canadian platforms such as CPQR, and provincial radiotherapy committees or forums. Peer-to-peer knowledge transfer can support readiness across jurisdictions.	Organization
DC3.2	**Incident Reporting** • Following any significant downtime or cyber event, ensure that all affected centres complete formal incident reports using existing provincial or national reporting systems (e.g., NSIR-RT Incident Reporting, provincial digital health incident portals). These reports should feed into structured learning reviews that drive quality improvement.	Organization + Technical
DC3.3	**Relation to IT Department** • Foster stronger integration between radiotherapy departments and IT services through regular meetings and the creation joint governance committees, including the definition of shared goals (primary focus on patient care), transparent and defined communication channels, cybersecurity reviews and shared risk assessments. • In larger regions with integrated systems, this relationship is critical for ensuring radiotherapy-specific needs are prioritized.	Organization

6. Overarching System Enablers

In addition to the six operational phases of emergency preparedness and response, the *Pan-Canadian Emergency Preparedness Framework for Radiotherapy Downtime* incorporates a set of overarching enablers that support long-term sustainability, organizational alignment, and culture change. These system-level elements include the active involvement of top management in risk

ownership and resource allocation, the establishment of strong partnerships with industry and system vendors, visible and accountable leadership during crises, and the integration of recognized standards and educational initiatives into professional development. By embedding these cross-cutting enablers, radiotherapy programs can ensure that preparedness is not isolated to technical operations but is recognized as a shared, strategic responsibility across institutional levels and intersectoral networks.

No.	**Action measure**	Cat
OT1 – Involvement of Top Management		
OT1.1	**Shared Responsibility and Knowledge Transfer** • Recognize that downtime preparedness involves multiple areas of hospital leadership, including radiotherapy, IT, cybersecurity, clinical leadership, and risk management. • Support cross-departmental coordination and planning, ensuring that relevant operational, clinical, and technical perspectives are incorporated into preparedness and response efforts. • Maintain mechanisms for ongoing knowledge sharing and communication among radiotherapy teams, CIO/IT leadership, and organizational risk management functions to support situational awareness and coordinated decision-making.	Organization + Human-related
OT1.2	**Costs** • Allocate funding for downtime preparedness and cybersecurity initiatives, including staffing, infrastructure, training, and vendor engagement. • Funding cases should be linked to business continuity, clinical risk mitigation, and quality/safety priorities already tracked in Canadian hospitals.	Organization
OT2 – Involvement of Industry and Providers		
OT2.1	**Partnership with Industry** • Leverage existing partnerships with vendors, cloud providers, and medical device manufacturers to support system resilience, coordinated incident response, and recovery activities. • Where appropriate, incorporate testing exercises (e.g., tabletop simulations) within vendors service agreements and collaborative initiatives that support sector-wide readiness and shared learning.	Organization + Human-related
OT3 – Leadership in Crisis		
OT3.1	**Visible Leadership Presence & Accountability** • Radiotherapy emergency preparedness should be supported by visible and accountable leadership during system disruptions, reinforcing organizational commitment to patient safety and continuity of care. Institutions should establish expectations that clinical and operational leaders maintain an active and visible presence during prolonged outages to support coordinated communication, triage decisions, and cross-team collaboration. Embedding this leadership visibility within organizational emergency governance helps ensure that frontline teams are	Organization + Human-related

	supported and that response efforts remain aligned across clinical, operational, and technical groups.	
OT3.2	**Staff and Patient Wellness** • Embed staff wellness checks into emergency workflows, especially during extended service disruptions. This includes rotating duties, debriefs, and providing wellness resources. Human resources and occupational health teams should be included in the Incident Management System (IMS). • Clinician-led discussions and psychosocial support that go beyond logistics to address patient stress related to system or care interruption. These steps help reduce anxiety during disruptions and support recovery of confidence as services are restored.	Human-related
OT4 – Standards and Education		
OT4.1	**IT Standards** • Radiotherapy programs should work in collaboration with institutional IT and cybersecurity subject matter experts to ensure that relevant cybersecurity frameworks are incorporated into organizational digital health standards and operational practices. • Radiotherapy teams should also participate in relevant training and preparedness activities to ensure awareness of cybersecurity risks and response procedures.	Organization + Human-related
OT4.2	**Risk Modelling** • Health systems and institutional IT and cybersecurity teams should incorporate radiotherapy-specific workflows and dependencies into broader threat modelling and risk assessment. • Collaboration with clinical leaders and system vendors can help ensure that potential vulnerabilities, downtime risks, and operational impacts on radiotherapy services are appropriately identified and reflected in organizational risk management processes.	Organization + Technical
OT4.3	**Education** • Canadian training programs should include downtime response, paper charting, verbal orders, and emergency treatment decision-making in clinical curricula for RTTs, MPEs, and residents.	Organization + Human-related

7. Conclusion

The Pan-Canadian Emergency Preparedness Framework Radiotherapy Downtime represents a milestone in strengthening resilience across Canada's radiotherapy landscape. Developed through international benchmarking, pan-Canadian surveys, and collaborative input from clinical, technical, and policy experts, it provides a structured, lifecycle-based model that integrates cybersecurity and emergency preparedness into one cohesive strategy.

This framework is intentionally designed to be both standardized and adaptable, aligning with international standards while reflecting Canadian realities, legislation, and health system

structures. Organized into six operational domains- Preparation, Prevention, Detection, Response, Recovery, and Continuous Improvement- and supported by overarching enablers on leadership, industry partnership, and education, the framework ensures a comprehensive approach that spans governance, technology, and workforce readiness.

Through its multidisciplinary action measures, the framework provides radiotherapy centres with clear guidance to enhance downtime preparedness, safeguard patient safety, and maintain operational continuity during both cyber and non-cyber disruptions. Its design emphasizes collaboration across IT, clinical, and administrative teams, ensuring that preparedness is recognized not as an isolated technical effort but as a shared institutional responsibility.

8. Next Steps

The next phase focuses on translating this framework into practical implementation tools and testing initiatives. Key actions include:

- Conducting knowledge mobilization activities to raise awareness of the work and support spread and scale.
- Supporting the adoption of pan-Canadian templates, checklists, and simulation protocols to operationalize the framework's domains.
- Exploring opportunities to integrate the framework into existing CPQR quality programs, accreditation pathways, and training curricula.
- Establishing a continuous feedback mechanism to evaluate framework adoption, gather lessons learned, and ensure iterative updates based on evolving threats and technologies.

In the long term, this framework lays the foundation for a nationally coordinated approach to radiotherapy resilience during unplanned and extended downtime.

9. References

[1] CityNews Toronto. *Flooding damages London, Ontario hospital equipment* [Internet]. 2021 Jul 24. Available from: https://toronto.citynews.ca/2021/07/24/flood-london-ontario-hospital-damage/

[2] CBC News. B.C.'s Abbotsford hospital suffers flood damage during atmospheric river [Internet]. 2021 Nov 17. Available from: https://www.cbc.ca/news/canada/british-columbia/abbotsford-hospital-flood-atmospheric-river-1.6250936

[3] Health Service Executive (HSE). Conti cyber-attack on the HSE: Full report [Internet]. Ireland;2021. Available from: https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf

[4] CBC News. Windsor hospital systems down in suspected cyberattack [Internet]. 2023 Nov 24. Available from: https://www.cbc.ca/news/canada/windsor-cyberattack-hospital-incident-1.7032916

[5] CTV News Northern Ontario. Sudbury hospital affected by ransomware attack; patient services impacted [Internet]. 2024 Feb 20. Available from: https://northernontario.ctvnews.ca/sudbury-hospital-hit-by-ransomware-attack-patient-services-affected-1.6782102

[6] Global News. Cyberattack on Newfoundland and Labrador healthcare system [Internet]. 2021 Nov 1. Available from: https://globalnews.ca/news/8341284/newfoundland-labrador-healthcare-cyberattack/

[7] Canadian Centre. For Cyber Security. Canadian Centre for Cyber Security. *Using security information and event management tools to manage cyber security risks (ITSM.80.024)* [Internet]. Government of Canada. Available from: https://www.cyber.gc.ca/en/guidance/using-security-information-event-management-tools-manage-cyber-security-risks-itsm80024

[8] European Society for Radiotherapy and Oncology (ESTRO). *ESTRO framework for radiation oncology departments to mitigate against cyberattacks* [Internet]. Available from: https://www.thegreenjournal.com/article/S0167-8140(25)05309-5/fulltext

[9] Peters S, O'Donovan A, Bellini M, et al. *ESTRO framework for radiation oncology departments to mitigate against cyberattacks*. Radiotherapy and Oncology. 2026;214:111305. doi:10.1016/j.radonc.2025.111305

[10] Institute of Global Health Innovation. *Essentials of Cybersecurity for Healthcare Organizations (ECHO)* [Internet]. Imperial College London. Available from: https://www.imperial.ac.uk/ig-hi/projects/cybersecurity/

[11] National Institute of Standards and Technology (NIST). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1* [Internet]. Gaithersburg, MD; 2018. Available from: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[12] World Health Organization (2018). WHO guidance for business continuity planning. World Health Organization. https://iris.who.int/handle/10665/324850. License: CC BY-NC-SA 3.0 IGO

[13] NHS England. *NHS England business continuity management toolkit*. Date published: 20 April 2023; last updated: 18 May 2023. NHS England. *Business continuity management toolkit* [Internet]. 2023. Available from: https://www.england.nhs.uk/publication/business-continuity-management-toolkit/

[14] International Organization for Standardization (ISO). *ISO 22301:2019 Security and resilience – Business continuity management systems – Requirements*. Geneva: ISO; 2019. Available from: https://www.bsigroup.com/en-CA/products-and-services/standards/iso-22301-business-continuity-management/

[15] CSA Group. *CSA Z1600-17 (R2022): Emergency and continuity management program*. Toronto: CSA Group; 2017. Available from: https://www.csagroup.org/store/product/Z1600-17/

[16] Waterloo Regional Health Network. *Network Downtime Process Policy*. Ontario, Canada; 2025 Jun.

[17] CHU de Québec–Université Laval. *Guide de pratique clinique en cas d'interruption de traitement*. Quebec, Canada; 2024 Jun 18.

[18] Ontario Health (Cancer Care Ontario). *Radiation Treatment Centres Emergency Preparedness MoU Checklist (v1.2)*. Toronto, Canada; 2023 Mar.

[19] Hamilton Health Sciences. *Draft Secondment Agreement for Health Workforce Deployment*. Ontario, Canada; 2021.

[20] HNHB Regional Cancer Program. *Pandemic Plan for Consolidation of Radiation Therapy Activity*. Ontario, Canada; 2020 May.

[21] HNHB Regional Cancer Program. *Process to Re-Direct Patient Care in Emergency Situations*. Ontario, Canada; 2021 Feb.

[22] HNHB Regional Cancer Program. *Functional Exercise: Systemic Therapy Staffing Shortage Simulation*. Ontario, Canada; 2021.

[23] HNHB Regional Cancer Program. *Pandemic Planning Exercise for Radiation Therapy*. Ontario, Canada; 2020 Dec.

[24] HNHB Regional Cancer Program. *Incident Management System Manual*. Ontario, Canada; 2022 Feb.

[25] Juravinski Cancer Centre. JCC IMS and IAP Process Overview. Ontario, Canada;2021

[26] HNHB Regional Cancer Program. RCP IMS Functional Exercise Review – ONA Briefing. Ontario, Canada; 2021 May 13.

[27] Hadnagy C, Fincher M. Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails. Wiley; 2015. 224 p.

[28] Scarfone KA, Mell PM. Guide to Intrusion Detection and Prevention Systems (IDPS) [Internet]. 0 ed. Gaithersburg, MD: National Institute of Standards and Technology; 2007 [cited 2025 July 1] p. NIST SP 800-94. Report No.: NIST SP 800-94. Available from: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf

[29] MITRE Corporation. MITRE ATT&CK®: A knowledge base of adversary tactics and techniques based on real-world observations [Internet]. MITRE; 2024. Available from: https://attack.mitre.org