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

Cadre pancanadien de préparation aux situations d'urgence en cas d'interruption des activités des centres de radiothérapie

---

Élaboré par le Partenariat canadien pour la qualité en radiothérapie (PCQR),

un comité permanent de l'Association canadienne des agences provinciales du cancer (ACAPC).

(v 1.0 31 mars 2026)

ACAPC
Association canadienne des agences provinciales du cancer

Préface

Le ***cadre pancanadien de préparation aux situations d'urgence en cas d'interruption des activités des centres de radiothérapie*** a été élaboré afin de faciliter l'évaluation et l'amélioration de l'état de préparation aux situations d'urgence et de la cybersécurité dans les centres de radiothérapie au Canada. Les services de radiothérapie reposant largement sur des systèmes numériques interconnectés, ils sont particulièrement vulnérables aux cyberattaques, aux défaillances du système et aux perturbations des infrastructures, qui peuvent compromettre la continuité des soins et les résultats des traitements. En établissant des lignes directrices pancanadiennes, des outils pratiques et des mécanismes de coordination, ce cadre vise à combler les lacunes critiques en matière de résilience de la radiothérapie, afin de garantir que les centres de radiothérapie partout au Canada puissent continuer à prodiguer des traitements vitaux, même en cas de crise impliquant des défaillances structurelles.

Ce projet est mené par le Partenariat canadien pour la qualité en radiothérapie (PCQR), un comité permanent de l'Association canadienne des agences provinciales du cancer (ACAPC). L'élaboration de ce cadre a été rendue possible grâce à la collaboration et au soutien financier de la Société du partenariat canadien contre le cancer et de Santé Canada.

L'ACAPC est le seul organisme représentant les agences provinciales du cancer et les programmes canadiens visant à diminuer le fardeau du cancer. L'ACAPC offre un forum aux dirigeants des systèmes visant à diminuer le fardeau du cancer du Canada pour discuter, apprendre et collaborer sur les questions affectant la prestation des soins aux patients atteints de cancer au Canada. En se concentrant sur les questions opérationnelles essentielles, l'ACAPC travaille efficacement et réagit rapidement aux problèmes urgents et émergents visant à diminuer le fardeau du cancer.

Le PCQR favorise une culture de la qualité et de la sécurité de l'administration de la radiothérapie par l'établissement de normes nationales, des initiatives d'amélioration de la qualité et l'apprentissage systémique fondé sur les données. Il veille au respect des normes du programme de radiothérapie d'Agrément Canada et supervise les efforts d'amélioration de la qualité du Système national de déclaration des accidents et incidents — radiothérapie (SNDAI-RT). Le PCQR travaille en étroite collaboration avec des associations professionnelles, notamment l'Association canadienne des technologues en radiation médicale (ACTRM), l'Association canadienne des infirmières en oncologie (ACIO), l'Organisation canadienne des physiciens médicaux (OCPM), l'Association canadienne de radio-oncologie (ACRO) et d'autres partenaires, afin de renforcer les services de radiothérapie grâce à la collaboration, à l'innovation et à l'amélioration continue.

Ce cadre résume les pratiques exemplaires en matière de préparation aux situations d'urgence et de cybersécurité dans le contexte de la radiothérapie. Il présente des mesures d'action détaillées regroupées par domaine du cycle de vie, et le manuel de ressources correspondant fournit des outils et des modèles destinés à faciliter une mise en œuvre pratique adaptée aux besoins locaux. En adoptant ce cadre, les centres de radiothérapie peuvent renforcer leur état de préparation aux situations d'urgence et leur posture en matière de cybersécurité, protéger les données sensibles des patients et garantir la continuité des traitements de radiothérapie vitaux en cas d'événements perturbateurs.

Remerciements

Un *groupe consultatif sur la préparation aux situations d'urgence en radiothérapie* a été établi, composé de responsables cliniques en radiothérapie, de professionnels des technologies de l'information en milieu hospitalier, de responsables de la qualité et de la gestion des risques, ainsi que de responsables de la cybersécurité, tous nommés par leurs programmes provinciaux respectifs visant à diminuer le fardeau du cancer. Cette approche a permis d'assurer une large représentation géographique et professionnelle partout au Canada. Le groupe consultatif a contribué à l'élaboration du cadre en menant des activités de consultation structurées, notamment une enquête nationale visant à évaluer l'état de préparation aux situations d'urgence, des discussions visant à cerner les vulnérabilités institutionnelles à partir de scénarios, la précision des domaines prioritaires à inclure dans le cadre, et des délibérations sur les outils et ressources potentiels de coordination pancanadienne.

Parallèlement, le *comité directeur du Partenariat canadien pour la qualité en radiothérapie (PCQR)* a assuré un contrôle stratégique en validant les conclusions émergentes, en identifiant les domaines nécessitant une normalisation pancanadienne et en veillant à la cohérence avec les priorités stratégiques plus générales. Leurs contributions ont mis l'accent sur une planification axée sur le patient, des solutions de secours à faible technologie et la conformité aux exigences réglementaires. Ce cadre a été renforcé davantage grâce à l'examen et aux commentaires d'experts nationaux et internationaux dans ce domaine, ainsi que de parties prenantes issues de diverses disciplines, ce qui a permis de garantir qu'il soit pratique, pertinent et en phase avec les réalités des environnements cliniques et opérationnels.

Nous tenons à remercier sincèrement les personnes suivantes pour le temps qu'elles nous ont consacré, leur expertise et leurs contributions :

Membres du groupe consultatif

Lisa Barbera — Alberta Health Services

Jason Berry — Action Cancer Manitoba

Jean-Pierre Bissonnette — Réseau universitaire de santé, Ontario

Dan Bond — Services de santé de Terre-Neuve-et-Labrador

Nick Chng — BC Cancer, Colombie-Britannique

Gavin Cranmer-Sargison - Saskatchewan Cancer Agency

Carol-Anne Davis — Régie de la santé de la Nouvelle-Écosse

Jon Dysart — Réseau de santé Horizon, Nouveau-Brunswick

Scott Gallant — Réseau de santé Vitalité, Nouveau-Brunswick

George Hajdok — Alberta Health Services

Gina Henneberg — Saskatchewan Cancer Agency

Joe Ho — Autorité provinciale des services de santé, Colombie-Britannique

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

Brian Liszewski — Santé Ontario (Action Cancer Ontario)

Eshwar Kumar — Réseau du cancer du Nouveau-Brunswick

Kristi MacKenzie — Association canadienne des agences provinciales du cancer

Krista MacLeod — Réseau de santé Horizon, Nouveau-Brunswick

Donia MacDonald — Services de santé de Terre-Neuve-et-Labrador

Jason Berry — Action Cancer Manitoba

Kathryn Moran — Régie de la santé de la Nouvelle-Écosse

Andrew Moull — Hamilton Health Sciences, Ontario

Natalie Pomerleau Dalcourt — Réseau de santé Vitalité, Nouveau-Brunswick

Gregory Salomons — Centre des sciences de la santé de Kingston, Ontario

Devin Schellenberg — BC Cancer, Colombie-Britannique

Brad Warkentin — Alberta Health Services

Yalda Zarif Zargarian Talasaz — étudiante stagiaire au programme Michener, analyse des données de santé numériques

Réviseurs

Marie Ambrosio — Waterloo Regional Health Network, Ontario

Jean-Pierre Bissonnette — Réseau universitaire de santé, Ontario

Stephen Breen — Centre des sciences de la santé Sunnybrook, Ontario

Renata Chmielewski - Santé Ontario (Action Cancer Ontario)

Tim Craig — Santé Niagara, Ontario

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

Eric Gutierrez — Santé Ontario (Action Cancer Ontario)

Nareesa Ishmail - Santé Ontario (Action Cancer 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 — Services de santé de Terre-Neuve-et-Labrador

Kathryn Moran — Régie de la santé de la Nouvelle-Écosse

Samuel Peters — Société européenne de radiothérapie et d'oncologie (ESTRO), Suisse

Nadia Petseva — Commission canadienne de sûreté nucléaire, gouvernement du Canada

Petra Reijnders — Maastricht Radiation Oncology Clinic (Maastro), Pays-Bas

Leah Shuparski-Miller - Commission canadienne de sûreté nucléaire, gouvernement du Canada

Jen Smith — Waterloo Regional Health Network, Ontario

Laurie Stillwaugh — Centre de cancérologie du Nord-Est Shirley et Jim Fielding, Ontario

Tynan Stevens — Régie de la santé de la Nouvelle-Écosse

Chris Thomas — Régie de la santé de la Nouvelle-Écosse

Christine Tompkins — Régie de la santé de la Nouvelle-Écosse

Steven Waytowich — Horizon Santé-Nord, Ontario

Shawn Wilson — Régie de la santé de la Nouvelle-Écosse

Leah Wolfe — Waterloo Regional Health Network, Ontario

Lixin Zhan - Waterloo Regional Health Network, Ontario

Mike Oliver- Horizon Santé-Nord, Ontario

Table des matières

1. Glossaire des abréviations (référence) 8
2. Introduction 11
2.1 Les centres de radiothérapie sont confrontés à des risques opérationnels croissants 11
2.2 Élaboration du cadre pancanadien 12
2.3 Public visé 13
2.4 Objectifs 13
2.5 Flexible et évolutif dans divers environnements cliniques 14
2.6 Promouvoir la collaboration 14
3. Méthodologie 15
3.1. Analyse du contexte 15
3.1.1. Revue de la littérature 15
3.1.2. Enquête pancanadienne sur la préparation aux situations d'urgence et la cybersécurité 17
3.1.3. Plans et ressources de préparation aux situations d'urgence 18
3.1.4. Intégration des outils de cybersécurité 22
4. Conception et élaboration du cadre 23
4.1 Structure du cadre 23
4.2 Cadre de cybersécurité de l'ESTRO 24
4.3 Résultats de l'enquête pancanadienne 25
4.4 Classification des mesures d'action 26
4.5 Répartition des mesures par domaine 27
5. Le cadre 28
5.1. Domaine de la préparation 28
5.2. Domaine de la prévention 41
5.3. Domaine de la détection 56
5.4. Domaine d'intervention 61
5.5. Domaine du rétablissement 73

5.6. Domaine de compte rendu et de l'amélioration continue 79
6. Facteurs habilitants généraux du système.....83
7. Conclusion 85
8. Prochaines étapes.....86
9. Références.....87

1. Glossaire des abréviations (référence)

Abréviation	Terme complet
ACADR	Alliance canadienne pour l'intelligence artificielle et données en radiothérapie
AFM	Authentification à facteurs multiples
ANS	Accord sur les niveaux de service
AQ	Assurance de la qualité
CCSN	Commission canadienne de sûreté nucléaire
CD	Disque compact
CIS	Center for Internet Security
CSA	Association canadienne de normalisation
CSF	Cadre de cybersécurité
DC	Amélioration continue après les interruptions (mesures après incident)
DICOM-RT	Digital Imaging and Communications in Medicine – Radiation Therapy
DME	Dossier médical électronique
DPI	Dirigeant principal de l'information
DPSI	Dirigeant principal de la sécurité de l'information
DSE	Dossier de santé électronique
DVD	Disque numérique polyvalent
ECHO	Principes fondamentaux de la cybersécurité dans les établissements de santé
EDR	Détection et intervention sur les terminaux
EII	Équipe d'intervention en cas d'incident
EPM	Expert en physique médicale
ESTRO	Société européenne de radiothérapie et d'oncologie
HDD	Haut débit de dose
HIMSS	Healthcare Information and Management Systems Society
HITRUST	Health Information Trust Alliance
GIES	Gestion des informations et des événements de sécurité
IA	Intelligence artificielle

Abréviation	Terme complet
IDS	Système de détection d’intrusion
ISO	Organisation internationale de normalisation
LA	Lettre d’accord
LINAC	Accélérateur linéaire
LPRPDE	Loi sur la protection des renseignements personnels et les documents électroniques
LPRPS	Loi sur la protection des renseignements personnels sur la santé
LPVPC	*Loi sur la protection de la vie privée des consommateurs*
LRMP	Loi sur les renseignements médicaux personnels
NHS	National Health Service
OMS	Organisation mondiale de la Santé
ORMS	Système de gestion de la résilience organisationnelle
OT	Facteur habilitant global (soutien à l’échelle du système)
PACS	Système d’archivage et de transmission d’images
PAI	Plan d’action en cas d’incident
PCA	Plan de continuité des activités
PCQR	Partenariat canadien pour la qualité en radiothérapie
PE	Protocole d’entente
PFVA	Planifier — faire — vérifier — agir
R&V	Système de contrôle et d’enregistrement
RBAC	Contrôle d’accès basé sur les rôles
RO	Radio-oncologie
ROIS	Système d’information en radio-oncologie
RPV	Réseau privé virtuel
RT	Radiothérapie
SGI	Système de gestion des incidents
SIL	Système d’information de laboratoire
SIO	Système d’information en oncologie
SNDAI-RT	Système national de déclaration des accidents et incidents — radiothérapie
SOC	Centre des opérations de sécurité

Abréviation	Terme complet
TDM	Tomodensitométrie
TPS	Système de planification de traitement
USB	Bus série universel
VLAN	Réseau local virtuel

2. Introduction

2.1 Les centres de radiothérapie sont confrontés à des risques opérationnels croissants

Les centres de radiothérapie exercent leurs activités dans des environnements techniques et physiques complexes et peuvent être confrontés à divers risques qui peuvent entraîner des interruptions imprévues ou prolongées, nuisant ainsi aux services de traitement essentiels.

Aux fins du présent cadre, on entend par *interruption imprévue* toute interruption inattendue des services de radiothérapie causée par des défaillances techniques, des perturbations des infrastructures, des risques environnementaux, des cyberincidents ou des contraintes de personnel, qui empêchent la prestation normale de radiothérapie ou le bon déroulement des activités cliniques connexes.

Une *interruption prolongée* est définie comme une perturbation de longue durée des services de radiothérapie — qui dure généralement au-delà du délai pouvant être géré par des solutions de contournement opérationnelles courantes — et qui a une incidence importante sur la capacité à dispenser les traitements prévus, à maintenir les flux de travail cliniques ou à accéder aux systèmes essentiels, et qui peut nécessiter des modifications des services, un triage des patients ou une coordination avec des partenaires externes.

Par exemple, en août 2023, la rupture d'une conduite au site du Programme régional de cancérologie de London, en Ontario, a entraîné l'annulation de tous les rendez-vous en consultation, ce qui a considérablement perturbé la prise en charge des patients[1]. De même, en novembre 2021, de graves inondations à Abbotsford, en Colombie-Britannique, ont entraîné l'annulation ou le report d'environ 70 rendez-vous de patients sur une période de 3 jours, tout en perturbant l'accès à la dialyse et à d'autres services de santé essentiels[2].

Outre les risques environnementaux et techniques, la montée des cybermenaces constitue une préoccupation sérieuse et croissante pour les établissements de santé. Des incidents internationaux très médiatisés, tels que l'attaque par rançongiciel de 2021 contre le Health Service Executive en Irlande et la fuite de données de 2018 impliquant le système SingHealth à Singapour, ont mis en évidence le risque de perturbations généralisées des services[3]. [4] Des incidents similaires se sont produits au Canada, notamment l'interruption prolongée des services survenue en 2023 à l'hôpital régional de Windsor, en Ontario, les cyberattaques de 2021 contre Eastern Health à Terre-Neuve-et-Labrador, ainsi que l'incident informatique de 2019 à Horizon Santé-Nord, à Sudbury, en Ontario[5] [6].

Les perturbations de la main-d'œuvre constituent également un risque opérationnel important pour les services de radiothérapie. La pandémie de COVID-19 a montré à quel point les effectifs peuvent être perturbés par la maladie, les obligations de quarantaine, l'épuisement professionnel et les redéploiements, ce qui peut limiter la capacité des centres à maintenir leurs activités normales. Dans de telles circonstances, les centres peuvent être contraints de trier les patients, de modifier les calendriers de traitement ou de transférer les soins vers des établissements partenaires disposant de la capacité nécessaire. Ces défis soulignent l'importance d'adopter des approches coordonnées en matière de planification de la main-d'œuvre et de soutien mutuel entre les centres de radiothérapie, notamment par des mécanismes de partage d'expertise, d'assistance à distance ou de redistribution temporaire de la charge de travail en cas de perturbation.

Ces événements soulignent la nécessité d'une approche coordonnée et résiliente en matière de préparation aux situations d'urgence et de cybersécurité au sein de la communauté de la radiothérapie. Au Canada, où la prestation des soins de santé relève de la compétence des provinces et concerne une population géographiquement dispersée, les centres de radiothérapie sont souvent situés à des distances considérables les uns des autres. Cette dispersion géographique et cette structure juridictionnelle peuvent limiter la disponibilité d'un soutien externe immédiat en cas de perturbations, ce qui renforce la nécessité d'un cadre national visant à promouvoir la cohérence, des normes communes et un soutien entre les centres.

2.2 Élaboration du cadre pancanadien

Le *Cadre pancanadien de préparation aux situations d'urgence en cas d'interruption des activités des centres de radiothérapie* a été élaboré en 2025 par le PCQR et a été identifié comme une priorité dans le plan de travail stratégique pluriannuel 2025-2027 du PCQR.

Ce cadre fournit des orientations claires et concrètes pour la gestion des interruptions prolongées et imprévues dans les centres de radiothérapie partout au Canada. Il s'appuie sur les enseignements tirés d'incidents survenus au Canada et à l'étranger et intègre les leçons issues des pratiques exemplaires et des normes internationales. Il permet aux centres de radiothérapie de se préparer, de prévenir, de détecter, d'intervenir, de rétablir leurs activités et de tirer des enseignements d'un large éventail d'incidents.

En fin de compte, ce cadre vise à :

- assurer la continuité de la prestation des traitements de radiothérapie vitaux ;
- renforcer la cybersécurité et la résilience opérationnelle des services de radiothérapie en collaboration avec les services informatiques des hôpitaux, les partenaires du système de santé et les prestataires de services externes ;

- contribuer à la protection des données de santé sensibles des patients en se conformant à la gouvernance institutionnelle en matière de cybersécurité et aux pratiques exemplaires.

2.3 Public visé

Ce cadre s'adresse aux responsables des services de radiothérapie (par exemple, les radio-oncologues, les experts en physique médicale [EPM], les radiothérapeutes et les administrateurs de service), ainsi qu'aux partenaires hospitaliers et régionaux, notamment les services de la technologie de l'information, les équipes de cybersécurité, les services de gestion des risques d'entreprise et les équipes d'intervention en cas d'incident à l'échelle de l'hôpital. Si les programmes de radiothérapie constituent des intervenants clés, une mise en œuvre efficace nécessite une action coordonnée à l'échelle des établissements et du système. Les responsabilités particulières pour chaque mesure dépendront des structures de gouvernance locales, des ressources disponibles et du fait que des fonctions, telles que la sécurité des technologies de l'information et les interventions d'urgence, soient gérées au sein du service, à l'échelle de l'hôpital ou sur le plan régional/provincial.

2.4 Objectifs

Les principaux objectifs suivants ont été définis pour orienter l'élaboration du cadre :

I. **Renforcer la résilience :** améliorer la capacité des centres de radiothérapie partout au Canada à assurer la sécurité et la continuité de leurs activités pendant les événements perturbateurs, tels que les catastrophes naturelles, les pannes d'équipement et les cyberattaques, et à se remettre efficacement après ceux-ci.
II. **Normaliser les lignes directrices en matière de préparation aux situations d'urgence :** fournir un cadre cohérent et évolutif que les centres de radiothérapie de toutes tailles et de tous niveaux de maturité technologique puissent adopter, garantissant ainsi des lignes directrices claires et applicables pour la gestion des interruptions prolongées et imprévues.
III. **Promouvoir une gestion et un partage sécurisés des données :** mettre en place des mesures de protection des données, de contrôle d'accès et de partage interinstitutionnel sécurisés, conformes aux réglementations nationales et provinciales.
IV. **Favoriser la collaboration interinstitutionnelle :** encourager les centres de radiothérapie à partager leurs pratiques exemplaires, à coordonner leurs efforts en cas de perturbations et à se soutenir mutuellement grâce à des protocoles de communication standardisés et à des accords de soutien mutuel.
V. **Renforcer le transfert de connaissances et la sensibilisation :** offrir des possibilités de transfert de connaissances et des documents de référence afin de

garantir que le personnel clinique, technique et administratif soit prêt à réagir efficacement en cas de situation d'urgence.

VI. **Faciliter la collecte de retours d'information pour une amélioration continue :** favoriser une culture d'apprentissage continu en recueillant les retours d'information des centres de radiothérapie et de l'ensemble du système de santé, en analysant les données relatives aux incidents et mettant à jour le cadre de référence en fonction des enseignements tirés.

2.5 Flexible et évolutif dans divers environnements cliniques

Compte tenu de la diversité des environnements de radiothérapie partout au Canada, qu'il s'agisse de grands établissements universitaires ou de petites cliniques communautaires, ce cadre a été conçu pour être flexible et adaptable. Les centres fonctionnent selon des structures de gouvernance variées, où le pouvoir décisionnel peut se situer à l'échelle du service, de l'hôpital, de la région ou de la province, ce qui influence la manière dont les ressources sont allouées et dont les changements sont mis en œuvre. De plus, les centres présentent des différences en matière de fournisseurs de services de radiothérapie, d'infrastructures de technologie de l'information et de niveaux de maturité technologique. À ce titre, ce cadre prévoit toute une gamme d'approches de mise en œuvre, allant des pratiques élémentaires de cybersécurité aux capacités plus avancées de détection des menaces et d'intervention en cas d'incident, permettant ainsi une adaptation aux réalités opérationnelles locales et aux contraintes organisationnelles.

2.6 Promouvoir la collaboration

Ce cadre souligne l'importance d'une collaboration coordonnée au sein des établissements (par exemple, les programmes de radiothérapie, les services informatiques des hôpitaux, les équipes de cybersécurité, le génie clinique, les services de communication et la direction), entre les établissements, ainsi qu'entre les administrations provinciales et territoriales. Une préparation et une gestion efficaces des interruptions imprévues ou prolongées nécessitent une définition claire des rôles, une vision commune de la situation et une prise de décision coordonnée à plusieurs échelons du système de santé.

En favorisant une collaboration structurée, des pratiques communes en matière de préparation aux situations d'urgence et un échange d'informations approprié, y compris les enseignements tirés des incidents ayant entraîné des interruptions, les organismes peuvent contribuer à des interventions coordonnées et rapides en cas de perturbation des services. Un contexte d'apprentissage pancanadien, qui permet de partager les expériences, les stratégies d'atténuation et les approches de rétablissement dans les différentes provinces et différents territoires, renforce la résilience collective et réduit la duplication des efforts.

Il est important de noter que les efforts visant à préserver la continuité des soins doivent être conciliés avec la sécurité des patients, les obligations réglementaires et la gestion des risques cliniques. Les flux de travail de rechange ou les mesures d'urgence mises en œuvre pendant les interruptions des activités doivent faire l'objet d'une évaluation formelle et d'une gestion rigoureuse afin d'éviter d'introduire des risques cliniques ou opérationnels imprévus.

Grâce à une collaboration intégrée et à un partage des connaissances, la communauté canadienne de radiothérapie peut renforcer sa préparation, protéger les données des patients et favoriser la prestation de soins sûre et résiliente à l'échelle nationale.

3. Méthodologie

La méthodologie utilisée pour élaborer le *Cadre pancanadien de préparation aux situations d'urgence en cas d'interruption des activités des centres de radiothérapie* a suivi une approche globale en plusieurs phases qui a intégré les pratiques exemplaires et la documentation internationales, la collecte de données à l'échelle pancanadienne et une large consultation des parties prenantes. Cette approche a permis de garantir que le cadre repose sur des données probantes et qu'il soit adapté aux réalités opérationnelles des centres de radiothérapie canadiens. Dans les cas où cela s'imposait, les enseignements tirés de l'utilisation concrète d'outils, tels que les systèmes de gestion des informations et des événements de sécurité (GIES), ont été mis en correspondance avec des mesures de suivi précises[7].

3.1. Analyse du contexte

3.1.1. Revue de la littérature

Une analyse détaillée du contexte a été menée afin d'évaluer les normes mondiales et les pratiques exemplaires en matière de préparation aux situations d'urgence et de cybersécurité, ainsi que leur pertinence pour la radiothérapie. Les principales références comprenaient :

- **Cadre de cybersécurité de l'ESTRO** : Élaboré par la Société européenne de radiothérapie et d'oncologie (ESTRO)[8], ce cadre présente un modèle de cycle de vie en six étapes spécialement conçu pour les services de radio-oncologie. Il met l'accent sur la planification de la continuité des activités, l'identification des systèmes critiques, les mesures de protection techniques, la formation du personnel et l'apprentissage continu après incident. Il traite plus particulièrement des cybermenaces dans le domaine de la radiothérapie, en formulant des

recommandations allant de la résilience avant un incident aux flux de travail de rétablissement après un incident.[9]

- **Recommandations ECHO en matière de cybersécurité clinique** : Élaborées par l'Institute of Global Health Innovation de l'Imperial College London, les lignes directrices ECHO visent à renforcer la maturité en matière de cybersécurité dans les établissements de santé. Elles comprennent un modèle de maturité structuré et des listes de contrôle pratiques portant sur la gouvernance, la détection des menaces, la planification de l'intervention en cas d'incidents et la sensibilisation du personnel. Ces lignes directrices mettent l'accent sur une approche multidisciplinaire et accordent la priorité à la sécurité des patients dans la planification de la cybersécurité[10].

- **Cadre de cybersécurité (CSF) du NIST** : Élaboré par l'Institut national américain des normes et des technologies (NIST), le CSF est une approche volontaire et fondée sur les risques en matière de cybersécurité, articulée autour de cinq fonctions essentielles : identifier, protéger, détecter, réagir et rétablir. Il comprend des catégories et sous-catégories détaillées correspondant aux résultats souhaités en matière de cybersécurité et renvoie à un large éventail de normes internationales. Le CSF est particulièrement apprécié pour son évolutivité et son adaptabilité dans divers secteurs, notamment celui des soins de santé[11].

- **Guide de l'Organisation mondiale de la Santé (OMS) pour la planification de la continuité des activités :** Élaboré par le service de préparation aux urgences sanitaires nationales du Programme des urgences sanitaires de l'OMS et le Règlement sanitaire international, ce guide propose un cadre structuré couvrant l'ensemble du cycle de vie de l'organisme, conçu pour renforcer la résilience et la continuité des opérations face à tous les types de risques. Il met l'accent sur les phases clés, l'évaluation des risques, l'identification des fonctions critiques, l'élaboration de plans, les simulations/exercices, le suivi et l'examen, dans le but de permettre au siège, aux bureaux régionaux et nationaux de maintenir ou de rétablir les services essentiels et de réagir efficacement en situation d'urgence. Ce guide s'aligne sur la politique de gestion des risques de l'OMS, le système de gestion de la résilience organisationnelle (ORMS) des Nations Unies et les obligations découlant du Règlement sanitaire international[12].

- **Trousse à outils du NHS England pour la gestion de la continuité des activités :** Élaborée par un groupe de travail mis en place par le NHS England, elle propose une trousse à outils complète, spécialement adaptée au secteur de la santé, destinée à aider les organismes et les prestataires du NHS à maintenir la continuité des

services essentiels en cas de perturbation. Cette trousse à outils s'articule autour du cycle Planifier — Faire — Vérifier — Agir (PFVA), conformément aux principes de la norme ISO 22301 et aux lignes directrices de 2018 sur les bonnes pratiques en matière de continuité des activités[13].

- **Norme ISO 22301 — Systèmes de gestion de la continuité des affaires :** Élaborée par l'Organisation internationale de normalisation (ISO), cette norme fournit un cadre international normalisé permettant aux organismes de planifier, de mettre en place, de mettre en œuvre, d'exploiter, de surveiller, de réviser, de maintenir et d'améliorer en permanence un système de gestion documenté visant à prévenir les incidents perturbateurs, à réduire leur probabilité et à garantir le rétablissement après leur survenue. La norme s'applique à toutes les organisations, indépendamment de leur type, leur taille ou leur nature, et vise à garantir que celles-ci puissent continuer à fournir des produits et des services selon une capacité prédéfinie acceptable en cas de perturbation[14].

- **Norme Z1600, Association canadienne de normalisation (Groupe CSA) :** Élaborée par le Groupe CSA, un organisme d'élaboration de normes reconnu et accrédité par le Conseil canadien des normes. La série Z1600 fournit des critères complets permettant aux organismes d'établir, de mettre en œuvre, d'évaluer et de maintenir des programmes de gestion des urgences et de la continuité des activités qui traitent de la prévention, de l'atténuation, de la préparation, de l'intervention et du rétablissement. L'édition 2017 (Z1600-17) remplace les éditions précédentes publiées en 2014 et 2008.[15]

3.1.2. Enquête pancanadienne sur la préparation aux situations d'urgence et la cybersécurité

Afin de mieux comprendre les pratiques actuelles en matière de préparation aux situations d'urgence et de cybersécurité dans le domaine de la radiothérapie au Canada, une enquête a été élaborée et transmise aux centres de radiothérapie du pays.

- **Conception de l'enquête** : L'enquête finale comprenait 30 questions de formats variés, alignées sur les 6 domaines du cycle de vie définis par le cadre de cybersécurité en radio-oncologie de l'ESTRO. Les thèmes abordés comprenaient la conformité législative, la redondance des systèmes, les pratiques d'hygiène en matière de cybersécurité, les protocoles de sécurité des patients, l'intervention en cas d'incident et les stratégies de rétablissement concrètes.

- **Diffusion de l'enquête** : L'enquête a été envoyée aux centres de radiothérapie du Canada en collaboration avec le groupe consultatif, en ciblant les responsables de la radiothérapie, les physiciens médicaux, les équipes informatiques des hôpitaux et les directeurs des opérations, en fonction de la structure organisationnelle de chaque province. Dans les grandes provinces, on a cherché à obtenir au moins deux ou trois réponses afin de refléter les variations au sein de la province, tandis qu'on attendait au moins une réponse détaillée de la part des plus petites provinces.

- **Pratique en milieu réel** : Les participants à l'enquête ont également été encouragés à soumettre les politiques, outils et procédures institutionnels existants afin de contribuer à l'élaboration du cadre. Plusieurs outils et protocoles partagés par les centres de radiothérapie et les programmes régionaux visant à diminuer le fardeau du cancer ont fourni des informations précieuses sur les pratiques en matière de préparation aux situations d'urgence.

- **Taux de réponse :** Des réponses ont été reçues de la part de 32 centres de radiothérapie répartis dans les 10 provinces. Dans certains cas, une seule réponse regroupait les commentaires de plusieurs centres. Au total, cela représente plus de la moitié des 49 centres de radiothérapie du Canada, y compris 2 sites satellites dotés d'un seul accélérateur linéaire (LINAC) en Ontario, affiliés à de plus grands centres régionaux. Grâce à la participation de toutes les provinces, l'ensemble des données reflète une perspective diversifiée et pancanadienne.

3.1.3. Plans et ressources de préparation aux situations d'urgence

Les centres de radiothérapie canadiens interrogés ont partagé plusieurs ressources et outils, qui ont contribué à l'élaboration du ***Manuel pancanadien de préparation aux situations d'urgence et de ressources en radiothérapie*** et ont favorisé le partage des connaissances entre les différentes provinces ainsi que les possibilités plus larges d'adaptation et de mise à l'échelle. Quelques exemples de ressources :

1. **Politique relative aux procédures en cas d'interruption du Waterloo Regional Health Network (2025) :** Cette politique définit en détail la procédure d'intervention en cas d'interruption du système d'information en radio-oncologie (ROIS) pour les services de radiothérapie. Elle comprend la mise en œuvre d'un protocole d'interruption de service imprimé, le passage à la prestation de soins hors ligne au moyen du téléchargement des plans par clé USB, la saisie manuelle des données dans des classeurs dédiés à l'interruption de service, ainsi que la réintégration des

données de traitement après le rétablissement du service. Cette procédure fait l'objet de tests préventifs et est intégrée à la formation annuelle[16].

Dans ce cadre, cette politique soutient les domaines de l'intervention et du rétablissement en proposant un processus opérationnel éprouvé en cas de panne du ROIS, accompagné d'outils visant à garantir la continuité des soins, la documentation manuelle et la restauration de l'intégrité des données après une interruption de service.

2. **Guide de pratique clinique en cas d'interruption de traitement du CHU de Québec–Université Laval (UL) (2024) :** Ce guide classe les patients en radiothérapie en fonction de l'urgence de leur état et de la sensibilité de celui-ci aux retards de traitement (catégories 1 à 3). Il définit les seuils au-delà desquels des mesures compensatoires, telles que l'ajustement de la dose ou le fractionnement accéléré, doivent être mises en œuvre. Le guide comprend également des exemples de processus opérationnels et de stratégies de triage utilisés lors d'interruptions cliniques antérieures, notamment des algorithmes de priorisation et la réaffectation des plages de traitement[17].

   Ce guide contribue aux domaines de la préparation et de l'intervention de ce cadre en proposant des procédures standardisées de triage des patients et en fournissant une justification clinique pour le report ou la modification des soins dans des situations où les ressources sont limitées.

3. **Santé Ontario (Action Cancer Ontario) — Liste de contrôle relative aux PE sur la préparation aux situations d'urgence (2023) :** Cet outil provincial aide les centres de radiothérapie de l'Ontario à officialiser leurs partenariats d'urgence grâce à des protocoles d'entente (PE). Il décrit les conditions techniques et cliniques préalables au transfert des soins aux patients entre des centres jumelés en cas d'interruption prolongée des services, tout en soutenant les programmes spécialisés. La liste de contrôle couvre le remboursement financier, le déploiement du personnel, les accords médico-légaux, le partage des données DICOM-RT et les protocoles de communication[18].
   Dans ce cadre, cet outil soutient les domaines de la préparation et de l'intervention en identifiant les aspects complexes à prendre en compte lors de l'examen du transfert des soins entre deux centres.

4. **Lettre d'accord (LA) du Programme régional de cancérologie de Hamilton Niagara Haldimand Brant — Redéploiement en radiothérapie (2021) :** Cette lettre d'accord (LA) établit un cadre juridique et opérationnel pour le redéploiement temporaire du personnel clinique entre deux établissements de santé en cas

d'interruption de service ou d'urgence. Elle a été élaborée de manière proactive afin de permettre un soutien rapide en matière de personnel entre les établissements, au besoin.
La lettre d'accord définit des dispositions clés, notamment la double responsabilité envers les organismes qui fournissent et reçoivent le personnel, des structures de supervision bien définies, l'indemnisation juridique, les modalités relatives aux salaires et aux avantages sociaux, ainsi que les clauses de résiliation. Bien que l'accord n'ait pas encore été mis en œuvre à ce jour, son élaboration témoigne d'une planification avancée en matière de préparation. La mise en place d'un tel accord réduit considérablement le temps et la charge administrative nécessaires à la mobilisation du personnel en cas de crise.
Dans ce cadre, cette LA soutient le domaine de la préparation et montre comment des accords formels de redéploiement du personnel peuvent renforcer la préparation aux situations d'urgence, en particulier dans les régions où les programmes de radiothérapie peuvent être contraints de partager leurs ressources en personnel lors d'interruptions prolongées[19].

5. **Document d'orientation sur le regroupement des services de radiothérapie du Programme régional de cancérologie de Hamilton Niagara Haldimand Brant (2020) :** Ce document présente les protocoles de planification visant à regrouper les services de radiothérapie entre différents sites en cas de perturbations importantes des services, en abordant plus particulièrement le transfert des activités entre les centres. Il aborde notamment la planification logistique, la coordination des transports, le transfert des fournitures et la documentation relative au financement des soins (c'est-à-dire les codes de facturation).
   Dans ce cadre, le protocole soutient les domaines de la préparation et de l'intervention en proposant des protocoles de planification des fortes augmentations d'activité et de réaffectation des capacités, notamment pour les scénarios de suspension régionale des services[20].

6. **Procédure de réorientation des soins aux patients en situation d'urgence du Programme régional de cancérologie de Hamilton Niagara Haldimand Brant (2021) :** Cette procédure a été élaborée pendant la pandémie de COVID-19 afin de faire face au risque de pénurie critique de personnel susceptible de compromettre la capacité du programme visant à diminuer le fardeau du cancer à fournir des services de radiothérapie. Elle fournit un cadre opérationnel permettant de transférer en toute sécurité les patients en oncologie d'un établissement à un autre lorsque la capacité locale de prise en charge est considérablement réduite. Le schéma de la procédure décrit les étapes nécessaires pour identifier les

établissements d'accueil (« hôtes »), gérer les transitions entre les rôles cliniques, coordonner la prestation des traitements de radiothérapie, harmoniser les flux de travail en matière de diagnostic et de documentation, concilier les considérations financières et définir les responsabilités en matière de communication entre les organismes.

Dans le cadre de ce programme, la structure et les principes de cette procédure ont servi de base aux domaines de la préparation et de l'intervention en informant les stratégies de continuité des soins et de réacheminement régional en situation d'urgence ou lors d'interruptions prolongées[21].

7. **Manuel d'exercices fonctionnels du Programme régional de cancérologie de Hamilton Niagara Haldimand Brant (2021) :** Ce document comprend un exercice sur table basé sur un scénario, conçu pour préparer les services de radiologie à faire face à des pénuries de personnel à grande échelle pendant la pandémie de COVID-19. L'exercice présente des modules structurés pour définir les objectifs en cas d'incident, activer les centres de commandement, trier les patients et coordonner la communication entre les hôpitaux partenaires. Il évalue l'état de préparation des établissements, les stratégies de transfert des capacités et l'utilisation d'outils de soutien consolidés, tels que les grilles de priorisation et les rapports sur les enseignements tirés.

   Dans ce cadre, cet exercice soutient les domaines de la préparation et de l'intervention à l'aide d'essais basés sur la simulation[22, 23]

8. **Manuel du système de gestion des incidents du Programme régional de cancérologie de Hamilton Niagara Haldimand Brant (2022) :** Ce manuel décrit la procédure à suivre pour mettre en place un centre de commandement régional ou multi-institutionnel. Il définit les rôles des principaux intervenants (par exemple, les responsables médicaux, la logistique et les communications) et comprend des outils standardisés de gestion des incidents, tels que les comptes rendus d'incident et les plans d'action en cas d'incident (PAI)[24].

   Dans ce cadre, le manuel soutient les domaines de la préparation et de l'intervention grâce à des outils structurés couramment utilisés dans la gestion des incidents.

9. **Présentation du système de gestion des incidents et du processus du plan d'action en cas d'incident du Centre de cancérologie Juravinski (2021) :** Ce document décrit le déroulement opérationnel et le processus décisionnel relatifs au renvoi des questions vers un organisme central de coordination. Il précise quand et comment les hôpitaux doivent mobiliser des partenaires pour une intervention coordonnée.

Dans ce cadre, ces processus opérationnels éclairent les domaines de la préparation, de l'intervention et du rétablissement en définissant des niveaux de communication et de recours hiérarchique standardisés[25, 26]

10. **Liste régionale de diffusion des informations du Programme régional de cancérologie de Hamilton Niagara Haldimand Brant (2021) :** Un outil de relais de communication qui permet de maintenir à jour un organigramme de communication entre les centres régionaux de cancérologie afin d'assurer une mobilisation rapide en cas d'urgence[19].

Dans ce cadre, ce modèle sert de référence pour les domaines de la préparation et de l'intervention en proposant un outil standardisé permettant de documenter les rôles clés et les coordonnées utiles en cas d'interruption imprévue et prolongée.

3.1.4. Intégration des outils de cybersécurité

Les services informatiques des hôpitaux mettent généralement en œuvre des outils de cybersécurité dans le cadre de stratégies de sécurité à l'échelle de l'établissement. Les programmes de radiothérapie doivent être impliqués afin de s'assurer que ces outils ne perturbent pas les systèmes cliniques essentiels, notamment la planification des traitements, les systèmes de contrôle et d'enregistrement (R&V), l'imagerie et les systèmes d'information en oncologie. Les catégories d'outils décrites ci-dessous représentent des approches couramment utilisées dans le secteur des soins de santé pour renforcer la cyberrésilience. Elles sont fournies à titre d'exemples illustratifs et ne constituent en aucun cas une liste normative ou approuvée. Le choix doit se fonder sur les politiques informatiques locales, les exigences cliniques et l'interopérabilité avec les flux de travail en radiothérapie.

1. **Plateformes de simulation d'hameçonnage :** Ces plateformes permettent de former le personnel à identifier et à répondre aux attaques d'ingénierie sociale, en particulier les menaces d'hameçonnage par courriel. Les simulations reproduisent des scénarios d'attaque réalistes, ce qui permet aux organismes d'évaluer le niveau de sensibilisation du personnel et de suivre les progrès réalisés au fil du temps. Il a été démontré que la réalisation régulière de simulations d'hameçonnage permettait de réduire le taux de réussite des attaques d'hameçonnage réelles[27].
2. **Systèmes de gestion des informations et des événements de sécurité (GIES) :** Les systèmes GIES servent de plateformes centralisées pour la collecte, la normalisation et l'analyse des données de journaux à l'échelle de l'infrastructure de technologie de l'information, y compris les périphériques réseau, les serveurs, les applications et les terminaux des utilisateurs. Ils assurent une surveillance en temps

réel et génèrent des alertes sur la base de signatures de menaces connues ou d'activités anormales[28].

3. **Outils de détection et d'intervention sur les terminaux (EDR) :** Les solutions EDR sont axées sur la surveillance des terminaux (par exemple, postes de travail, ordinateurs portables, appareils mobiles). Ces outils détectent les comportements malveillants et réagissent à ceux-ci, tels que les tentatives d'accès non autorisées, l'exécution de logiciels suspects ou les mouvements latéraux au sein de l'environnement. Beaucoup d'entre eux intègrent des mesures de réponse automatisées, comme l'isolation des terminaux compromis du réseau. L'EDR s'avère particulièrement utile dans les environnements cliniques décentralisés comportant plusieurs points d'accès[29].

4. Conception et élaboration du cadre

4.1 Structure du cadre

L'élaboration du *Cadre pancanadien de préparation aux situations d'urgence en cas d'interruption des activités des centres de radiothérapie* s'est appuyée sur une approche multisource comprenant une analyse approfondie de la littérature, une analyse comparative internationale et un processus de consultation pancanadien structuré. L'objectif était d'ancrer le cadre dans les pratiques exemplaires mondiales tout en garantissant son adaptabilité au contexte opérationnel et réglementaire des centres de radiothérapie canadiens.

Le cadre de cybersécurité de l'ESTRO a constitué un point de référence essentiel pour la conception structurelle [9] ; il propose un modèle basé sur le cycle de vie visant à renforcer la résilience numérique dans le domaine des soins contre le cancer. S'inspirant de ce modèle, le cadre canadien a été adapté pour inclure six domaines fonctionnels couvrant l'ensemble du spectre de la cybersécurité et de la préparation aux situations d'urgence, de la prévention avant incident au rétablissement après incident. Ces domaines servent de fondement à un ensemble de mesures d'action ciblées qui tiennent compte des défis uniques liés aux flux de travail, à l'infrastructure et aux relations interorganisationnelles des centres de cancérologie canadiens.

L'adaptation canadienne intègre des considérations cliniques, opérationnelles et techniques, en mettant l'accent sur une approche multidisciplinaire du renforcement de la résilience. Des informateurs clés partout au pays ont souligné que le cadre doit prendre en compte non seulement les événements à faible fréquence et à fort impact (par exemple, les attaques par rançongiciel ou les catastrophes naturelles) ainsi que les pannes complètes du système (par exemple, défaillance des serveurs ou du système),

mais aussi les dégradations du système, telles qu'un ralentissement considérable du fonctionnement ou des défaillances partielles de certaines fonctionnalités. Ces dégradations surviennent plus fréquemment que les pannes complètes et peuvent perturber le déroulement clinique, la continuité des soins et la sécurité des patients de manière presque aussi importante. Par conséquent, le cadre qui en résulte est conçu pour être évolutif, fondé sur des données probantes et ancré dans les vulnérabilités opérationnelles et les lacunes pratiques observées en situation réelle.

4.2 Cadre de cybersécurité de l'ESTRO

Le cadre de l'ESTRO comporte six domaines clés[9]. Il présente un modèle en six étapes adapté aux services de radio-oncologie, qui reflète une approche globale du cycle de vie :

1. **Préparation** : Conception et préparation des procédures pour les situations d'urgence et la continuité des activités
2. **Prévention** : Mise en œuvre de mesures de protection techniques et organisationnelles
3. **Détection** : Surveillance des systèmes afin de détecter les signes de perturbation ou des cyberincidents
4. **Intervention** : Activation des protocoles d'intervention en cas d'incident, gestion des communications et maintien de la continuité des soins aux patients
5. **Rétablissement** : Restauration des systèmes, validation des données et reprise des activités normales
6. **Amélioration continue** : Réalisation d'analyses après incident et mise à jour des plans en fonction des enseignements tirés

Les six domaines de la cyberrésilience et de la résilience opérationnelle en radiothérapie s'appuient sur trois catégories complémentaires de mesures d'action. Ces catégories offrent une approche structurée pour planifier, mettre en œuvre et évaluer les mesures de protection liées à la technologie, à l'organisme et aux personnes.

I. **Technologique (T) :** Matériel informatique, logiciels et solutions de sécurité des réseaux
II. **Organisationnelle (O) :** Politiques, structures de gouvernance et mécanismes de coordination
III. **Axée sur l'humain (H) :** Formation du personnel, sensibilisation et considération des facteurs humains

4.3Résultats de l’enquête pancanadienne

Une enquête menée en 2025 a permis d’obtenir un aperçu pancanadien des pratiques en matière de préparation aux situations d’urgence et de cybersécurité dans les centres de radiothérapie. Bien que la méthodologie détaillée et les taux de réponse soient décrits dans la section 3, les conclusions générales mettent en évidence des tendances et des lacunes qui ont directement éclairé l’élaboration du cadre.

Parmi les principaux enseignements, on peut citer les suivants :

- **Gouvernance et responsabilité :** La cybersécurité et la gestion des systèmes techniques étaient généralement assurées par les services informatiques des hôpitaux ou des autorités sanitaires, tandis que la préparation clinique et la continuité des soins aux patients relevaient de la direction des programmes de radiothérapie. Cela a souligné la nécessité d’une coordination interfonctionnelle plus claire et de modèles intégrés d’intervention en cas d’incident.
- **Redondance et capacité de rétablissement :** Les centres plus grands ou plus centralisés disposaient souvent d’une redondance pour les systèmes critiques, tandis que les sites plus petits ou ruraux comptaient sur des solutions hébergées par des fournisseurs ou disposaient de capacités de secours limitées.
- **Simulation et formation :** Les exercices formels de simulation d’interruption, les exercices sur table et les essais de flux de travail hors ligne n’ont pas été menés de manière systématique, ce qui souligne l’importance de simulations régulières pour garantir l’état de préparation.
- **Coordination interinstitutionnelle :** Les accords relatifs au transfert de patients ou au redéploiement du personnel en cas d’interruption prolongée étaient rares, ce qui souligne la nécessité de mettre en place des mécanismes de collaboration régionaux préétablis.
- **Défis communs :** Parmi les problèmes récurrents figuraient les infrastructures existantes, les effectifs limités (en informatique et en physique clinique), les contraintes budgétaires et la mobilisation variable des fournisseurs pour mettre en place des procédures d’urgence réalisables.

Ces conclusions ont guidé les recommandations du cadre en matière de gouvernance, de redondance, de formation, de collaboration entre les services et entre les établissements, ainsi que de processus de rétablissement structurés.

4.4 Classification des mesures d'action

Au total, **194 mesures d'action** ont été identifiées et classées selon les six domaines clés du *Cadre pancanadien de préparation aux situations d'urgence en cas d'interruption imprévue et prolongée des activités des centres de radiothérapie*. Ces domaines (prévention, préparation, détection, intervention, rétablissement et amélioration continue) reflètent le modèle du cycle de vie des incidents adopté par l'ESTRO, garantissant ainsi la cohérence avec les pratiques exemplaires internationales tout en permettant une adaptation au contexte local.

Chaque mesure d'action a été examinée et classée dans le domaine qui reflétait le mieux sa fonction opérationnelle principale au sein de la résilience du système de radiothérapie. Bien que de nombreuses mesures touchent plusieurs phases du cycle de vie, seul leur alignement le plus critique a été retenu à des fins de classification, afin d'éviter les doublons et de garantir la clarté de la mise en œuvre.

Afin de favoriser davantage la collaboration interdisciplinaire et l'allocation des ressources, chaque mesure a également été classée dans l'une des trois catégories suivantes :

- **Technologique (T)** — Mesures portant sur les infrastructures, les systèmes numériques, les outils logiciels, la planification de la redondance et les infrastructures de cybersécurité.
- **Organisationnelle (O)** — Mesures axées sur la gouvernance, l'élaboration de politiques, les procédures de recours hiérarchique, la coordination entre les services et entre les établissements, ainsi que les accords avec les fournisseurs. *Il est important de noter que la catégorie « Organisationnelle » englobe des responsabilités pouvant dépasser le contrôle ou l'influence directs du programme de radiothérapie, notamment la direction de l'hôpital, les services informatiques, les autorités provinciales ou les prestataires de services contractuels*.
- **Axée sur l'humain (H)** — Mesures qui donnent la priorité à la formation du personnel, aux campagnes de sensibilisation, aux simulations de triage, aux flux de communication et à la clarification des rôles.

Cette classification à deux niveaux (par domaine et par type) garantit une approche équilibrée, permettant aux établissements d'évaluer leurs points forts et leurs lacunes en matière de capacités techniques, de préparation organisationnelle et de ressources humaines. En reconnaissant explicitement que certaines mesures organisationnelles ne relèvent pas directement du programme de radiothérapie, le cadre précise quelles mesures nécessitent une collaboration avec des parties prenantes institutionnelles ou provinciales plus larges. Cette approche permet aux équipes informatiques, aux responsables des

programmes de radiothérapie et aux décideurs politiques d'identifier clairement les responsabilités et de coordonner la mise en œuvre de composantes particulières du cadre.

4.5 Répartition des mesures par domaine

Les mesures d'action ont été réparties entre les six domaines clés du cycle de vie du cadre, un petit sous-ensemble ayant été classé comme recoupant plusieurs domaines ou non attribué en raison de sa nature générale ou fondamentale.

Cette répartition reflète les priorités identifiées par les parties prenantes, les pratiques exemplaires internationales et les points de défaillance courants observés lors d'incidents réels. Elle souligne également la nécessité d'un équilibre entre la planification proactive de la continuité des activités, les mesures de protection techniques, l'intervention en temps réel en cas d'incident et l'apprentissage à long terme du système.

Domaine	Nombre de mesures	Exemples
Préparation	40	Modèles d'inventaire des risques, cartographie des rôles, accords juridiques, exercices sur table
Prévention	37	AFM[1], gestion des correctifs, formation du personnel sur l'hameçonnage
Détection	17	GIES[2], alerte d'anomalies, surveillance des terminaux
Intervention	48	Activation du système de commandement en cas d'incident, procédures manuelles de traitement, triage des patients
Rétablissement	22	Protocoles de restauration, revalidation des systèmes, réintégration des dossiers
Amélioration continue	22	Compte rendu après incident, révision du cadre, mécanismes de retour d'information du personnel
Autre	8	Diffusion du cadre, coordination de la surveillance nationale, mobilisation de fonds

[1] Authentification à facteurs multiples.
[2] Gestion des informations et des événements de sécurité

Cette répartition renforce la nécessité d'investir non seulement dans les infrastructures de cybersécurité, mais aussi dans la gouvernance, la formation et les leçons tirées des incidents. La forte présence de mesures de prévention et de préparation reflète l'importance accordée par le cadre canadien et les cadres internationaux à l'atténuation proactive des risques.

5. Le cadre

5.1. Domaine de la préparation

La préparation établit les éléments fondamentaux nécessaires à des interventions coordonnées, rapides et efficaces en cas d'interruption de service, qu'elles soient causées par des cyberattaques, des défaillances d'infrastructure ou des urgences externes. Ce domaine vise à renforcer la préparation organisationnelle grâce à la mise en place d'un plan de continuité des activités formalisé, de structures de gouvernance, d'évaluations de base des risques et d'une harmonisation des parties prenantes. Il comprend l'élaboration de systèmes d'inventaire des actifs critiques, la précision des rôles et des responsabilités au sein des services informatiques, cliniques et des partenaires fournisseurs, ainsi que la garantie d'une bonne maîtrise des cadres établis. La préparation porte également sur la connaissance de la législation et la conformité réglementaire en incitant les établissements à identifier leurs obligations au titre des lois sur la protection de la vie privée. Les centres de radiothérapie canadiens ayant participé à l'enquête pancanadienne ont systématiquement identifié l'absence de planification formelle, le manque de clarté des rôles et la méconnaissance des politiques comme des obstacles majeurs à la préparation. À ce titre, ce domaine intègre des enseignements tirés de la réalité dans tout le pays, en mettant l'accent sur des mesures pragmatiques de préparation, telles que la cartographie des systèmes, l'évaluation des capacités de base et l'intégration de la cybersécurité dans les structures plus larges de planification d'urgence. Les mesures décrites dans ce domaine constituent des conditions préalables à toutes les phases suivantes du cadre et sont essentielles pour ancrer la cybersécurité et la préparation aux situations d'urgence dans la culture opérationnelle des programmes de radiothérapie.

N°	**Mesure d'action**	Catégorie
PP0 — Préparation générale		
PP0.1	**Comprendre la vulnérabilité des systèmes de radiothérapie et de soins de santé ainsi que la menace que représentent les interruptions prolongées** • Sensibiliser au fait que les centres de cancérologie canadiens sont exposés à diverses menaces, notamment les cyberattaques, les pannes matérielles ou logicielles et les catastrophes environnementales.	Organisationnelle

	• Sensibiliser aux vulnérabilités créées par des utilisateurs non formés ou mal informés, ainsi qu'aux lacunes en matière de préparation. • Sensibiliser à la nécessité d'être toujours prêt à intervenir rapidement et à assurer la continuité des soins en cas d'interruption prolongée. • Sensibiliser à la valeur, au caractère sensible et aux exigences réglementaires en matière de protection des données des patients en oncologie.	
PP0.2	**Comprendre les implications d'une interruption prolongée et imprévue** • Mieux comprendre les risques cliniques liés aux interruptions du traitement par radiothérapie, notamment les fractions retardées ou manquées. • Mieux comprendre les répercussions sur la sécurité des patients, notamment les erreurs de traitement résultant de solutions de contournement manuelles et les préjudices potentiels liés au report des soins. • Mieux comprendre les risques de perte ou de violation des données, y compris les répercussions sur la confidentialité, la conformité et la confiance. • Mieux comprendre les risques pour la réputation des programmes visant à diminuer le fardeau du cancer et des établissements partenaires en cas d'interruption des services.	Organisationnelle
PP0.3	**Comprendre les aspects concernés** • Mieux comprendre les personnes et les aspects concernés par les interruptions des services de radiothérapie, notamment les patients, les équipes cliniques, le personnel technique, le service informatique, les fournisseurs et les fonctions administratives. • Veiller à ce que les comportements des employés, les technologies utilisées et l'ensemble des processus opérationnels et cliniques soient conformes aux exigences établies en matière de continuité des activités et de sécurité des technologies de l'information. • Tenir compte des partenaires externes, tels que les programmes régionaux visant à diminuer le fardeau du cancer, les services informatiques des hôpitaux et les prestataires de services contractuels, afin de garantir une préparation coordonnée.	Organisationnelle
PP0.4	**Comprendre le coût des mesures de préparation** • Être conscient des coûts en ressources (humaines et financières) liés à la mise en œuvre de contre-mesures et de mesures préventives, tant en matière de cybersécurité que de préparation aux interruptions de service (par exemple, systèmes redondants, accords de prise en charge en cas de fortes augmentations d'activité, formation du personnel). • Veiller à ce qu'un processus budgétaire soit en place pour assurer la pérennité des mesures de préparation, y compris les mises à niveau régulières, la maintenance et les exercices. • Lors de la planification des budgets, tenir compte des coûts liés au rétablissement après une interruption prolongée, notamment la	Organisationnelle

	restauration des systèmes, la perte de productivité, la réorientation des patients et la réparation de la réputation. • Évaluer, à l'échelle de l'établissement ou du système de santé, si une assurance cybersécurité est appropriée pour aider à compenser les répercussions financières d'un incident de cybersécurité majeur. L'étendue de la couverture, les exclusions (par exemple, le paiement de rançons, les amendes réglementaires), les obligations de déclaration et les contrôles de sécurité imposés par l'assureur doivent être clairement compris à l'avance. Les décisions relatives à la souscription et aux limites de couverture relèvent généralement de la direction de l'hôpital ou de la région plutôt que des programmes de radiothérapie individuels, mais les responsables de la radiothérapie doivent en comprendre les implications en matière de rétablissement après une interruption et de traitement des réclamations.	
PP0.5	**Comprendre les exigences légales, réglementaires et politiques canadiennes applicables** • Identifier et consigner toutes les lois et tous les règlements fédéraux et provinciaux applicables en matière d'information sur la santé, tels que : la *LPRPS (Ontario), la LPRPDE (fédérale)* et les lois équivalentes dans les différentes provinces (HIA en Alberta, la *LRMP* en Manitoba, etc.), ainsi que les *initiatives fédérales* pertinentes (par exemple, les règlements de la CCSN, le projet de loi C-27 : la LPVPC et la LIAD, en cours d'examen). • Harmoniser les mesures relatives aux interruptions de service, à la cybersécurité et au rétablissement avec les normes réglementaires et professionnelles reconnues, telles que les exigences d'autorisation de la Commission canadienne de sûreté nucléaire (CCSN) et les codes de pratique du PCQR, afin de garantir que les pratiques de radiothérapie répondent aux attentes légales et de sécurité dans chaque province. • Intégrer les obligations légales et réglementaires dans les manuels relatifs aux interruptions de service, les PE et les PCA (par exemple, le partage de données en vertu de la LPRPS/LPRPDE, les mesures de protection de la vie privée pour la documentation manuelle). • Veiller à ce que le personnel soit informé de ces exigences au moyen d'une orientation, de formations de mise à niveau et d'exercices annuels d'interruption de service, afin de renforcer la conformité et les pratiques opérationnelles sécuritaires au sein du centre.	Organisationnelle
PP0.6	**Comprendre le contexte des partenaires et des parties prenantes** • Les programmes de radiothérapie doivent recenser toutes les parties prenantes internes et externes indispensables au maintien des services de radiothérapie en cas de perturbations. • Cartographier les relations, les rôles et les interdépendances entre les programmes visant à diminuer le fardeau du cancer, les services informatiques des hôpitaux, les réseaux provinciaux et les fournisseurs.	Organisationnelle

	• Veiller à ce que chacun connaisse les protocoles en cas d'interruption des services et les procédures de recours hiérarchique.	
PP0.7	**Comprendre les exigences en matière de communication pendant les interruptions** • Définir les personnes à informer, par qui et par quels moyens en cas d'interruption de service. • Veiller à ce que les plans de communication s'adressent au personnel interne, aux partenaires externes, aux patients et au grand public. • Intégrer les exigences en matière de communication dans les exercices de simulation d'interruption.	Organisationnelle + Axée sur l'humain
PP0.8	**Comprendre les objectifs de temps de rétablissement et les seuils d'interruption de service acceptables** • Identifier et définir la durée maximale d'interruption acceptable pour les systèmes critiques avant que les soins aux patients ne soient affectés de manière importante. Reconnaître que ces seuils peuvent varier d'un établissement à l'autre en fonction de l'infrastructure locale, du soutien disponible de la part des cliniques environnantes et de l'expérience acquise lors d'incidents similaires. • Définir des critères d'établissement des priorités pour rétablir les services, en tenant compte des systèmes et des processus les plus critiques pour la sécurité des patients et la continuité des soins. • Consigner ces objectifs de rétablissement et ces seuils d'interruption acceptables dans les plans de continuité des activités et de rétablissement après sinistre, en précisant les hypothèses, les contraintes et la justification qui les sous-tendent. • Réviser et mettre à jour régulièrement ces seuils, en fonction des enseignements tirés d'incidents réels d'interruption de services, de simulations ou de mises à niveau du système, afin de garantir qu'ils restent réalistes et réalisables.	Organisationnelle + Technologique
PP1 — Identification des systèmes, des outils, des processus et des parties prenantes, ainsi que de leurs faiblesses		
PP1.1	**Inventaire du matériel, des logiciels et des dépendances réseau** • Tenir un inventaire détaillé de tout le matériel et les logiciels utilisés dans le cadre des activités de radiothérapie, y compris les systèmes de planification de traitement, les systèmes d'information en oncologie (par exemple, ARIA, système d'information sur les patients en oncologie [OPIS]), les appareils d'imagerie et l'infrastructure de technologie de l'information associée. • Décrire tous les appareils qui communiquent ensemble, y compris les flux de données, les interfaces définies et l'architecture de réseau. • Vérifier et mettre à jour régulièrement l'inventaire, de préférence à l'aide d'un système automatisé de gestion des actifs, et en vérifier l'exactitude lors d'audits ou d'exercices de simulation d'interruptions de service. • Conserver les coordonnées facilement accessibles (par exemple, sous forme de copies papier) des fournisseurs et autres contacts d'assistance.	Technologique

PP1.2	**Catégorisation des systèmes et des processus** • Identifier et classer de manière générale les systèmes de radiothérapie, les données et les processus opérationnels en fonction de leur risque relatif d'interruption, de perte de données ou de perturbation des soins aux patients, en reconnaissant qu'une catégorisation exhaustive ou très détaillée pourrait ne pas être réalisable. • Se concentrer principalement sur les systèmes sous le contrôle ou l'influence directe du programme de radiothérapie, tels que les systèmes de planification de traitement, les systèmes d'information en oncologie, l'imagerie et d'autres outils opérationnels spécifiques au service (par exemple, la planification des rendez-vous, les plateformes de communication). • Il convient de noter que les systèmes à l'échelle de l'hôpital, tels que les DME, ne relèvent généralement pas du champ d'action ni du contrôle direct du service de radiothérapie, mais il est important de connaître leurs dépendances pour assurer la coordination avec les équipes informatiques de l'hôpital lors de la planification des interruptions ou du rétablissement. • Identifier les principales interfaces, les dépendances et les points de défaillance potentiels de haut niveau, afin d'orienter l'établissement des priorités et la planification du rétablissement, sans pour autant impliquer que l'inventaire détaillé des systèmes organisationnels relève de la responsabilité du programme de RT.	Technologique
PP1.3	**Priorités des systèmes** • Établir des priorités claires pour les systèmes de radiothérapie et les systèmes connexes en déterminant ceux qui sont essentiels au fonctionnement clinique quotidien et ceux qui peuvent être temporairement suspendus sans compromettre la sécurité des patients. • Définir la séquence de restauration des systèmes à la suite d'une panne, en tenant compte de l'urgence clinique, de la cartographie des dépendances, des répercussions opérationnelles et des exigences réglementaires applicables, y compris les obligations de conformité de la Commission canadienne de sûreté nucléaire (CCSN) relatives à l'administration de la radiothérapie et aux systèmes de sécurité. • Veiller à ce que les décisions en matière des priorités tiennent compte à la fois de la continuité des soins aux patients et de la conformité réglementaire, en particulier lorsque les interruptions de service pourraient avoir une incidence sur les équipements soumis à autorisation ou sur les seuils de sécurité des traitements. • Passer régulièrement en revue et mettre à jour les priorités du système afin de refléter les changements dans les flux de travail, les technologies, les modèles de prestation des traitements et toute mise à jour des directives réglementaires.	Technologique
PP1.4	**Documentation des configurations et des points d'intégration**	Technologique

	• Tenir à jour une documentation détaillée des configurations de système, des paramètres d'interface et des points d'intégration du réseau. • Veiller à ce que cette documentation soit conservée hors ligne en toute sécurité afin de pouvoir être consultée en cas de rétablissement après une interruption de service. • Conserver les mots de passe des comptes de service principaux, tant pour les systèmes sur site que pour les systèmes en ligne, dans un endroit sûr et sécurisé.	
PP1.5	**Analyse des risques/évaluation des risques** • Procéder à des analyses exhaustives des risques afin d'identifier les menaces et les faiblesses au sein des systèmes, des flux de travail et des processus de gestion des données en radiothérapie. Ces analyses doivent porter sur la cybersécurité, les défaillances matérielles et logicielles, les dépendances à l'égard des fournisseurs et les risques environnementaux. • Mener cette évaluation de manière collaborative, en étroite collaboration avec le service de radiothérapie et les équipes informatiques, de génie clinique et administratives concernées de l'hôpital, afin de garantir la prise en compte de tous les aspects techniques, cliniques et opérationnels. L'évaluation doit également tenir compte **du temps et des ressources nécessaires** à sa réalisation. • Les analyses des risques doivent être réalisées au moins une fois par an, ainsi que chaque fois que l'environnement évolue, par exemple en cas de modifications du système, de mises à jour logicielles ou de changements dans les flux de travail. • Réaliser une analyse des lacunes afin d'identifier les principaux défis, les répercussions et les stratégies d'atténuation envisageables. • Faire appel à du personnel hautement qualifié (par exemple, des spécialistes en sécurité des technologies de l'information, des physiciens médicaux, des ingénieurs cliniques, etc.) dans le cadre du processus d'évaluation. • Évaluer la faisabilité des traitements en l'absence de systèmes critiques, tels que les systèmes R&V, et consigner les risques ainsi que les approches d'atténuation. • Réévaluer régulièrement les risques, en utilisant des outils d'auto-évaluation lorsqu'ils sont disponibles, et envisager de faire appel à des services ou outils tiers de gestion des risques lorsque des compétences spécialisées sont nécessaires. Consigner clairement toutes les conclusions, les stratégies d'atténuation et les rôles/responsabilités des équipes de RT et informatiques de l'hôpital dans les plans de continuité des activités ou de rétablissement après sinistre.	Technologique + Axée sur l'humain
PP1.6	**Identification proactive des vulnérabilités** • Évaluer les risques et les vulnérabilités de l'ensemble du matériel, des logiciels (y compris les applications développées en interne ou sur	Technologique

	mesure) et des services fournis par les fournisseurs liés à la radiothérapie, en tenant compte à la fois de la cybersécurité et de la résilience opérationnelle. Cette évaluation devrait être réalisée par un groupe de travail collaboratif composé d'experts multidisciplinaires, notamment du personnel de radio-oncologie, des physiciens médicaux, des spécialistes en technologie de l'information, des ingénieurs cliniques et des fournisseurs de systèmes. • Pour les logiciels développés en interne ou localement, il convient de s'assurer que les pratiques de conception, de codage et de déploiement répondent aux exigences de sécurité et de fiabilité, notamment en matière de contrôle d'accès, de consignation, de tests et de validation. Consigner ces considérations de conception dans le cadre du processus d'évaluation des risques. • Examiner ou réaliser des audits de sécurité des fournisseurs et des évaluations de la gestion des risques liés aux tiers, en veillant à ce que les accords sur les niveaux de service (ANS) prévoient des mesures de préparation aux interruptions de service ainsi que la cybersécurité. • Identifier les points de défaillance uniques et s'assurer que des stratégies d'atténuation sont en place, telles que la redondance, des systèmes de secours ou des flux de travail de rechange.	
PP1.7	**Gestion des parties prenantes** • Comprendre les objectifs, les responsabilités et les rôles de toutes les parties prenantes, notamment les patients, le personnel de la santé, la direction, les fournisseurs et l'ensemble de la chaîne d'approvisionnement en radiothérapie. • Identifier les vulnérabilités liées au facteur humain (par exemple, manque de formation, non-respect des procédures) et définir des stratégies pour y remédier au moyen de formations, d'exercices et de protocoles clairement consignés. • Établir des politiques de communication, de confidentialité et de sécurité pour toutes les parties prenantes, applicables tant en période de fonctionnement normal qu'en cas d'interruption prolongée.	Organisationnelle + Axée sur l'humain
PP1.8	**Coopération régionale** • Établir et maintenir des mécanismes visant à organiser et à faciliter la coopération régionale en matière de préparation et d'intervention en cas d'interruption des activités de radiothérapie. • Impliquer les organismes professionnels et non gouvernementaux, selon le cas, y compris les agences provinciales du cancer, les réseaux hospitaliers et les partenaires de gestion des urgences. • Soutenir les accords d'assistance mutuelle, de partage des ressources et de transfert coordonné des patients dans les différentes provinces et différents territoires en cas d'interruption prolongée.	Organisationnelle
PP1.9	**Tirer parti des enseignements tirés des incidents passés** • Intégrer les enseignements tirés d'incidents passés (par exemple, les pénuries de personnel liées à la COVID-19, les attaques par rançongiciel) dans les protocoles d'intervention immédiate. Tenir à jour une base de connaissances ou des archives de comptes rendus	Organisationnelle + Axée sur l'humain

	après incident dans le cadre de vos processus d'amélioration continue.	
PP2 — Définir un plan de continuité des activités (PCA)		
PP2.1	**Plan de continuité des activités (PCA)** • Tenir à jour un plan de continuité des activités (PCA) officiel dans le cadre de l'assurance de la qualité globale, avec des copies papier accessibles sur les postes de travail pour toutes les modalités. • Ce plan devrait inclure des procédures prédéfinies pour la gestion des incidents, des phases de continuité définies, des processus de restauration, l'implication des instances compétentes et des procédures de recours hiérarchique. Ces éléments devraient garantir que le personnel de première ligne connaisse ses rôles et ses responsabilités en matière de recours hiérarchique, plutôt que de devoir gérer seul des situations complexes ou à haut risque. Le PCA doit également prévoir des solutions techniques de contournement en cas d'interruption des systèmes, accompagnées de directives claires concernant les processus d'évaluation et d'approbation de la sécurité, afin de garantir que les procédures temporaires ne compromettent pas les soins aux patients ou la sécurité clinique. • Dans la mesure du possible, le PCA doit définir des dispositions relatives à un réseau d'urgence ou virtuel préconfiguré (par exemple, pour relier le SIO, les LINAC, le TPS et les systèmes de TDM) qui pourrait être activé en cas de perturbation du système. Ce réseau devrait être conçu pour fonctionner indépendamment de l'environnement défaillant et être clairement documenté dans le PCA. Certains centres canadiens ont exploré ou testé des environnements ROIS isolés ou des VLAN comme solutions de secours potentielles. • Intégrer au PCA des mesures visant à assurer la continuité des communications, telles que des lignes téléphoniques dédiées ou une ligne d'assistance centralisée permettant aux patients et aux prestataires référents d'obtenir des informations en temps réel sur les interruptions de service. Le plan doit également définir des voies de communication d'urgence pour faciliter le triage et le transfert aux échelons supérieurs pour les besoins urgents en cas d'interruption, y compris des solutions de secours, telles que le télécopieur, les lignes téléphoniques d'urgence ou les canaux de courriel sécurisés. • Prévoir un soutien proactif du personnel en cas de perturbations prolongées, en tenant compte de la pression opérationnelle et émotionnelle liée à des périodes d'interruptions prolongées. Le PCA doit définir des stratégies visant à favoriser le bien-être du personnel, telles que la rotation des tâches pour gérer la charge de travail, la tenue de comptes rendus d'équipe réguliers et la mise en place de tournées de la direction ou de bien-être afin d'apporter un soutien et de maintenir la conscience situationnelle au sein du personnel. • Veiller à ce que le PCA aborde également la gouvernance en matière de résilience du système et les processus de rétablissement, et qu'il	Organisationnelle + Technologique

	identifie clairement les équipes informatiques, de direction et de sécurité chargées de la surveillance et de la prise de décision.	
PP2.2	**Plan de communication** • Définir les processus de communication pour les employés, les patients, les fournisseurs, la direction et les parties prenantes externes. • Prévoir des moyens de communication de rechange (courriel privé, appareils mobiles, applications de messagerie sécurisées). • Identifier les personnes clés, le calendrier et les procédures de recours hiérarchique pour les notifications internes et externes, notamment les conseillers juridiques, les organismes chargés de l'application de la loi et les médias. • Créer des modèles de communication pouvant être complétés par les informations pertinentes et envoyés par courriel aux patients, aux médias, etc. • Élaborer des scénarios pour le personnel en contact direct avec les patients, y compris des réponses aux questions couramment posées. Le personnel doit se préparer à communiquer ces messages à l'aide de scénarios simulés.	Organisationnelle
PP2.3	**Compensation des interruptions de traitement** • Tenir à jour les directives, formules et outils radiobiologiques permettant de compenser les interruptions de traitement. • Fournir des documents standard et des outils de calcul pour guider les ajustements de dose.	Technologique
PP2.4	**Documentation écrite** • Créer des modèles papier pour les documents essentiels spécifiques à la radiothérapie, notamment les prescriptions de traitement, les listes de diagnostics, les schémas thérapeutiques, les notes de séance, les formulaires d'admission, les références d'imagerie et le suivi des progrès, etc. • Diffuser des guides pratiques concis et d'autres ressources afin de faciliter la documentation manuelle précise des processus essentiels de radiothérapie, garantissant ainsi la continuité des soins en cas d'interruption. • Accorder une attention particulière aux dossiers cliniques et administratifs liés à la radiothérapie.	Organisationnelle + Technologique
PP2.4.1	**Matériel et ressources** • Veiller à ce que tout le matériel et les équipements nécessaires à la continuité des activités soient disponibles, notamment des ordinateurs de secours, des clés USB, des télécopieurs, des lecteurs de DVD, des photocopieurs, des imprimantes, de l'encre en poudre, du papier, des stylos/crayons, des chemises, des annuaires téléphoniques, des protocoles, des listes de contrôle en cas d'interruption et un manuel pour les interruptions prolongées.	Organisationnelle + Technologique
PP2.5	**Traitement sans système de contrôle et d'enregistrement (R&V)**	Technologique

	• La prestation de radiothérapie sans système R&V est généralement peu sûre et n'est pas recommandée pour les traitements contemporains, sauf potentiellement dans des cas palliatifs très simples où les risques sont minimes. • Toute possibilité de traitement sans système R&V doit être abordée explicitement dans les plans d'urgence de la CCSN et doit inclure des mesures strictes d'assurance qualité (AQ), des protocoles de vérification rigoureux et une autorisation réglementaire. • L'accent doit rester principalement sur le maintien de l'accès aux systèmes R&V au moyen de redondances, de procédures en cas d'interruption de service et d'une assistance des fournisseurs, plutôt que de tenter d'administrer l'intégralité du traitement en leur absence.	
PP2.6	**Stratégie de sauvegarde complète** • Mettre en place des systèmes de sauvegarde automatisés et chiffrés pour toutes les infrastructures critiques. • Adopter le principe de sauvegarde 3-2-1-1-0 : conserver trois copies des données, sur deux supports différents, dont une hors site, une hors ligne/immuable, et zéro erreur lors de la vérification. • Veiller à ce que les procédures de sauvegarde planifiées incluent les fichiers de configuration, les données des patients, les calendriers de traitement et les journaux d'AQ, et qu'elles soient conformes aux réglementations provinciales et aux spécifications des fournisseurs.	Technologique
PP2.7	**Direction** • Définir les rôles et les responsabilités des cadres supérieurs en matière de prise de décision et de surveillance en cas d'interruption de service.	Organisationnelle
PP2.8	**Paiement d'une rançon en cas de cyberattaque** • Définir dans le PCA la manière dont les demandes de rançon seront gérées, y compris les protocoles de négociation et les critères de décision. **Remarque importante :** Il n'est pas recommandé de payer une rançon à la suite d'une cyberattaque pour plusieurs raisons, notamment l'absence de garantie quant à la récupération des données, le risque d'encourager de nouvelles attaques, les conséquences légales et réglementaires potentielles, les pertes financières et les coûts cachés, ainsi que les préoccupations liées à la confidentialité des données.	Organisationnelle + Axée sur l'humain
PP2.9	**Accords avec les hôpitaux environnants** • Tenir à jour des listes de contacts clés, sous forme électronique et sur papier, pour les centres de cancérologie environnants/partenaires, y compris les responsables administratifs et les autres membres du personnel essentiels. • Conclure des accords formels avec d'autres centres pour accueillir des patients en cas de panne et/ou redéployer le personnel entre les centres, lorsque cela est possible. Dans le cadre de ces accords, veiller à ce que la faisabilité du transfert de données et l'atténuation des risques liés aux dossiers incomplets soient prises en compte.	Organisationnelle + Axée sur l'humain

	• Définir et consigner, à l'avance, l'ensemble de données cliniques minimal requis pour le transfert et l'admission des patients dans les centres d'accueil. Cet ensemble de données doit être normalisé, dans la mesure du possible, entre les établissements partenaires et intégré au plan de continuité des activités (PCA), y compris sous forme électronique et sur papier, en vue d'une utilisation en cas d'interruption prolongée.	
PP2.10	**Triage des patients** • Définir les critères de priorisation des patients pour le traitement en cas d'interruption de service, en faisant la distinction entre les nouveaux cas et les cas en cours et en déterminant les déclencheurs d'orientation.	Organisationnelle + Axée sur l'humain
PP2.11	**Simulations et exercices du PCA** • Définir les calendriers et les méthodes pour les tests du PCA (exercices sur table, fonctionnels, à grande échelle) et mettre à jour les plans en fonction des enseignements tirés.	Organisationnelle
PP2.12	**Implication des fournisseurs** • Sur la base d'une approche locale, préciser la distinction entre les rôles du fournisseur de systèmes et du service informatique local lors d'une interruption de service, des sauvegardes et de la restauration du service. • Définir clairement les rôles du fournisseur en matière d'assistance, notamment en ce qui concerne la sécurité des technologies de l'information, les délais de sauvegarde et de restauration, ainsi que les vérifications et modifications à effectuer par le fournisseur une fois le service rétabli. • Clarifier à l'avance les exigences des fournisseurs.	Organisationnelle
PP2.13	**Coopération et harmonisation** • Conformément au PCA de l'hôpital, veiller à ce que le PCA du service de radiothérapie s'intègre au PCA global et à la stratégie de sécurité de l'hôpital, en collaboration avec la direction et les équipes informatiques.	Organisationnelle
PP2.14	**Experts externes** • Définir les procédures à suivre pour faire appel à des spécialistes externes (consultants en cybersécurité, experts en criminalistique numérique, prestataires de services de rétablissement après sinistre) lorsque les ressources internes sont insuffisantes. • Identifier les organismes chargés de l'application de la loi concernés et établir à l'avance les points de contact appropriés (par exemple, les services de police locaux, les unités de lutte contre la cybercriminalité). La définition proactive de ces relations favorise une notification rapide, une intervention coordonnée et l'accès à une expertise ou à une intervention en matière de sécurité lorsqu'elles sont nécessaires.	Organisationnelle
PP3 — Rôles et responsabilités précis/équipe d'intervention en cas d'incident (EII)		

PP3.1	**Équipe d'intervention en cas d'incident (EII)** • Mettre en place une équipe multidisciplinaire d'intervention en cas d'incident, composée de représentants de tous les domaines concernés du programme de radiothérapie, notamment des radio-oncologues, des physiciens médicaux, des radiothérapeutes, du personnel infirmier, du personnel administratif, du service informatique et des services de technologie médicale. • Veiller à ce que l'équipe soit formée pour intervenir en cas d'incidents liés à la cybersécurité ou à des interruptions des activités.	Organisationnelle + Axée sur l'humain
PP3.2	**Rôles et responsabilités** • Utiliser un cadre de gouvernance pour définir clairement et attribuer les responsabilités, les pouvoirs et l'obligation de rendre compte à chaque membre de l'équipe d'intervention en cas d'incident. • Tenir compte du fait que les rôles, les responsabilités et les activités lors des interruptions de service peuvent différer des activités normales et doivent être adaptés aux conditions et aux ressources locales.	Organisationnelle + Axée sur l'humain
PP3.3	**Personnel clé** • Identifier les membres clés du personnel au sein du service de radiothérapie et du service informatique qui possèdent la formation, l'autorité et la responsabilité officielle nécessaires pour coordonner les mesures d'intervention. • Définir des procédures avec l'équipe de sécurité des technologies de l'information ou le dirigeant principal de la sécurité de l'information afin de garantir un transfert de connaissances, une continuité et une communication efficaces en cas d'incident. • Privilégier la définition formelle des rôles, des responsabilités et des procédures de recours hiérarchique plutôt que de se fier à la conscience situationnelle individuelle, qui peut varier lors d'événements particulièrement stressants.	Organisationnelle + Axée sur l'humain
PP3.4	**Partenaires externes en sécurité des technologies de l'information** • Les services de radiothérapie peuvent collaborer avec les équipes informatiques et de cybersécurité de l'hôpital ou des autorités sanitaires afin d'assurer un recours hiérarchique et une coordination rapides en cas d'incidents touchant les systèmes de RT. • Établir des procédures claires pour la communication et le partage d'informations avec ces équipes, y compris les détails à fournir et les personnes à contacter.	Organisationnelle
PP4 — Connaissance des exigences légales et réglementaires		
PP4.1	**Connaissance des cadres reconnus** • Les programmes de radiothérapie et les responsables informatiques ou opérationnels des hôpitaux concernés doivent connaître les cadres de cybersécurité et de continuité des activités reconnus à l'échelle internationale et applicables au secteur de la santé, tels que le CSF du NIST, la norme ISO 27001, les directives de cybersécurité de HIMSS, les Contrôles du Center for Internet Security (CIS) et le CSF de HITRUST.	Organisationnelle

PP4.2	**Connaissance des aspects légaux** • La direction des programmes de radiothérapie, en collaboration avec le service chargé de la protection de la vie privée, le service juridique et le service informatique de l'hôpital, doit veiller à ce que les politiques opérationnelles, de cybersécurité et de préparation aux situations d'urgence respectent les lois canadiennes applicables en matière de protection de la vie privée et des données de santé (par exemple, la LPRPS, lois provinciales équivalentes, la LPRPDE), y compris les exigences obligatoires en matière de déclaration des violations et des incidents. • Les procédures opérationnelles doivent intégrer les exigences de la CCSN en matière de sûreté radiologique, de protection physique des sources scellées et les considérations de cybersécurité associées, en particulier pour les sources de haute activité utilisées en curiethérapie à HDD, par scalpel gamma et en téléthérapie au cobalt. • Les plans d'intervention en cas d'incident doivent prévoir des procédures claires pour assurer une notification réglementaire en temps opportun lors d'événements liés à la sécurité, de compromissions de système ou de violations concernant la sécurité des sources scellées.	Organisationnelle
PP4.3	**Accès à des experts en cybersécurité** • Veiller à ce que le programme de radiothérapie dispose d'un accès continu à une expertise en matière de gouvernance de la cybersécurité, telle qu'un dirigeant principal de la sécurité de l'information ou une fonction équivalente au niveau de l'hôpital. • Établir des voies de consultation formelles permettant aux responsables cliniques de consulter des experts en cybersécurité et en continuité des activités lors de la planification, des tests ou de la mise à jour du PCA. • Consigner les procédures de renvoi vers des spécialistes externes lorsque l'expertise interne est insuffisante (voir les sections PP2.14 Experts externes, PP3.3 Personnel clé et PP3.4 Partenaires externes en sécurité des technologies de l'information).	Organisationnelle
PP4.4	**Agrément/Certification** • Le programme de radiothérapie doit collaborer avec le service informatique de l'hôpital et les fournisseurs concernés afin de s'assurer de leur conformité aux normes de sécurité des technologies de l'information reconnues, telles que la norme ISO/IEC 27001. • Dans la mesure du possible, intégrer les conclusions des audits informatiques externes et des certifications des fournisseurs dans la planification des interruptions des activités de radiothérapie et de la cybersécurité. • Tenir compte du statut d'agrément et de certification lors de la sélection des fournisseurs ou des discussions sur leur implication, en collaboration avec les équipes d'approvisionnement et de l'informatique (voir la section PP2.12 Implication des fournisseurs).	Organisationnelle + Technologique

5.2. Domaine de la prévention

La prévention désigne un ensemble complet de mesures de protection proactives conçues pour réduire les vulnérabilités, renforcer les défenses du système et minimiser la probabilité et les répercussions des interruptions de service dans les activités de radiothérapie. Ces perturbations peuvent résulter d'incidents de cybersécurité, de défaillances d'infrastructure, de pannes chez les fournisseurs ou de risques environnementaux. Le domaine de la prévention met l'accent sur la mise en œuvre de contrôles techniques, organisationnels et procéduraux à différents échelons, à la fois dans les systèmes informatiques spécifiques à la radiothérapie et dans ceux de l'entreprise. Les principales stratégies consistent notamment à sensibiliser au sujet de la cybersécurité, à dispenser des formations adaptées aux différents rôles, à mettre en place une gestion rigoureuse des accès et des identités des utilisateurs, à l'application rapide des correctifs système, à maintenir la protection des terminaux et à segmenter les réseaux afin de contenir les menaces potentielles. Il intègre également des protocoles de chiffrement, des processus sécurisés de stockage et d'archivage des données, des contrôles d'accès physiques et à distance, ainsi que des systèmes de sauvegarde robustes, tels que des stratégies de stockage hors site immuables, isolées ou hors réseau, comme l'infonuagique. Afin de garantir la résilience, ces mesures sont renforcées par des tests réguliers des flux de travail d'urgence, y compris des simulations d'interruption de service et des procédures de restauration.

N°	**Mesure d'action**	Catégorie
PR0 — Prévention générale		
PR0.1	**Comprendre le mécanisme des perturbations du système** • Acquérir une compréhension pratique de la manière dont les défaillances techniques, informatiques et matérielles se répercutent sur les systèmes de radiothérapie et les flux de travail, afin de cartographier les dépendances entre les applications cliniques, les systèmes de planification de traitement, les systèmes d'information en oncologie, les plateformes d'imagerie, les services réseau et les interfaces externes, dans le but d'identifier les points de défaillance uniques. • Reconnaître comment les perturbations, qu'elles soient malveillantes (par exemple, le chiffrement par rançongiciel, les activités par déni de service) ou non malveillantes (par exemple, des erreurs de configuration, des mises à jour échouées, la dégradation du matériel), peuvent nuire au bon fonctionnement, réduire les performances ou compromettre l'intégrité des données. • Comprendre en quoi les dégradations partielles du système (par exemple, latence, disponibilité limitée des fonctionnalités)	Axée sur l'humain

	diffèrent sur le plan opérationnel des pannes complètes et peuvent nécessiter des stratégies d'atténuation distinctes.	
PR0.2	**Gouvernance** • Mettre en place une structure de gouvernance formelle chargée de surveiller toutes les mesures préventives liées à la résilience du système. Cette structure doit définir des responsabilités claires entre le personnel informatique de l'hôpital ou du système de santé et celui du service de radiothérapie, notamment en ce qui concerne l'application de correctifs, les contrôles d'accès des utilisateurs, les mises à jour logicielles, la formation du personnel et la vérification des sauvegardes. La gouvernance en matière de prévention doit être revue périodiquement et s'appuyer sur les obligations légales ainsi que sur les stratégies organisationnelles de cybersécurité. La direction doit également favoriser une culture clinique où les mesures préventives sont prioritaires, même dans des conditions de charge de travail élevée**.**	Organisationnelle
PR0.3	**Contrôle de la sécurité et coordination des interventions** • Mettre en place ou s'associer à une structure officielle chargée des opérations de sécurité, telle qu'un dirigeant principal de la sécurité de l'information (DPSI), un centre des opérations de sécurité (SOC) ou un service informatique hospitalier disposant de protocoles de recours hiérarchique bien définis en matière de cybersécurité. Pour les centres de plus petite taille ou ceux ne disposant pas d'analystes en cybersécurité en interne, il convient de nommer une personne chargée de la liaison afin d'assurer la coordination avec le soutien informatique externe et les équipes provinciales d'intervention en cas de cyberincident. Cela garantit une visibilité en temps réel des menaces et une intervention unifiée lorsque des risques d'interruption surviennent.	Organisationnelle + Axée sur l'humain
PR0.4	**Soutien externe et mécanismes de transfert des risques** • Définir à l'avance les processus et les accords contractuels nécessaires pour faire appel à une expertise externe en cas de perturbations majeures, notamment des sociétés de cybersécurité, des prestataires de services de rétablissement après sinistre, des conseillers juridiques et des spécialistes en criminalistique numérique. • Veiller à ce que les accords sur les niveaux de service (ANS) conclus avec les fournisseurs de technologies critiques (par exemple, les systèmes de planification de traitement, les systèmes de contrôle et d'enregistrement, les systèmes d'information en oncologie, les fournisseurs de DME) définissent clairement les responsabilités, les délais d'intervention, les procédures de recours hiérarchique et l'assistance au rétablissement en cas d'incidents de cybersécurité ou de pannes prolongées.	Organisationnelle + Axée sur l'humain

	• Préciser les rôles et les responsabilités entre le service de radiothérapie (RT), la direction de l'hôpital et les services informatiques de l'hôpital ou régionaux. Dans la plupart des cas, la gestion des incidents de cybersécurité, la restauration des infrastructures et la collaboration avec les prestataires externes seront dirigées par le service informatique de l'hôpital ou les autorités régionales, tandis que le service de RT sera responsable de définir les exigences cliniques, les procédures d'urgence pour les flux de travail et les priorités en matière de sécurité des patients pendant le rétablissement. Les responsabilités doivent être consignées afin d'éviter toute ambiguïté en cas d'incident. • Le cas échéant, et, selon ce qui est déterminé à l'échelle de l'organisme, envisager des mécanismes de transfert des risques financiers (par exemple, une cyberassurance) afin d'atténuer les coûts de rétablissement et de soutenir la continuité des opérations. Les décisions concernant la souscription d'une assurance et l'étendue de la couverture relèvent généralement de la direction de l'hôpital ou du système de santé plutôt que des programmes de RT individuels. • Reconnaître que la structure et la mise en œuvre de ces mécanismes dépendront des modèles de gouvernance locaux, des capacités internes et du fait que les fonctions informatiques et de cybersécurité soient gérées à l'échelle de l'hôpital, de la région ou de la province.	
PR1 — Sensibilisation et formation		
PR1.1	**Culture de sensibilisation à la cybersécurité et aux interruptions** • Établir et maintenir une culture de cybersécurité et de préparation aux interruptions de service parmi l'ensemble du personnel, y compris le personnel clinique, informatique et administratif. • Mettre en place des programmes réguliers de formation du personnel visant à renforcer la sensibilisation et la préparation à tous les types de scénarios d'interruption de service, y compris les incidents de cybersécurité, les pannes des DME et les perturbations de l'infrastructure. • La formation doit inclure des volets pratiques, tels que la sensibilisation à l'hameçonnage, les pratiques numériques sécurisées, les procédures de flux de travail hors ligne, ainsi que la familiarisation avec les plans de continuité des activités (PCA) locaux et les procédures de recours hiérarchique. • Renforcer la sensibilisation par la diffusion régulière d'alertes internes, des enseignements tirés des incidents passés (cyber ou non) ayant entraîné des interruptions de service, ainsi que	Organisationnelle + Axée sur l'humain

	par des messages à l'échelle de l'organisme précisant les rôles et responsabilités de chacun en cas de panne. • Intégrer ces efforts aux programmes institutionnels existants en matière de qualité, de sécurité et de gestion des risques afin d'assurer une surveillance, une responsabilisation et une amélioration continues.	
PR1.2	**Programmes de formation spécifiques aux rôles** • Mettre en place une formation structurée et adaptée aux rôles des différents groupes professionnels (par exemple, les radiothérapeutes, les radio-oncologues, les physiciens médicaux, le personnel administratif) sur les bonnes pratiques en matière de cybersécurité, les procédures de déclaration des incidents et les procédures à suivre en cas d'interruption de service, en fonction de leurs responsabilités. • Veiller à ce que la formation soit dispensée lors de l'intégration et, par la suite, au moins une fois par an, avec des mises à jour tenant compte de l'évolution des menaces, des technologies et des exigences réglementaires. • Fournir des instructions sur les obligations légales et réglementaires applicables (par exemple, la LPRPS, la LPRPDE, les lois provinciales équivalentes), ainsi que des attentes claires concernant la documentation, la communication et les procédures de rétablissement en cas d'incident. • Mettre l'accent sur le renforcement des connaissances individuelles, de la sensibilisation et de la précision des rôles afin de garantir que le personnel comprenne *quoi faire* et *qui prévenir* en cas de perturbation.	Organisationnelle
PR1.3	**Simulations d'hameçonnage et exercices d'ingénierie sociale** • Les programmes de radiothérapie doivent coordonner leurs efforts avec le service informatique de l'hôpital afin de s'assurer que le personnel participe à des simulations périodiques d'hameçonnage et à des initiatives de sensibilisation à l'ingénierie sociale. • Privilégier la compréhension des principaux enseignements et des procédures de recours hiérarchique plutôt que le suivi des performances au fil du temps au sein du programme de radiothérapie lui-même. • Mettre l'accent sur la sensibilisation aux communications suspectes et aux procédures de déclaration appropriées afin de maintenir une bonne hygiène en matière de cybersécurité.	Organisationnelle + Axée sur l'humain
PR1.4	**Sensibilisation des fournisseurs et des fabricants** • Intégrer les exigences en matière de cybersécurité dans les processus d'approvisionnement auprès des fournisseurs et d'évaluation des contrats. Les centres de radiothérapie doivent s'assurer que les fournisseurs disposent de certifications en matière de cybersécurité (par exemple, ISO 27001), d'un service d'intervention adéquat en cas d'incident et de	Technologique

	configurations par défaut sécurisées pour les dispositifs et logiciels médicaux. Ces éléments sont particulièrement essentiels pour les plateformes de TPS et de R&V en nuage.	
PR2 — Application des correctifs système		
PR2.1	**Mises à jour des correctifs** • Veiller à ce que les systèmes essentiels à la prestation des services de radiothérapie soient régulièrement mis à jour à l'aide de correctifs de sécurité et de mises à jour système. • Les calendriers d'application des correctifs doivent être coordonnés entre le service informatique de l'établissement et le programme de radiothérapie, en tenant compte des activités cliniques et de la sécurité des patients. • Étant donné que de nombreuses applications critiques en radio-oncologie (par exemple, les systèmes de planification de traitement, les systèmes de contrôle et d'enregistrement, les consoles de radiothérapie) sont des dispositifs médicaux réglementés et sensibles à leur environnement logiciel, tous les correctifs, mises à niveau du système d'exploitation et modifications de configuration doivent être examinés en consultation avec le fournisseur afin de confirmer la compatibilité, la validité des configurations et la conformité réglementaire. • Les déploiements de correctifs doivent être consignés, validés et testés afin de garantir le bon fonctionnement continu des logiciels cliniques avant leur application à grande échelle.	Technologique
PR2.2	**Procédure de mise à jour** • Mettre en place et consigner une procédure de gouvernance formelle pour la gestion des mises à jour du système et des correctifs de sécurité. Cette procédure doit définir les circuits d'approbation, les processus d'évaluation des risques, les critères d'établissement des priorités (y compris la gestion des vulnérabilités urgentes ou du jour zéro), les exigences en matière de gestion du changement et les normes de documentation. • Définir clairement les responsabilités en matière de prise de décision et de surveillance, en précisant quelles tâches relèvent du service informatique de l'établissement, des équipes de cybersécurité de l'hôpital et de la direction du programme de radiothérapie (RT). Cela implique notamment de préciser qui est autorisé à reporter, à accélérer ou à déployer progressivement les mises à jour en fonction du risque clinique, des recommandations du fournisseur et de leur incidence sur les opérations. • Exiger une consultation et une validation écrites du fournisseur pour toute mise à jour touchant les logiciels ou systèmes de dispositifs médicaux réglementés qui fonctionnent dans des configurations prises en charge par le fournisseur.	Organisationnelle

	• Définir des protocoles de communication et de notification afin de garantir que les parties prenantes cliniques et techniques concernées soient informées des mises à jour prévues et averties sans délai des mesures correctives urgentes. • Intégrer des exigences en matière de traçabilité, notamment l'examen périodique des performances de la gestion des correctifs, le suivi des exceptions, les avis des fournisseurs et la documentation des décisions fondées sur les risques.	
PR2.3	**Contrôle des modifications** • Mettre en œuvre des politiques strictes de contrôle des modifications pour tous les systèmes de radiothérapie. Toute modification apportée à un système, que ce soit un correctif, un changement de configuration ou une mise à jour, doit suivre un processus structuré comprenant des étapes de test, d'approbation et de validation, ainsi que la documentation des opérations effectuées. • Veiller à la conformité continue avec les spécifications des fournisseurs et les normes de sécurité, et mettre hors service les systèmes obsolètes ou non pris en charge qui présentent des risques pour la continuité des opérations ou la sécurité des patients.	Organisationnelle
PR3 — Protection des terminaux (logiciels antivirus)		
PR3.1	**Logiciels de protection** • Veiller à ce que les terminaux utilisés dans l'environnement de radiothérapie, notamment les postes de travail cliniques, les consoles de traitement et les appareils mobiles, soient protégés par des mesures de sécurité appropriées (par exemple, antivirus, anti-maliciel, solution de détection et d'intervention sur les terminaux [EDR] et filtrage Web), en coordination avec le service informatique de l'hôpital. • Tenir compte du fait que les systèmes à usage général couramment utilisés au sein des services de radiothérapie (par exemple, l'accès aux courriels, les postes de travail de bureau et les périphériques réseau partagés) peuvent présenter une exposition plus importante aux cybermenaces que les équipements de traitement spécialisés et doivent donc être inclus dans les stratégies de protection. • Veiller à ce que les solutions de protection déployées sur les dispositifs médicaux réglementés ou les systèmes gérés par les fournisseurs soient approuvées par les fournisseurs respectifs et compatibles avec les configurations de système prises en charge. • Tout déploiement ou modification de la configuration des logiciels de protection sur les dispositifs médicaux réglementés doit se faire en consultation et avec l'accord des fournisseurs de systèmes, afin d'éviter toute interférence	Technologique

	involontaire avec les performances cliniques ou la conformité réglementaire. • Dans la mesure du possible, surveiller l'utilisation des privilèges administratifs et veiller à ce que tout comportement inhabituel soit signalé aux équipes informatiques ou de sécurité de l'hôpital pour examen.	
PR3.2	**Mises à jour régulières** • Tous les logiciels de protection doivent être mis à jour régulièrement afin de se défendre contre l'évolution des menaces et de minimiser le risque de corruption ou de défaillance du système. • Les mises à jour doivent être gérées de manière centralisée, selon un modèle d'abonnement, et inclure des alertes automatisées pour les terminaux obsolètes ou non conformes.	Technologique
PR3.3	**Protection des dispositifs et systèmes médicaux** • Mettre en œuvre et maintenir les mesures de cybersécurité pour les dispositifs médicaux utilisés en radio-oncologie uniquement en étroite collaboration avec le fournisseur du système et avec son accord explicite, afin de garantir le bon fonctionnement continu, la validité des configurations et la conformité réglementaire. • Tenir compte du fait que de nombreux systèmes de radiothérapie (par exemple, les consoles d'accélérateurs linéaires, les systèmes d'imagerie, les plateformes de planification de traitement et de contrôle et d'enregistrement) sont des dispositifs médicaux réglementés qui fonctionnent dans des environnements logiciels étroitement contrôlés. Tout contrôle de sécurité, toute modification de configuration, toute mise à jour du système d'exploitation ou tout déploiement de logiciel de protection doit donc être examiné et vérifié avec le fournisseur. • Assurer une séparation adéquate entre la gestion générale des actifs informatiques et les systèmes cliniques de radio-oncologie, tout en garantissant une surveillance coordonnée entre le service informatique de l'hôpital, les équipes de cybersécurité et le programme de radiothérapie. • S'assurer que les logiciels de sécurité et les terminaux ne nuisent pas aux performances du système, aux contrôles de sécurité ou à la conformité réglementaire. Lorsque le fournisseur le permet, segmenter ces appareils au sein du réseau afin d'isoler davantage les risques et de limiter la propagation latérale des menaces.	Organisationnelle + Technologique
PR4 — Architecture de réseau		
PR4.1	**Pare-feu** • Veiller à ce que des pare-feu de niveau d'entreprise soient déployés et gérés de manière centralisée afin d'assurer un	Technologique

	contrôle strict du trafic entre les systèmes de radiothérapie et les réseaux externes ou non cliniques. • Configurer les règles de pare-feu selon le principe du moindre privilège, en permettant uniquement les communications entrantes et sortantes explicitement autorisées et nécessaires aux activités cliniques (par exemple, les connexions d'assistance des fournisseurs, les interfaces système approuvées). • Passer régulièrement en revue et consigner les règles de pare-feu afin de supprimer les ports ouverts inutiles ou les voies d'accès anciennes susceptibles d'accroître l'exposition aux risques. • S'assurer que les configurations de pare-feu sont coordonnées avec les équipes informatiques et de cybersécurité de l'hôpital et qu'elles s'alignent sur l'architecture de sécurité globale de l'établissement.	
PR4.2	**Segmentation de réseau** • Concevoir une architecture réseau visant à réduire l'exposition des systèmes de radiothérapie aux réseaux hospitaliers ou publics plus larges, en recourant à des stratégies de segmentation adaptées à l'infrastructure locale et au modèle de gouvernance. • Dans la mesure du possible, isoler logiquement les systèmes clés (par exemple, les LINAC, les serveurs d'imagerie, les systèmes de planification de traitement, les plateformes de contrôle et d'enregistrement) à l'aide de VLAN, de sous-réseaux ou de contrôles équivalents. Tenir compte du fait que le degré et la structure de la segmentation dépendront de l'architecture du réseau local et des contraintes informatiques de l'établissement. • Envisager la mise en œuvre d'une micro-segmentation au sein de l'environnement de radiothérapie afin de limiter davantage les mouvements latéraux entre les systèmes ou les composants fonctionnels. Cette approche, qui est de plus en plus considérée comme à l'avant-garde, permet un contrôle et un confinement plus précis du trafic. • Les stratégies de segmentation doivent favoriser le confinement des logiciels malveillants, limiter la propagation interne des menaces et permettre une restauration prioritaire du système en cas d'interruption prolongée. • La conception et la mise en œuvre de la segmentation doivent être coordonnées avec les équipes informatiques et de cybersécurité de l'établissement et vérifiées auprès des fournisseurs lorsque des dispositifs médicaux réglementés sont concernés.	Technologique
PR5 — Gestion des utilisateurs et des accès		
PR5.1	**Contrôle d'accès basé sur les rôles (RBAC)**	Organisationnelle

	• Définir et appliquer des privilèges d'accès en fonction des rôles cliniques et opérationnels (par exemple, radio-oncologue, physicien médical, thérapeute, administrateur informatique, etc.) • Appliquer le principe du moindre privilège afin de limiter l'accès aux seuls systèmes et ensembles de données essentiels aux fonctions spécifiques à chaque rôle. • Les politiques RBAC doivent prendre en charge les flux de travail de secours sécurisés en cas d'interruption de service, afin de garantir que les utilisateurs critiques conservent l'accès aux systèmes essentiels ou aux outils hors ligne.	
PR5.2	**Application des politiques relatives aux mots de passe** • Mettre en place des politiques de mot de passe rigoureuses comprenant des exigences en matière de longueur minimale, de complexité et de cycles d'expiration. • Configurer des protocoles de temporisation de connexion et de verrouillage automatique pour les terminaux non surveillés dans les salles de traitement et les postes de planification. • S'assurer que les options de réinitialisation des mots de passe restent opérationnelles en cas d'interruption du système ou d'isolation du réseau (par exemple, protocoles hors ligne du service d'assistance informatique).	Technologique
PR5.3	**Authentification à facteurs multiples (AFM)** • La mise en œuvre et la gouvernance de l'AFM sont généralement gérées par le service informatique de l'hôpital ou de l'autorité sanitaire et ne relèvent pas directement du champ d'action du programme de radiothérapie. • Les services de radiothérapie doivent travailler en collaboration avec les équipes informatiques de l'hôpital afin de comprendre comment l'AFM est appliquée aux systèmes couramment utilisés dans les flux de travail de radiothérapie, en particulier pour l'accès à distance ou les comptes à privilèges élevés. • Lorsque les politiques d'AFM ont une incidence sur les activités cliniques (par exemple, l'accès aux systèmes R&V, aux archives d'imagerie ou à d'autres systèmes critiques), le personnel de radiothérapie doit connaître les marches à suivre et les procédures de recours hiérarchique applicables, y compris les processus d'urgence approuvés en cas de panne du réseau.	Technologique
PR5.4	**Enregistrement et surveillance des accès** • Mettre en place l'enregistrement et la surveillance en temps réel des activités des utilisateurs, en particulier pour les comptes à privilèges élevés (par exemple, les administrateurs de domaine, les administrateurs PACS). • Mettre en place des systèmes d'alerte signalant tout comportement de connexion anormal ou tout accès à des	Organisationnelle + Technologique

	ensembles de données sensibles en dehors des flux de travail standard. • S'assurer que les journaux sont conservés et sauvegardés de manière sécurisée, en prévoyant des procédures de vérification manuelle des journaux si les systèmes GIES ne sont pas disponibles lors d'une interruption de service.	
PR6 — Protection des données		
PR6.1	**Chiffrement des données** • Le chiffrement des données liées à la radiothérapie, en transit ou inactives, est généralement mis en œuvre au moyen de l'infrastructure de technologie de l'information de l'hôpital et des configurations de système prises en charge par les fournisseurs. • Les programmes de radiothérapie doivent collaborer avec les services informatiques de l'hôpital et les fournisseurs de systèmes afin de déterminer quelles capacités de chiffrement sont prises en charge par les systèmes cliniques (par exemple, les systèmes de planification de traitement, les systèmes d'information en oncologie, les plateformes d'imagerie) et comment ces mesures de protection sont mises en œuvre dans la pratique. • Veiller à ce que les méthodes de chiffrement utilisées pour les données cliniques critiques restent compatibles avec les configurations prises en charge par les fournisseurs et les exigences réglementaires. • Lors de la planification des interruptions de service ou du rétablissement du système, tenir compte de la manière dont les contrôles de chiffrement peuvent affecter l'accès aux données, leur récupération et leur interopérabilité en cas d'urgence, et coordonner vos efforts avec le service informatique et les fournisseurs afin d'assurer la continuité des soins.	Technologique
PR6.2	**Stockage et conservation des données** • Établir et consigner des calendriers de conservation pour les ensembles de données liés aux traitements, conformément aux lois provinciales sur la protection des renseignements liés à la santé et aux politiques de l'établissement. • Veiller à ce que les données critiques soient stockées de manière redondante sur différents systèmes (par exemple, serveurs de planification de traitement, archives indépendantes des fournisseurs) et à ce que des voies d'accès de secours soient définies afin d'assurer la continuité en cas de panne du réseau, d'interruption des services des fournisseurs ou de défaillance matérielle. • Élaborer une stratégie de récupération des données claire et concrète, en collaboration avec le service informatique de l'établissement et les fournisseurs concernés, en précisant	Technologique

	comment les données peuvent être restaurées rapidement et en toute sécurité dans différents scénarios de perturbation. • Effectuer régulièrement des tests des procédures de sauvegarde et de restauration afin de vérifier l'accessibilité, la compatibilité des systèmes et les délais de rétablissement, en s'assurant que le rétablissement est possible, même lorsque les réseaux principaux sont hors service. • Consigner toutes les activités de sauvegarde, de restauration et de test afin de garantir la préparation opérationnelle, la traçabilité et l'amélioration continue.	
PR6.3	**Politique relative aux dispositifs de stockage portables** • Élaborer un protocole normalisé pour la gestion des dispositifs de stockage portables (par exemple, clés USB, disques durs externes) utilisés pour l'importation/l'exportation des données des patients, y compris les procédures d'analyse antivirus et les processus de validation. • Limiter l'utilisation à des terminaux prédéfinis et surveillés, et restreindre l'accès aux systèmes cliniques aux dispositifs autorisés. • En cas d'urgence, l'utilisation autorisée de clés USB chiffrées peut faciliter le transfert hors ligne des patients ou la poursuite manuelle des traitements.	Technologique + Axée sur l'humain
PR6.4	**Systèmes sécurisés d'archivage et de récupération** • Mettre en place des archives pour les données cliniques et opérationnelles critiques, avec le balisage des métadonnées et des fonctionnalités de recherche. • S'assurer que les processus de récupération fonctionnent avec les formats numériques et non numériques, afin de permettre aux équipes de radiothérapie de retrouver les informations essentielles même en cas de pannes prolongées. • Les protocoles d'accès aux archives hors ligne (par exemple, les horaires imprimés, les disques miroirs) doivent être testés et consignés.	Technologique
PR7 — Restrictions d'accès physique et à distance		
PR7.1	**Architecture d'accès à distance sécurisé** • Veiller à ce que tous les accès à distance aux systèmes de radiothérapie passent par des RPV sécurisés ou des tunnels chiffrés avec vérification des terminaux et enregistrement des accès. • L'accès aux systèmes critiques doit être lié au rôle de l'utilisateur et limité dans le temps, en particulier lors de situations d'urgence ou de séances d'assistance technique par les fournisseurs. • Les flux de travail à distance pour la planification hors site ou la collaboration entre centres doivent respecter les réglementations provinciales en matière de protection de la vie privée (par exemple, la LPRPS, la LPRPDE) et inclure des	Technologique + Organisationnelle

	protocoles d'accès d'urgence sans compromettre l'intégrité du système.	
PR7.2	**Politique d'accès** • Mettre en œuvre des politiques formalisées régissant l'accès des tiers, notamment des fournisseurs de logiciels, des prestataires informatiques et des cliniciens affiliés. • Tout accès externe doit être préalablement approuvé, consigné et soumis à une surveillance en temps réel. • Les accords sur les niveaux de service (ANS) d'urgence doivent définir des procédures d'assistance à distance en cas de pannes prolongées, y compris des procédures de gestion des identifiants de secours et des protocoles de recours hiérarchique en cas d'interruption de service.	Organisationnelle + Technologique
PR7.3	**Accès physique** • Limiter l'accès physique aux équipements sensibles et aux postes de travail grâce à l'authentification par badge ou à des zones cliniques verrouillées. • Veiller à ce que les serveurs, les systèmes R&V et le matériel réseau soient hébergés dans des salles sécurisées dotées de contrôles environnementaux et d'un système de surveillance. • Mettre en place des protocoles permettant le verrouillage rapide des espaces physiques en cas d'incidents de cybersécurité, de catastrophes naturelles ou d'autres situations d'urgence. • Pendant les interruptions de service, sécuriser l'accès aux sauvegardes imprimées, aux postes de travail hors ligne et aux dispositifs USB utilisés pour la prestation manuelle des soins. • Procéder à des inspections régulières des zones cliniques et des salles de serveurs afin de vérifier que les équipements sont correctement entreposés, que les contrôles environnementaux fonctionnent et que les mesures de sécurité physique sont maintenues.	Organisationnelle + Axée sur l'humain + Technologique
PR8 — Sauvegardes et copies papier		
PR8.1	**Infrastructure réseau et serveur redondante** • Concevoir des serveurs de secours et/ou des environnements réseau local isolés capables de prendre temporairement en charge les opérations essentielles en cas de panne du système central ou des services infonuagiques. • Pour les systèmes hébergés dans le nuage, définir des mécanismes contractuels et techniques permettant un basculement rapide ou l'accès à un cache local en cas de perte de connectivité.	Technologique
PR8.2	**Copies hors ligne des données** • Identifier les données critiques en radiothérapie nécessaires pour assurer la continuité des soins en cas de pannes prolongées du système (par exemple, les horaires des patients, leurs coordonnées, les prescriptions de traitement, les	Technologique

	références d'imagerie pertinentes et les paramètres clés de planification). • Les stratégies visant à maintenir l'accès à ces données doivent être élaborées en coordination avec les politiques informatiques et les exigences de sécurité de l'hôpital. Dans certains établissements, la conservation de données hors du réseau principal (par exemple, sur des clés USB ou des systèmes autonomes) peut ne pas être autorisée ; il convient alors d'envisager d'autres approches sécurisées. • Si des copies hors ligne ou isolées sont autorisées, veiller à ce qu'elles respectent les politiques de l'établissement en matière de sécurité et de chiffrement et qu'elles se limitent à l'ensemble minimal de données nécessaire pour permettre une prise de décision clinique en toute sécurité pendant les interruptions de service. • Définir clairement les procédures d'accès et d'utilisation de ces données lorsque les systèmes principaux ne sont pas disponibles, y compris la manière dont le personnel récupère et examine les informations en l'absence des interfaces électroniques habituelles (par exemple, en consultant les dossiers archivés ou la documentation imprimée lorsque les systèmes en réseau sont inaccessibles). • Le cas échéant, veiller à ce que l'ensemble minimal prédéfini de données de transfert nécessaire à une éventuelle réorientation du patient vers un autre centre soit maintenu et révisé périodiquement avec les parties prenantes concernées.	
PR8.3	**Résilience du stockage infonuagique** • Veiller à ce que les systèmes hébergés dans le nuage (par exemple, les ROIS ou les DME) disposent de plans d'urgence consignés pour les situations où l'accès à Internet est interrompu. Ces plans doivent traiter de l'accès local (par exemple, bases de données mises en cache, copies hors ligne), de la connectivité de secours (par exemple, 5G) et des options de secours prises en charge par les fournisseurs. Toutes les mesures doivent être conformes aux lois canadiennes sur la protection de la vie privée (par exemple, la LPRPS, la LPRPDE).	Organisationnelle + Technologique
PR8.4	**Copies papier** • Conserver des copies papier des informations critiques relatives au traitement, nécessaires à la continuité des soins en cas de panne du système. Il peut s'agir notamment de copies papier d'horaires, de schémas thérapeutiques, de détails sur le fractionnement et de coordonnées. Évaluer la possibilité de fournir aux patients des copies papier simplifiées ou résumées des informations pertinentes sur le traitement (par exemple, les calendriers de rendez-vous, les instructions de traitement) afin de garantir la continuité des soins pendant	Organisationnelle + Technologique

	les interruptions de service, tout en assurant le respect de la confidentialité et de la réglementation. • Passer régulièrement en revue les informations essentielles aux flux de travail manuels et veiller à ce que les copies imprimées soient mises à jour de manière régulière (quotidiennement, hebdomadairement ou selon les besoins).	
PR8.5	**Procédure de restauration et de validation des données** • Définir des procédures claires et détaillées pour la restauration des données de chaque système de radiothérapie critique, y compris l'ordre de restauration, les dépendances entre les systèmes et les points de contrôle de validation après le rétablissement. • Mettre en place des processus de validation formels afin de confirmer que les données restaurées sont complètes, cohérentes et correctement synchronisées avec les systèmes en ligne, et de prévenir toute duplication, corruption ou perte. • Planifier et mener des exercices de restauration de routine afin de vérifier que les procédures consignées sont efficaces et que le personnel est en mesure de les mettre en œuvre avec précision dans le cadre de scénarios simulant des interruptions de service. • Consigner toutes les activités de restauration, les résultats de validation et les enseignements tirés afin de garantir la traçabilité, l'amélioration continue et la préparation opérationnelle.	Technologique
PR9 — Test des plans de réaction, d'intervention et de rétablissement		
PR9.1	**Test du plan de continuité des activités** • Organiser des exercices sur table annuels ou semestriels simulant des scénarios d'interruption prolongée (par exemple, cyberattaque, panne du système DME, inondation). Ces exercices doivent inclure les responsables cliniques, les équipes informatiques et les partenaires régionaux. Les comptes rendus doivent servir de base aux mises à jour du PCA. • Prévoir des tests réguliers des procédures de rétablissement et mettre à jour les plans de rétablissement en conséquence.	Organisationnelle + Technologique
PR9.2	**Exercices de simulation d'interruption de service** • Organiser des exercices de simulation reproduisant des scénarios d'interruption de service réels, tels qu'une défaillance des systèmes informatiques, une panne de logiciels cliniques ou un incident de cybersécurité. • Faire participer des équipes interdisciplinaires (par exemple, des radiothérapeutes, des oncologues, des physiciens médicaux, le personnel informatique et administratif) afin de tester les procédures d'intervention, les protocoles de communication, les stratégies de continuité des soins aux	Organisationnelle

	patients et les processus de transfert des patients, y compris le transfert des données des patients, le cas échéant. • Dans la mesure du possible, utiliser des patients fictifs, de la documentation hors ligne et des systèmes de non-production pour simuler en toute sécurité les activités cliniques. • Réaliser des exercices sur table ou des exercices basse fidélité au moins une fois par an, et mener des simulations fonctionnelles à grande échelle tous les un à deux ans, ou plus fréquemment en cas de changements majeurs apportés au système, d'introduction de nouvelles technologies ou de changements de personnel. • Consigner les enseignements tirés de chaque exercice et mettre à jour les procédures en cas d'interruption de service en conséquence afin d'améliorer en permanence l'état de préparation.	
PR9.3	**Test des flux de travail analogiques** • Effectuer régulièrement des tests complets des processus de traitement à l'aide de dossiers papier et de protocoles hors ligne, dans un environnement contrôlé et simulé plutôt qu'avec de vrais patients, afin de vérifier que le personnel est en mesure de suivre les procédures en cas d'interruption de service en toute sécurité. • Veiller à ce que les simulations soient menées parallèlement aux processus habituels, en utilisant des patients fictifs ou des ensembles de données d'essai afin de ne pas compromettre la sécurité clinique ni la conformité réglementaire. • Mettre l'accent sur l'identification des éventuelles lacunes, erreurs humaines ou inefficacités des flux de travail susceptibles de se produire lors d'un incident réel, sans recourir à des flux de travail sur papier pour les soins réels aux patients lorsque des systèmes électroniques sûrs sont disponibles. • Consigner les enseignements tirés et mettre à jour les procédures en cas d'interruption de service afin de renforcer la préparation, de minimiser les risques et de soutenir la formation du personnel clinique.	Organisationnelle
PR9.4	**Audits** • Faire appel à des fournisseurs certifiés pour évaluer les vulnérabilités de l'infrastructure au moyen d'audits externes. Veiller à ce que les recommandations issues des audits soient suivies et intégrées dans les mises à jour du PCA.	Organisationnelle
PR9.5	**Tests de pénétration** • Les tests de pénétration des réseaux hospitaliers et des systèmes cliniques sont généralement menés à l'échelle de l'établissement ou de l'autorité sanitaire par les équipes informatiques ou de cybersécurité de l'hôpital et peuvent nécessiter une autorisation organisationnelle.	Technologique

	• Les programmes de radiothérapie peuvent communiquer avec ces équipes afin de déterminer si les systèmes liés à la radiothérapie sont inclus dans ces évaluations et d'identifier tout résultat pouvant avoir une incidence sur la continuité des soins ou la sécurité des patients. • Lorsque des résultats pertinents sont identifiés, la direction du programme de radiothérapie doit coordonner ses efforts avec le service informatique et les fournisseurs afin de comprendre les répercussions opérationnelles potentielles et de soutenir la planification de mesures d'atténuation appropriées.	

5.3. Domaine de la détection

Le domaine de la détection met l'accent sur l'identification précoce des menaces, des anomalies et des défaillances de l'infrastructure susceptibles de compromettre la prestation sûre et continue des services de radiothérapie. Dans le contexte pancanadien, ce domaine ne se limite pas aux cybermenaces, mais englobe également des sources plus larges d'interruption des systèmes, telles que les défaillances logicielles, les perturbations chez les fournisseurs ou les pannes d'infrastructure. Une surveillance proactive, la vigilance du personnel et des canaux de communication clairs sont essentiels pour une détection et un confinement précoces. Les centres canadiens ont fait état de différentes capacités à tirer parti d'outils, tels que les systèmes GIES (gestion des informations et des événements de sécurité), les systèmes de détection d'anomalies et les protocoles de recours hiérarchique internes. Le tableau suivant présente des mesures concrètes adaptées au contexte canadien, favorisant une détection en temps opportun, la visibilité des menaces et une évaluation rapide de la situation pour toutes les formes de perturbations numériques.

N°	**Mesure d'action**	Catégorie
DE1 — Détection en temps réel		
DE1.1	**Surveillance des réseaux** • Veiller à ce que des outils de surveillance, ainsi que des outils de détection et d'intervention en continu, soient utilisés sur tous les réseaux auxquels le service a accès.	Technologique
DE1.2	**Sensibilisation aux systèmes de surveillance** • Les programmes de radiothérapie doivent consigner les contacts informatiques ou de cybersécurité de l'établissement chargés de surveiller les systèmes de détection d'intrusion (IDS) et les systèmes de détection ou de surveillance des anomalies susceptibles d'avoir une incidence sur l'infrastructure de radiothérapie. • Définir des procédures de recours hiérarchique claires entre le service de radiothérapie et les équipes informatiques et de	Technologique

	sécurité de l'hôpital, en cas d'activité suspecte touchant les systèmes de radiothérapie. • Le cas échéant, veiller à ce que les systèmes ou réseaux spécifiques à la radiothérapie soient intégrés aux programmes de surveillance de l'établissement, en coordination avec le service informatique de l'hôpital et les fournisseurs.	
DE1.3	**Identification des activités suspectes** • Apprendre à identifier les activités suspectes qui peuvent indiquer une cyberattaque imminente. • Il s'agit notamment d'un ralentissement des performances du réseau, d'une augmentation du trafic réseau, de la réception de courriels provenant de sources frauduleuses connues, de modifications inattendues dans des fichiers clés sur des lecteurs réseau, d'une activité inhabituelle sur des comptes à privilèges élevés, de configurations de fichiers et de registres altérées, de grandes quantités de données compressées dans des zones inutilisées du système, de pièces jointes exécutables dans les courriels, de modifications inattendues de fichiers clés sur des disques reliés au réseau, de processus inconnus chiffrant des fichiers, ou d'une augmentation importante du trafic réseau sur des ports inattendus.	Technologique + Axée sur l'humain
DE1.4	**Disposer des outils de surveillance adéquats** • Veiller à ce que des outils de surveillance et de détection appropriés soient mis en place afin de maintenir une conscience situationnelle sur l'ensemble des systèmes de radiothérapie critiques. Cela inclut des outils d'analyse du trafic réseau, de surveillance des terminaux, d'enregistrement des événements et de détection des anomalies. • Les outils de surveillance doivent permettre l'identification précoce des perturbations du système, des incidents de cybersécurité ou des défaillances opérationnelles, afin de garantir une intervention et une atténuation rapides. • Sélectionner des outils compatibles avec l'environnement clinique et qui n'interfèrent pas avec la prestation des traitements ni avec les exigences de conformité réglementaire. • Intégrer les outils de surveillance dans la stratégie globale de détection et d'intervention en cas d'incident, en définissant clairement les rôles en matière de surveillance, de remontée d'alerte et de correction. • Passer régulièrement en revue et mettre à jour les outils, les configurations et les seuils d'alerte afin de s'adapter à l'évolution des menaces et aux changements dans l'environnement informatique et clinique.	Technologique
DE1.5	**Examen des systèmes de détection** • Les systèmes de détection sont généralement gérés et contrôlés par les équipes informatiques ou de cybersécurité de	Technologique

	l'hôpital afin de faire face à l'évolution des menaces, y compris les vulnérabilités du jour zéro. • Les programmes de radiothérapie doivent maintenir une communication avec les équipes informatiques et de sécurité de l'établissement afin de comprendre comment les mises à jour ou les modifications apportées aux systèmes de détection peuvent avoir une incidence sur l'infrastructure ou les flux de travail de la radiothérapie. • Veiller à ce que des procédures de recours hiérarchique claires soient en place afin que les menaces potentielles touchant les systèmes de radiothérapie puissent être rapidement signalées aux équipes informatiques et de sécurité concernées.	
DE1.6	**Test des systèmes de détection** • Veiller à ce que les systèmes de détection soient testés régulièrement au sein de votre organisme.	Technologique, Organisationnelle
DE1.7	**Centres des opérations de sécurité** • Les services de radiothérapie doivent pouvoir faire appel à des experts en cybersécurité ou à des centres des opérations de sécurité (SOC), que ce soit en interne ou dans le cadre d'accords avec des tiers, afin de faciliter la détection des menaces et de mettre en œuvre des protocoles d'intervention pendant ou en dehors des heures de bureau.	Organisationnelle
DE1.8	**Vigilance du personnel et signalement** • Promouvoir une culture de vigilance en encourageant le personnel à signaler tout comportement inhabituel des systèmes ou toute communication suspecte. • Mener des campagnes de sensibilisation visant à encourager le personnel à se considérer comme des « pare-feu humains » et intégrer des procédures de signalement dans les formations sur les interruptions de service.	Organisationnelle
DE1.9	**Retour d'information sur les incidents et apprentissage en boucle** • Veiller à ce que toutes les activités suspectes signalées, qu'elles donnent lieu ou non à des incidents réels, soient examinées et mises à profit pour en tirer des enseignements. Les enseignements tirés doivent être consignés et pris en compte dans les formations, la configuration de systèmes ou la mise à jour des politiques.	Organisationnelle
DE1.10	**Partage entre établissements des informations sur les menaces** • Renforcer les relations avec les agences provinciales du cancer, les hôpitaux partenaires et les organismes nationaux (par exemple, l'ISMP Canada pour le SNDAI-RT et le PCQR) afin de permettre un partage rapide des renseignements sur les menaces et des seuils de déclenchement en cas d'interruption de service. Utiliser les réseaux existants (pour les alertes et le partage de cas).	Organisationnelle

DE1.11	**Le rôle de l'intelligence artificielle (IA) dans la détection précoce des cyberattaques** • Reconnaître que l'IA est de plus en plus intégrée aux outils de cybersécurité pour faciliter la détection précoce et exhaustive des activités suspectes. • Les nouveaux algorithmes d'IA permettent d'analyser les tendances sur les réseaux, les terminaux et les applications afin d'identifier les anomalies ou les menaces potentielles plus rapidement que les systèmes traditionnels à base de règles. • Bien que les outils d'IA soient encore en pleine évolution, la connaissance de leurs capacités peut aider les programmes de radiothérapie à planifier leur intégration future, à renforcer leurs stratégies de surveillance et à améliorer leurs délais d'intervention en cas de cyberincidents potentiels. • Se tenir au courant des offres des fournisseurs et des pratiques exemplaires du secteur afin d'évaluer comment les solutions de sécurité fondées sur l'IA peuvent compléter les mesures de cybersécurité existantes sans perturber les flux de travail cliniques.	Technologique
DE2 — Processus de communication		
DE2.1	**Communication rapide lors des interruptions de service** • Mettre en place des protocoles de communication structurés et rapides, à activer immédiatement dès la détection de toute interruption de service importante. • La communication doit suivre des procédures de recours hiérarchique prédéfinies impliquant la direction du service de radio-oncologie, les équipes des activités cliniques, les services informatiques et de cybersécurité, les centres de commandement des hôpitaux et les parties prenantes des programmes régionaux visant à diminuer le fardeau du cancer. S'assurer que les options multicanaux sont préconfigurées, accessibles hors ligne et testées régulièrement. • Définir clairement les rôles, les responsabilités et le calendrier de chaque étape de recours hiérarchique afin de minimiser la confusion et les retards lors d'événements critiques.	Organisationnelle
DE2.2	**Intégration proactive avec les services informatiques et opérationnels** • Favoriser une collaboration continue entre les équipes de radiothérapie et les services informatiques et opérationnels de l'établissement afin de garantir une compréhension commune des interdépendances entre les systèmes et des priorités cliniques en cas d'interruption. • Intégrer les flux de travail spécifiques à la radiothérapie et les systèmes critiques pour la sécurité dans les plans de continuité plus généraux de l'établissement. • Désigner des personnes chargées de la liaison informatique et opérationnelle, disposant de connaissances sur	Organisationnelle

	l'infrastructure de RT, afin d'assurer une coordination rapide des mesures d'intervention, de la prise de décision et de la circulation de l'information en cas d'urgence.	
DE3 — Compréhension des répercussions sur les services (sensibilisation opérationnelle)		
DE3.1	**Perte d'accès aux dossiers de santé électroniques (DSE)** • Disposer de flux de travail d'urgence prédéfinis pour rétablir les dossiers papier, en garantissant la continuité de l'identification des patients, du suivi des traitements et de la communication avec les médecins référents.	Technologique
DE3.2	**Perte d'accès au système d'imagerie** • Mettre en place des stratégies de rechange pour accéder aux données d'imagerie essentielles en cas de panne du système, en coordination avec le service informatique de l'hôpital et conformément aux politiques sur la protection des renseignements personnels. • Des approches telles que le transfert de données d'imagerie sur des supports portables (par exemple, CD-ROM/DVD) ne doivent être envisagées que si elles sont autorisées par les politiques de l'établissement et doivent respecter les exigences applicables en matière de confidentialité et de sécurité des renseignements personnels sur la santé. • Dans la mesure du possible, privilégier les méthodes sécurisées et approuvées par l'établissement pour le partage ou la récupération d'images afin d'assurer la continuité des soins lors de la coordination des traitements entre établissements ou lors des transferts de patients.	Technologique + Organisationnelle
DE3.3	**Manque d'accès aux systèmes d'information de laboratoire (SIL)** • L'accès aux systèmes d'information de laboratoire est généralement géré par l'hôpital ou l'établissement et ne relève généralement pas du champ d'action direct du programme de radiothérapie. • Dans les situations où les résultats de laboratoire sont nécessaires pour les soins de radiothérapie (par exemple, pour déterminer l'admissibilité au traitement ou coordonner un traitement systémique concomitant), le personnel de radiothérapie doit suivre les procédures de l'établissement pour obtenir les résultats critiques en cas de panne du système, en coordination avec les services cliniques concernés et les équipes informatiques de l'hôpital.	Technologique + Organisationnelle
DE3.4	**Répercussions globales sur le service de radiothérapie** • Évaluer les répercussions potentielles d'une panne du système sur les activités de radiothérapie, notamment l'accès aux dossiers des patients, aux outils de diagnostic et de planification (par exemple, SIO, TPS), aux systèmes de planification des rendez-vous et à la configuration des accélérateurs linéaires.	Technologique

	• Planifier et consigner les stratégies d'intervention tenant compte des différents niveaux d'incidence, y compris la restauration progressive des services, la réorientation des patients en toute sécurité ou l'utilisation de flux de travail manuels validés lorsque cela est cliniquement possible. • Attribuer les responsabilités pour la surveillance des systèmes touchés et la coordination des efforts de rétablissement en collaboration avec le service informatique de l'hôpital et les autres services concernés.	

5.4. Domaine d'intervention

Le domaine d'intervention traite des mesures immédiates nécessaires pour contenir, stabiliser et gérer les répercussions d'un incident entraînant une interruption imprévue, qu'il soit causé par des cyberattaques, une défaillance de l'infrastructure ou des catastrophes naturelles. Cette section présente des mesures pragmatiques et adaptées au contexte régional ou provincial pour mobiliser les équipes d'intervention, garantir la sécurité des patients, impliquer les responsables informatiques et cliniques, et rétablir partiellement ou totalement les activités de soins dans des conditions difficiles. Elle met l'accent sur les exigences réglementaires en matière de déclaration (par exemple, le CIPVP), les stratégies d'assistance mutuelle entre établissements et la communication axée sur le patient, en particulier dans le cadre des lois sur la protection des données de santé, telles que la LPRPS. Elle reconnaît également l'importance des structures de gouvernance locales, du renforcement des effectifs en cas de fortes augmentations d'activité, des flux de travail analogiques et des stratégies de continuité des soins adaptées tant aux grands centres urbains qu'aux établissements ruraux. Le tableau suivant résume les mesures d'action associées à la phase d'intervention, regroupées en actions générales, coordination de l'équipe d'intervention, isolation des systèmes, correction des vulnérabilités et continuité des soins.

N°	Mesure d'action	Catégorie
RS0 — Évaluation initiale et identification des répercussions		
RS0.1	**Évaluation immédiate de la situation** • Obtenir une vue d'ensemble rapide de l'incident et en évaluer l'ampleur, notamment les systèmes touchés, les répercussions potentielles sur les patients et les vecteurs de compromission possibles. • Les mesures de confinement initiales doivent se concentrer sur l'isolation segmentée des systèmes concernés plutôt que sur la mise hors service de l'ensemble du réseau hospitalier. La mise hors service complète du réseau ne doit être envisagée qu'en dernier recours, par exemple en l'absence de	Technologique

	segmentation ou si les capacités de détection sont insuffisantes. • Toute décision de déconnecter ou de mettre hors service des segments du réseau doit être prise en étroite collaboration avec les équipes informatiques et de cybersécurité de l'hôpital ; les serveurs, les ordinateurs personnels et les autres clients doivent rester sous tension afin de préserver les preuves criminalistiques nécessaires à l'enquête. • À titre de précaution générale, la restriction temporaire de l'accès à Internet peut contribuer à limiter la propagation externe des logiciels malveillants, mais les procédures doivent permettre de rétablir rapidement les systèmes ou segments de réseau non touchés afin de maintenir les activités cliniques. Toutes les mesures de confinement, les critères de recours hiérarchique et les responsabilités en matière de coordination doivent être prédéfinis dans le plan de continuité des activités (PCA) et testés lors d'exercices de simulation afin de garantir une intervention rapide, sûre et conforme à la loi.	
RS0.2	**Atténuation** • Évaluer la situation afin d'identifier les mesures potentielles permettant de limiter les conséquences, de contenir les perturbations ou d'empêcher l'aggravation de la situation. • Évaluer les mesures d'atténuation immédiates et réalisables, telles que l'isolation des systèmes touchés, le passage à des flux de travail hors ligne ou l'activation des procédures de secours. • Établir les priorités en matière de mesures d'atténuation en fonction de la sécurité des patients, de la protection des données et de la continuité des soins. • Consigner toutes les mesures d'atténuation prises, y compris leur justification et leurs résultats, afin de faciliter l'analyse après incident et l'amélioration continue.	Technologique
RS0.3	**Segmentation de réseau** • Évaluer si les systèmes critiques peuvent être isolés ou segmentés afin de maintenir une continuité partielle des services en cas d'incident. Par exemple, les systèmes de planification des traitements et d'information en oncologie (ROIS) peuvent fonctionner sur un segment de réseau sécurisé et « propre » pendant que les systèmes touchés sont confinés. • Envisager à la fois la macro-segmentation (séparation du réseau de radiothérapie du réseau hospitalier global) et la micro-segmentation (isolation de petits groupes ou de dispositifs individuels) afin de limiter l'exposition et de contenir les menaces. • S'assurer que les stratégies de segmentation sont compatibles avec les flux de travail cliniques et qu'elles n'introduisent	Technologique

	aucun risque pour la sécurité ni n'enfreignent les exigences réglementaires. • Consigner les configurations de segmentation, les dépendances et les procédures pour activer les réseaux isolés dans le cadre du PCA. • Coordonner avec le service informatique et les fournisseurs pour s'assurer que les segments isolés restent connectés aux données essentielles et que le rétablissement du service après l'incident se déroule sans heurts.	
RS0.4	**Identification des systèmes non touchés** • Passer en revue tous les systèmes de radiothérapie (par exemple, TPS, tomodensitomètres, LINAC, ROIS) afin de déterminer lesquels restent opérationnels et n'ont pas été touchés par l'incident. • Évaluer si ces systèmes peuvent continuer à fournir des services partiels en toute sécurité pendant que les systèmes touchés sont isolés ou en maintenance. • Donner la priorité à la continuité des traitements urgents des patients, en veillant à ce que l'utilisation des systèmes non touchés ne compromette pas la sécurité, la qualité ou la conformité réglementaire. • Répertorier les systèmes disponibles, leur état de fonctionnement et toute restriction d'utilisation pendant l'incident. • Coordonner les efforts avec les équipes cliniques, de physique médicale et informatiques afin de mettre en place des flux de travail temporaires qui tirent parti des systèmes non touchés, tout en garantissant l'exactitude des dossiers et en minimisant les répercussions sur les patients.	Technologique
RS1 — Principes fondamentaux de l'intervention opérationnelle		
RS1.1	**La sécurité des patients comme principe fondamental** • La sécurité des patients doit guider toutes les décisions prises pendant les interruptions de service. Évaluer les risques liés aux méthodes de secours, telles que la transmission en mode fichier ou l'utilisation de flux de travail analogiques sans systèmes de contrôle et d'enregistrement (R&V). Consigner les raisons justifiant le recours à des techniques non standard et consulter la direction clinique avant de reprendre les traitements modifiés.	Organisationnelle
RS1.2	**Redéploiement du personnel et atténuation des risques** • Définir des stratégies internes de redéploiement du personnel, selon les besoins. • Évaluer les lacunes en matière de compétences lors de l'attribution de nouvelles fonctions et mettre en place des systèmes de jumelage, des protocoles de supervision ou des attentes de charge de travail réduite afin de gérer les risques cliniques.	Organisationnelle

RS1.3	**Mobilisation des dirigeants** • Mobiliser immédiatement les équipes de direction, notamment les chefs de service de radio-oncologie (RO), les responsables de programme et les responsables de la sécurité des technologies de l'information. • Activer les structures de direction en place pour faciliter la prise de décision opérationnelle en temps opportun, les décisions à haut risque ou concernant l'ensemble du système étant transmises au centre de commandement de l'établissement.	Organisationnelle
RS1.4	**Priorité accordée à la radiothérapie dans le rétablissement informatique** • Collaborer avec les équipes informatiques de l'hôpital pendant la phase de rétablissement afin de donner la priorité à la restauration des systèmes de radiothérapie, en tenant compte de leur dépendance à l'égard d'une infrastructure numérique spécialisée. • Veiller à ce que les besoins en radiothérapie soient activement pris en compte dans les priorités de rétablissement informatique de l'établissement, en particulier lorsque plusieurs services critiques sont en concurrence pour être rétablis.	Organisationnelle
RS1.5	**Dispositions relatives au renforcement des effectifs en cas de fortes augmentations d'activité** • Intégrer au PCA des modèles réalistes de renforcement des effectifs en cas de fortes augmentations d'activité, tels que la prolongation des quarts de travail, la proposition d'heures supplémentaires, l'augmentation temporaire des heures de travail pour le personnel à temps partiel et la réaffectation de personnel qualifié provenant d'activités moins prioritaires ou non urgentes. Ces mesures devraient constituer les premières mesures prises en cas de fortes augmentations d'activité. • Définir des critères de déclenchement clairs pour les mesures de gestion de fortes augmentations d'activité (par exemple, une interruption de service supérieure à 24 heures, un retard important dans les traitements, une capacité réduite du système) et établir des procédures d'approbation et de recours hiérarchique conformes aux conventions collectives et aux politiques de gestion de la fatigue de l'établissement. • En fonction de la durée prévue ou confirmée de l'interruption de service, mettre progressivement en œuvre des stratégies plus complexes de gestion de fortes augmentations d'activité. En cas de perturbations prolongées, cela peut inclure le recours à des accords régionaux d'assistance mutuelle, la formation polyvalente du personnel aux fonctions essentielles ou le recours à d'anciens employés ou à des retraités qui sont toujours titulaires d'un permis d'exercice et des qualifications	Organisationnelle

	requises. Il ne faut recourir à ces mesures que si les procédures de vérification des certifications, d'autorisation en matière de santé au travail et d'intégration par les RH ont été réalisées. • Coordonner toutes les décisions relatives au renforcement des effectifs avec la direction de l'hôpital et les ressources humaines afin de garantir le respect des exigences réglementaires, des conventions collectives et des normes de santé au travail. • Communiquer de manière transparente les attentes au personnel, notamment la durée prévue, la redistribution de la charge de travail et les aides disponibles pour réduire la fatigue et garantir la sécurité des patients.	
RS1.6	**Tenue du registre des incidents et documentation** • Consigner toutes les décisions et mesures prises pendant les interruptions de service à l'aide d'un format standardisé de plan d'action en cas d'incident (PAI) ou d'outils de documentation spécifiques aux interruptions de service. Indiquer les références temporelles, les parties responsables, les décisions prises dans des conditions contraignantes et les justifications à l'appui en vue d'audits ultérieurs ou d'examens médico-légaux.	Organisationnelle + Axée sur l'humain
RS1.7	**Prise de décision en groupe** • Mettre en place des équipes décisionnelles multidisciplinaires prédéfinies (par exemple, radio-oncologue, radiothérapeute, responsable informatique, physicien médical) afin de coordonner les actions en cas d'interruption. • Définir clairement les rôles, les responsabilités et les procédures de recours hiérarchique afin que les décisions soient consignées, justifiées et conformes aux politiques en matière de sécurité des patients et de l'établissement. • Veiller à ce que l'équipe ait accès à toutes les informations pertinentes et aux protocoles prédéfinis pour orienter ses décisions, plutôt que de se fier à un consensus ponctuel.	Organisationnelle + Axée sur l'humain
RS1.8	**Interdépendances avec d'autres services** • Anticiper les répercussions en cascade d'une interruption de service en radiologie, au laboratoire, à la pharmacie et dans d'autres services. Activer et/ou définir des protocoles de secours pour les transferts d'imagerie essentiels (par exemple, utilisation de CD-ROM en cas de panne du PACS), les demandes d'analyses de laboratoire manuelles et le suivi centralisé des médicaments.	Organisationnelle + Axée sur l'humain
RS2 — Réunions de l'équipe d'intervention en cas d'incident		
RS2.1	**Activer l'équipe d'intervention en cas d'incident (EII) de radiothérapie** • Mobiliser rapidement l'EII spécifique à la RT dès qu'une interruption importante est identifiée (cyberattaque ou autre	Organisationnelle

	perturbation). Respecter les rôles et les étapes d'intervention définis dans le PCA, en mobilisant les responsables cliniques, techniques et administratifs concernés.	
RS2.2	**Structure de commandement et coordination en cas d'incident** • Mettre en place un calendrier de réunions structuré pour l'équipe d'intervention en cas d'incident (EII), adapté à la gravité et à la phase de l'incident. Au cours de la phase initiale d'évaluation et de confinement, les réunions peuvent avoir lieu plusieurs fois par jour ; à mesure que la situation se stabilise, leur fréquence peut passer à une fois par jour ou selon les besoins. • Consigner toutes les réunions, décisions, mesures à prendre et responsabilités attribuées afin de garantir la responsabilité, la traçabilité réglementaire et la continuité entre les quarts de travail. • Désigner un centre de commandement officiel, physique ou virtuel, qui servira de centre de coordination central pour la gestion de l'incident. Cet emplacement doit être prédéfini dans le PCA et activé immédiatement en cas de recours hiérarchique. • S'assurer que le centre de commandement dispose des ressources essentielles, notamment des outils de communication (téléphones sécurisés, autre accès aux courriels, radios si nécessaire), des listes de contacts sur papier, des manuels en cas d'interruption, des inventaires des systèmes, des procédures de recours hiérarchique et des modèles de documentation. • Si la co-implantation physique n'est pas possible (par exemple, en raison de restrictions liées au contrôle des infections ou de limitations infrastructurelles), mettre en place une structure de commandement virtuelle sécurisée avec des contrôles d'accès clairement définis et des méthodes de communication de secours.	Organisationnelle
RS2.3	**Désigner un centre de commandement** • Utiliser un espace dédié (physique ou virtuel) pour les opérations de l'équipe d'intervention en cas d'incident, équipé des outils, des documents et des systèmes de communication indispensables.	Organisationnelle
RS3 — Activer le plan de continuité des activités (PCA)		
RS3.1	**Activer le plan de continuité des activités** • Activer le plan de continuité des activités (PCA). Analyser la situation réelle et suivre la procédure correspondante définie dans le PCA prévu pour ce type de situation.	Organisationnelle
RS3.2	**Adaptation du PCA** • Étant donné que le PCA prédéfini peut ne pas couvrir la situation ou les circonstances actuelles, assurer la capacité	Organisationnelle

	d'adapter le plan en conséquence, au début après avoir analysé la situation et tout au long de la crise.	
RS3.3	**Paiement de la rançon** • Définir dans le PCA la manière dont les demandes de rançon seront gérées, notamment les procédures de recours hiérarchique, les pouvoirs décisionnels, les exigences en matière de consultation juridique, la participation des assureurs spécialisés en cybersécurité (le cas échéant) et la coordination avec les organismes chargés de l'application de la loi. • Les décisions relatives au paiement d'une rançon doivent être prises aux échelons les plus élevés de la direction de l'établissement, en consultation avec des conseillers juridiques, des experts en cybersécurité, des assureurs et les autorités compétentes. • En règle générale, le paiement d'une rançon est déconseillé, car il ne garantit pas la récupération des données, peut exposer l'organisme à de nouvelles attaques, peut entraîner des risques juridiques ou réglementaires (notamment des violations de sanctions) et peut compromettre les efforts plus larges de cyberdissuasion. Le PCA doit donc privilégier la prévention, le confinement, la restauration des systèmes et la récupération à partir de sauvegardes validées comme principales stratégies de rétablissement. • Si une négociation ou une communication avec les auteurs de la menace s'avère nécessaire, celle-ci ne doit être menée que par l'intermédiaire d'experts externes qualifiés (par exemple, des sociétés spécialisées dans la réponse aux cyberincidents) et jamais par le personnel clinique ou opérationnel.	Organisationnelle + Axée sur l'humain
RS4 — Isoler les systèmes infectés		
RS4.1	**Isoler les sections du réseau compromises** • Déconnecter les segments touchés du réseau et veiller à ce que les zones non touchées puissent continuer à fonctionner dans la mesure du possible. L'accès à Internet pourrait également devoir être temporairement suspendu. Cet isolement favorise le confinement et permet de mener les enquêtes en toute sécurité.	Technologique
RS4.2	**Réseau d'urgence ou réseau virtuel** • Si possible, activer un réseau d'urgence ou un réseau virtuel préconfiguré (par exemple, pour relier le SIO, les LINAC, le TPS et les systèmes de TDM). Ce réseau doit fonctionner indépendamment du système compromis et être défini dans le PCA. Certains centres canadiens ont testé des environnements ROIS isolés ou des VLAN comme solutions de secours.	Technologique
RS4.3	**Vérification de l'accès pendant l'isolation**	Technologique

	• Lors de l'isolation du réseau, vérifier quels systèmes (par exemple, LINAC, TDM, systèmes R&V) restent accessibles, et quelles données de traitement peuvent toujours être récupérées localement. Ces informations permettent de décider s'il convient d'assurer la continuité des soins sur site à l'aide de processus hors ligne.	
RS4.4	**Solution de contournement pour l'accès au nuage** • Activer les méthodes d'accès d'urgence disponibles pour les systèmes hébergés dans le nuage, telles que les points d'accès mobiles, les répliques locales de bases de données ou les accès hybrides au nuage, afin de garantir un accès continu aux systèmes de radiothérapie pendant les interruptions. • Coordonner avec les équipes informatiques et de confidentialité de l'établissement lors de l'activation de l'accès d'urgence au nuage, en veillant à ce que les mesures prises restent conformes aux exigences provinciales et fédérales applicables en matière de protection de la vie privée et des données (par exemple, la LPRPS).	Technologique + Organisationnelle
RS5 — Correction des vulnérabilités		
RS5.1	**Correction des vulnérabilités** • Une fois la cause profonde (vecteur d'attaque ou défaillance du système) identifiée, corriger rapidement la vulnérabilité. Cela peut impliquer l'installation des correctifs manquants, la correction des erreurs de configuration ou le remplacement des composants compromis. Si aucune cause définitive n'est identifiée, une reconstruction complète du système peut s'avérer nécessaire. • Les responsables de la sécurité des technologies de l'information et les fournisseurs doivent collaborer avec la direction clinique pour s'assurer que les procédures de restauration sont sûres et conformes.	Technologique
RS5.2	**Désinfecter et mettre à jour les appareils** • Commencer à vérifier, nettoyer et mettre à jour tous les terminaux concernés (ordinateurs, serveurs, équipements réseau). Bien identifier les systèmes « propres » et les isoler des autres jusqu'à ce que l'ensemble de l'environnement ait été vérifié. Ce processus doit être consigné de manière exhaustive à des fins d'audit interne et de protection médico-légale.	Technologique
RS6 — Mettre en œuvre des procédures relatives à la continuité des soins		
RS6.0	**Recueillir les informations sur les patients** • Recueillir les informations essentielles relatives au traitement à partir de toutes les sources disponibles (copies papier, patients, personnel, communications antérieures, systèmes hébergés par des fournisseurs). • Cela comprend la vérification des données démographiques, du diagnostic, du schéma thérapeutique, du calendrier de fractionnement, ainsi que de tout dossier papier ou rapport	Organisationnelle + Technologique + Axée sur l'humain

	imprimé. La coordination avec les services de gestion des informations de santé et le respect des directives de la LPRPS sont essentiels.	
RS6.1 — Communication		
RS6.1.1	**Communication proactive avec les parties prenantes** • Mettre en œuvre le plan de communication prévu dans le PCA. Informer le personnel, les fournisseurs, la direction, les établissements partenaires et les autres parties prenantes de l'incident. Veiller à ce que les mises à jour soient communiquées en temps opportun, cohérentes et conformes au message officiel de l'établissement. Attribuer des responsabilités claires (qui communique quoi, quand et à qui) afin de réduire la confusion et la désinformation. • Établir une stratégie de communication dédiée aux patients, en tenant compte du fait que les canaux numériques habituels (par exemple, les portails patients, les systèmes de prise de rendez-vous automatisés, les courriels des hôpitaux) pourraient ne pas être disponibles. Mettre en place d'autres moyens de communication, tels que les appels téléphoniques directs, les messages sécurisés sur mobile, les notifications par message texte (si autorisées), les bannières sur le site Web, les scénarios pour les centres d'appels ou les réunions en personne. • Fournir aux patients des informations claires et concrètes : statut des rendez-vous, plans de continuité des soins, décisions de triage, garanties de sécurité, délais prévisibles et moyens de contact en cas d'urgence. • Veiller à ce que la communication soit coordonnée avec les équipes de confidentialité, juridiques et de direction, en particulier si des renseignements personnels sur la santé ont pu être compromis. • Consigner toutes les communications importantes à des fins de gouvernance, de réglementation et d'examen après incident.	Organisationnelle + Axée sur l'humain
RS6.1.2	**Circuits d'information internes** • Veiller à ce que les membres de l'équipe soient tenus informés au moyen de réunions informelles, de courriels ou de notes d'information imprimées. Partager les comptes rendus des réunions de l'équipe d'intervention en cas d'incident. Dans les établissements canadiens, cela implique d'informer les responsables cliniques et administratifs de toutes les disciplines (par exemple, RO, RT, physique médicale, soins infirmiers, prise de rendez-vous et enregistrement, informatique en oncologie).	Organisationnelle
RS6.1.3	**Plateformes de communication de rechange** • Utiliser des solutions de rechange sécurisées en cas de panne des systèmes internes (par exemple, téléphones	Technologique + Organisationnelle

	personnels, applications de messagerie sécurisées, outils basés sur le nuage). Veiller à ce que les renseignements personnels sur la santé soient chiffrés et consigner les communications à des fins d'examen juridique. Dans les régions éloignées, envisager l'utilisation de registres papier ou de lignes téléphoniques fixes. • Déterminer si les méthodes de communication de rechange prédéfinies identifiées lors de la phase de préparation (par exemple, applications de messagerie chiffrées, lignes téléphoniques de secours, radios) doivent être activées. • Vérifier le bon fonctionnement des canaux de communication de secours en temps réel et prendre note de tout écart par rapport aux performances attendues pour un examen ultérieur.	
RS6.1.4	**Lignes téléphoniques dédiées** • Mettre en place une ligne d'assistance centralisée ou un centre d'appels permettant aux patients et aux prescripteurs d'obtenir des informations en temps réel sur les perturbations des soins, comme indiqué dans le PCA.	Technologique + Organisationnelle
RS6.1.5	**Communication avec les médias** • Collaborer avec l'équipe de communication ou de relations avec les médias de l'hôpital afin de fournir des mises à jour spécifiques à la radiothérapie lors d'un incident, qui pourront être diffusées au public grâce à des sites Web, des communiqués de presse et les réseaux sociaux. • Le rôle du service de RO est de fournir des informations cliniques et opérationnelles précises concernant les services de radiothérapie. Utiliser les modèles de communication déjà approuvés, s'ils sont disponibles.	Organisationnelle + Axée sur l'humain
RS6.1.6	**Voies de communication d'urgence** • Veiller à ce que les situations urgentes (par exemple, le triage et le transfert aux échelons supérieurs pour les besoins urgents) disposent de canaux directs, tels que des téléphones d'urgence ou des chaînes de courriels chiffrées, comme indiqué dans le PCA.	Organisationnelle
RS6.2 — Continuité des soins		
RS6.2.1	**Prise de décision relative à la continuité des soins** • Lancer la planification de la continuité des soins. Décider s'il convient de reprendre les traitements sur le site en utilisant des flux de travail hors ligne ou de transférer les patients vers des établissements partenaires. Cette décision doit tenir compte de la priorité des patients, de la disponibilité du système et des accords entre établissements.	Organisationnelle + Axée sur l'humain
RS6.2.2	**Priorisation de la prise en charge des patients** • Appliquer des protocoles de triage clinique pour donner la priorité aux cas urgents (par exemple, les cancers de la tête et	Organisationnelle + Axée sur l'humain

	du cou, du col de l'utérus ou d'autres cancers à haut risque) afin de réduire au minimum les retards de traitement susceptibles de nuire aux résultats. • Harmoniser la priorisation avec les directives provinciales ou nationales, telles que les cadres de triage en oncologie élaborés pendant la pandémie de COVID-19 ou d'autres normes reconnues pour la gestion des capacités de traitement limitées. • Veiller à ce que les protocoles soient consignés, communiqués au personnel et intégrés au PCA, avec une flexibilité permettant de s'adapter au volume local de patients et aux ressources disponibles.	
RS6.3 — Traitements sur site		
RS6.3.1	**Évaluation des traitements hors ligne** • Procéder à une évaluation des risques cliniques et de sécurité avant d'entamer tout traitement hors ligne, y compris l'évaluation du risque potentiel de mauvaise utilisation, des processus de vérification disponibles et de la capacité à assurer la sécurité de l'administration du traitement sans connexion au système standard. • Si cette évaluation confirme que la procédure est sûre et réalisable, entamer le traitement sur place en utilisant les modes hors ligne disponibles (par exemple, les fonctionnalités proposées par le fournisseur, telles que le mode fichier), en s'appuyant sur une documentation papier, des processus de vérification manuels et des listes de contrôle du personnel. • Vérifier que le traitement hors ligne est autorisé dans le cadre de votre autorisation et de la réglementation, car certains établissements peuvent ne pas être autorisés à traiter en mode hors ligne. Le cas échéant, les plans d'urgence peuvent devoir être examinés ou approuvés par la Commission canadienne de sûreté nucléaire (CCSN).	Technologique + Organisationnelle
RS6.3.2	**Configuration manuelle des traitements** • Conformément au PCA, utiliser les plans DICOM enregistrés ou définir des configurations de base pour les traitements palliatifs (par exemple, électrons) lorsque le logiciel de traitement n'est pas disponible. Enregistrer manuellement chaque fraction et chaque champ de traitement.	Technologique + Organisationnelle
RS6.3.3	**Listes de contrôle pour l'AQ et la sécurité** • Mettre en place des listes de contrôle prédéfinies pour l'AQ (par exemple, double signature, journaux horodatés) afin de limiter les risques lors de l'administration de traitements en mode hors ligne.	Organisationnelle + Axée sur l'humain
RS6.3.4	**Assistance des fournisseurs pour le mode hors ligne** • Coordonner avec les fournisseurs du ROIS afin d'obtenir l'accès au mode fichier ou aux fonctionnalités hors ligne pour	Technologique + Organisationnelle

	la prestation des traitements. Intégrer les protocoles de communication avec les fournisseurs dans le PCA.	
RS6.4 — Réorientation des patients		
RS6.4.1	**Transfert vers d'autres établissements** • Si les traitements ne peuvent pas être poursuivis sur le site, transférer les patients vers des centres régionaux disposant de capacités suffisantes. Recourir aux accords interprovinciaux le cas échéant.	Organisationnelle
RS6.4.2	**Collaboration avec les hôpitaux partenaires** • Communiquer avec les hôpitaux désignés dans les PE préétablis (voir la section PP2.9). Si aucun accord n'existe, en conclure un rapidement. Organiser la logistique et les protocoles de transfert.	Organisationnelle
RS6.4.3	**Redéploiement du personnel pour faciliter les transferts** • Le redéploiement du personnel de radiothérapie (radiothérapeutes, radiologues, physiciens médicaux) afin d'assurer la prise en charge des patients dans le centre d'accueil ne doit être envisagé que lorsque cela est réalisable et autorisé par les accords, les politiques locales, les syndicats et les dispositions en matière de responsabilité civile et d'assurance, et lorsque cela est jugé sans danger (voir la section PP2.9). • Si un redéploiement du personnel est possible, mettre en place des systèmes de jumelage, des séances d'orientation et des réunions sur les mesures de sécurité afin de minimiser les risques liés à l'intégration et d'assurer la continuité des soins.	Organisationnelle + Axée sur l'humain
RS6.4.4	**Transfert des données sur les traitements** • S'assurer que chaque patient est accompagné d'un dossier clinique complet : diagnostic, plan de traitement, état actuel, imagerie, traitements antérieurs et/ou antécédents de ré-irradiation, ainsi que tout rapport pertinent.	Technologique + Organisationnelle
RS6.5 — Processus autres que la radiothérapie		
RS6.5.1	**Continuité des fonctions cliniques connexes** • Déterminer quels autres processus cliniques (par exemple, consultations, imagerie, simulation, planification) peuvent se poursuivre. Cela dépend de la disponibilité des systèmes (par exemple, PACS, laboratoire).	Organisationnelle
RS6.5.2	**Aperçu et visualisation des processus** • Maintenir un système de suivi visuel à jour concernant l'état des patients, les visites et les tâches. Utiliser des tableaux blancs, des feuilles de calcul ou des plateformes infonuagiques (si disponibles).	Technologique + Organisationnelle
RS6.6 — Documentation des traitements		
RS6.6.1	**Documentation papier de l'ensemble des soins** • En plus de la documentation papier de chaque séance de traitement (RS6.3.2), veiller à consigner chaque étape des	Technologique + Organisationnelle

	traitements sur papier ; utiliser les modèles de documentation prédéfinis (PP2.4) • Conserver les dossiers de traitement sous forme imprimée avec toutes les informations, ainsi que les notes écrites à la main (données démographiques, diagnostic, anamnèse, consentement du patient, prescription, planification, notes d'évolution, commentaires généraux, rapports, résultats d'examens d'imagerie, etc.)	
RS6.6.2	**Rapports** • Définir où conserver les renseignements médicaux (rapports écrits à la main ou à la machine, images sur CD/DVD, résultats de laboratoire, etc.) et comment en transférer des copies d'un établissement à l'autre.	Organisationnelle
RS6.6.3	**Accès aux imprimantes et aux photocopieurs** • Veiller à disposer d'imprimantes et de photocopieurs capables de fonctionner sans réseau.	Technologique
RS6.7 — Documentation des incidents		
RS6.7.1	**Consigner toutes les mesures prises lors d'un incident** • Tenir un registre détaillé des décisions, des mesures et des étapes de recours hiérarchique mises en œuvre par l'équipe d'intervention en cas d'incident et le personnel opérationnel tout au long de l'incident.	Organisationnelle
RS6.7.2	**Aperçu de l'état de la crise** • Utiliser des outils visuels centralisés (par exemple, des tableaux blancs, des tableaux de bord du centre de commandement) pour suivre l'évolution de la crise et les principaux défis.	Organisationnelle

5.5. Domaine du rétablissement

Le domaine du rétablissement décrit la transition systématique des opérations d'urgence vers la restauration complète des systèmes cliniques et numériques. Cette phase est essentielle pour assurer la continuité des soins aux patients, préserver l'intégrité des données et atténuer les répercussions à long terme à la suite d'une interruption de service. Les activités de rétablissement sont classées selon des dimensions techniques et organisationnelles et mettent l'accent sur la collaboration entre les équipes de radio-oncologie, les services informatiques et les partenaires externes, tels que les fournisseurs et les assureurs. Les principales mesures comprennent la reprise progressive des services, l'assurance de la qualité des systèmes restaurés, la saisie rétroactive des données hors ligne, une communication efficace et la gestion des retards cliniques.

N°	**Mesure d'action**	Catégorie
RC0 — Rétablissement générale		
RC0.1	**Fonction de rétablissement**	Organisationnelle

	• Mettre en œuvre le processus de rétablissement tel que défini dans le PCA une fois que le confinement et la stabilisation ont été assurés. Veiller à ce que les critères d'activation, la surveillance par la direction et l'ordre des étapes de rétablissement soient clairement respectés. • La fonction de rétablissement englobe toutes les activités coordonnées nécessaires pour restaurer les systèmes, valider l'intégrité des données, reprendre les activités cliniques normales et renforcer la résilience à la suite d'un cyberincident ou d'une interruption prolongée. • Définir clairement les rôles et les délais pour la saisie rétroactive des informations générées pendant l'interruption (par exemple, documentation papier, dossiers de traitement manuels) dans les systèmes électroniques une fois ces derniers restaurés. Mettre en place des étapes de validation afin d'éviter toute perte de données, duplication ou erreur de transcription. • Suivre la progression du rétablissement par rapport aux objectifs de temps de rétablissement prédéfinis et communiquer les mises à jour sur l'état d'avancement aux équipes cliniques et à la direction jusqu'à ce que la pleine capacité opérationnelle soit rétablie. • Mener un examen structuré après le rétablissement afin d'identifier les améliorations à apporter au système, les optimisations des flux de travail et les mesures de renforcement de la résilience.	
RC0.2	**Reprise progressive jusqu'au retour aux activités normales** • Une fois que les systèmes ont été entièrement rétablis, les processus de traitement habituels ne peuvent pas reprendre immédiatement dans leur intégralité. Un redémarrage progressif accompagné de contrôles de sécurité complets doit être effectué, ce qui peut prendre beaucoup de temps.	Organisationnelle
RC0.3	**Collaboration** • La coordination du rétablissement doit impliquer la direction du programme de radio-oncologie, les services informatiques de l'hôpital et les fournisseurs de ROIS, comme décrit dans le PCA. En outre, les responsables locaux de la protection de la vie privée, les conseillers juridiques, les organismes chargés de l'application de la loi et les fournisseurs de cybersécurité doivent participer à l'analyse judiciaire, au confinement des menaces et à la restauration du système. • Le cas échéant, les autorités sanitaires provinciales peuvent également apporter leur aide pour la coordination du soutien au rétablissement et les communications entre les instances compétentes.	Organisationnelle + Axée sur l'humain
RC0.4	**Accès aux sauvegardes**	Technologique

	• Accéder aux données du système et les restaurer à partir des sauvegardes disponibles, conformément aux procédures définies dans le plan de continuité des activités (PCA) et aux protocoles de rétablissement de l'établissement, en veillant à ce que les mesures prises restent conformes aux lois applicables en matière de protection de la vie privée, notamment la LPRPS et la LPRPDE. • Dans la mesure du possible, récupérer les données de sauvegarde à l'aide d'une infrastructure fonctionnant indépendamment du réseau central compromis de l'hôpital, comme des systèmes autonomes ou physiquement isolés, conformément au PCA, afin de garantir une restauration sécurisée du système.	
RC0.5	**Communication des attentes** • Préciser clairement à toutes les parties prenantes, y compris les équipes cliniques, la direction de l'hôpital, les patients et les autorités provinciales, que le rétablissement complet et le retour à un fonctionnement normal pourraient prendre plusieurs semaines, voire plusieurs mois. Ce délai dépend de l'ampleur de l'incident, des capacités informatiques et de l'assistance apportée par les fournisseurs.	Organisationnelle + Axée sur l'humain
RC1 — Activer le plan de rétablissement		
RC1.1	**Lancer le processus de rétablissement** • Dès que l'ampleur de l'incident a été déterminée et que les vulnérabilités ou les points d'entrée ont été corrigés, le processus de rétablissement doit être lancé.	Organisationnelle
RC2 — Méthode de rétablissement		
RC2.1	**Définir le processus de rétablissement à utiliser** • Conformément au PCA, la méthode de rétablissement à utiliser doit maintenant être déterminée. Cela dépend fortement de l'ampleur de l'incident et des sauvegardes disponibles.	Technologique
RC2.2	**Configurer de nouveaux ordinateurs** • Si la situation l'exige, configurer de nouveaux ordinateurs et ordinateurs portables ou envisager une réinitialisation complète des appareils existants, et les identifier clairement afin qu'il soit évident quels ordinateurs sont neufs et sains et lesquels ne doivent pas encore être utilisés.	Technologique
RC2.3	**Reconstruire l'ensemble de l'infrastructure de technologie de l'information** • Selon l'ampleur de l'incident, il peut être nécessaire de reconstruire l'ensemble de l'infrastructure de technologie de l'information (serveurs, bases de données, réseau, etc.).	Technologique
RC2.4	**Reconstruction du ROIS** • La réinstallation du ROIS est effectuée, si nécessaire, en collaboration avec le fournisseur canadien agréé ou le sous-	Technologique

	traitant tiers qui prend en charge le système (par exemple, les fournisseurs de ROIS). • Les systèmes sont restaurés conformément aux configurations préalablement validées et testés à l'aide des protocoles de vérification fournis par le fournisseur. La documentation doit être conforme à la LPRPS et aux directives de l'établissement relatives à la protection des renseignements personnels.	
RC2.5	**Restauration des données** • Restauration à partir de sauvegardes hors ligne et chiffrées conservées dans le cadre du plan de sauvegarde des données.	Organisationnelle
RC2.6	**Préparation à saisir à nouveau les données** • Identifier toutes les informations cliniques, opérationnelles et liées aux traitements générées pendant l'interruption (par exemple, données démographiques des patients, paramètres de traitement, notes d'évolution, formulaires de consentement) qui doivent être saisies à nouveau dans les systèmes numériques. • Attribuer des responsabilités claires pour chaque flux de données, que ce soit aux responsables cliniques, aux physiciens médicaux ou au personnel administratif, et définir les délais, les flux de travail et les procédures de vérification. • Veiller à la conformité avec les politiques de l'établissement, les réglementations en matière de protection de la vie privée (par exemple, la LPRPS) et les exigences des systèmes des fournisseurs afin de minimiser les risques d'erreur et de non-conformité juridique lors de la nouvelle saisie des données.	Organisationnelle + Axée sur l'humain
RC2.7	**Saisie à nouveau des données après le rétablissement** • Lors de la saisie à nouveau des données recueillies pendant l'interruption (par exemple, à partir de dossiers papier ou de sauvegardes sur clé USB), les établissements doivent suivre les procédures de validation définies par l'hôpital, les protocoles de double vérification et les processus d'AQ médicale. Cela inclut la vérification de l'exactitude des doses et du fractionnement grâce à la surveillance des physiciens médicaux et des radio-oncologues. Les mesures de protection de la vie privée supplémentaires prévues par la LPRPS doivent être respectées lors du traitement des dossiers temporaires.	Organisationnelle + Technologique
RC2.8	**Contrôle de sécurité après le paiement d'une rançon** • Comme indiqué précédemment, il n'est pas recommandé de payer une rançon à la suite d'une cyberattaque pour plusieurs raisons, notamment l'absence de garantie quant à la récupération des données, le risque d'encourager de nouvelles attaques, les conséquences légales et réglementaires potentielles, les pertes financières et les coûts cachés, ainsi que les préoccupations liées à la confidentialité des données. Toutefois, si la rançon a été payée et que le système a été débloqué par les pirates informatiques, il ne faut pas encore	Technologique

	leur faire confiance, même si tout semble fonctionner normalement. Des contrôles de sécurité approfondis doivent être effectués afin d'éliminer tout logiciel malveillant résiduel.	
RC3 — Vérification des données de rétablissement		
RC3.1	**Assurance de la qualité, restauration des données et cohérence des données** • La saisie à nouveau des données doit respecter les protocoles organisationnels en matière d'intégrité des données, tels que ceux définis par le service de protection de la vie privée ou l'équipe AQ de l'hôpital. • Des outils d'AQ spécifiques à la radiothérapie (par exemple, comparaison avec les plans de traitement initiaux, audits de contrôle et d'enregistrement) doivent être utilisés afin de minimiser le risque de perte de données ou d'erreur de traitement. La documentation doit être conservée en toute sécurité conformément aux directives de la LPRPS.	Organisationnelle
RC3.2	**Vérification des processus** • Vérifier si les processus habituels fonctionnent, par exemple à l'aide d'un essai fictif ou d'un test de bout en bout.	Organisationnelle + Technologique
RC3.3	**Continuité des soins** • Déterminer la marche à suivre pour les patients actuellement pris en charge dans le cadre de la procédure d'urgence. Ces patients peuvent être pris en charge selon les procédures habituelles ou continuer leur traitement dans le cadre de la procédure d'urgence. Cela s'applique en particulier aux patients qui ont été orientés vers d'autres sites.	Organisationnelle + Technologique
RC4 — Communication (interne)		
RC4.1	**Communication régulière** • Informer régulièrement les employés de l'état d'avancement des travaux de rétablissement, notamment pour leur donner une idée du moment où les processus habituels pourront reprendre. • Informer les autres parties prenantes (patients, prestataires, cadres supérieurs, fournisseurs) dès que certaines mesures ont été prises. • Organiser régulièrement (quotidiennement) des réunions de crise pendant la phase de rétablissement. • La communication sur les canaux publics doit être coordonnée par les services des relations publiques ou de la communication de l'hôpital. • Des lignes dédiées aux médias ou des mises à jour d'urgence peuvent être publiées sur les sites Web des hôpitaux et sur des portails provinciaux de confiance, si nécessaire.	Organisationnelle
RC4.2	**Communication avec les patients** • Communiquer régulièrement avec les patients pour les tenir informés de l'avancement du processus de rétablissement.	Organisationnelle

RC5 — Définir la fin du rétablissement et reprendre les activités normales		
RC5.1	**Déclaration** • Dès que les processus de rétablissement sont terminés, que les données ont été vérifiées et que les processus habituels fonctionnent à nouveau, l'incident peut être considéré comme clos. Déclarer que la restauration des systèmes et la récupération des données sont terminées et en informer toutes les parties prenantes.	Organisationnelle + Axée sur l'humain
RC5.2	**Retour à la normale** • Passer des procédures d'urgence aux processus de traitement habituels en adoptant une approche progressive par étapes, plutôt qu'une date de reprise unique et fixe. • Rétablir progressivement les services en fonction de la stabilité du système, de l'intégrité validée des données, des effectifs disponibles et des priorités cliniques. Définir clairement les critères nécessaires pour passer d'une phase à l'autre (par exemple, rétablissement partiel du système, extension des horaires, capacité de service complète). • Communiquer chaque transition de phase et les niveaux de service attendus au personnel, aux patients, aux fournisseurs et à la direction afin d'assurer une harmonisation et de gérer les attentes. • Ne déclarer officiellement la reprise complète des services qu'une fois que tous les systèmes critiques ont été vérifiés, que les traitements en attente ont été pris en charge ou font l'objet d'une gestion active, et que les procédures d'urgence ne sont plus nécessaires. • Consigner le processus de transition et maintenir un état de préparation aux situations d'urgence au cas où des problèmes réapparaîtraient lors de la reprise progressive des activités.	Organisationnelle
RC5.3	**Compensation des interruptions de traitement** • En cas d'interruptions de traitement, évaluer l'incidence clinique potentielle en fonction du type de tumeur, de la dose totale administrée, de la durée globale du traitement et des facteurs spécifiques au patient. • Lorsqu'il est cliniquement indiqué, envisager des stratégies de compensation fondées sur des principes radiobiologiques établis et des recommandations professionnelles (par exemple, ajustements du calendrier, fractions supplémentaires ou traitement accéléré), selon les recommandations du radio-oncologue traitant en collaboration avec le service de physique médicale. • Les décisions relatives à la compensation doivent être individualisées et clairement consignées dans le dossier du patient, avec les justifications et les informations communiquées au patient.	Organisationnelle + Technologique

	• Comme aucune norme nationale canadienne unique n'impose de formules de compensation particulières, les services doivent disposer de recommandations cliniques locales afin de favoriser une prise de décision cohérente et fondée sur des données probantes.	

5.6. Domaine de compte rendu et de l'amélioration continue

Le dernier domaine du cadre porte sur l'évaluation après incident et le renforcement du système par l'apprentissage structuré, la responsabilisation et la diffusion des connaissances. Ce domaine est essentiel pour transformer les expériences de crise en renseignements exploitables qui réduisent les risques futurs et renforcent la résilience institutionnelle. Les mesures incluses dans cette catégorie couvrent les processus complets de compte rendu, les examens formels des performances du système, l'adaptation des protocoles d'intervention et la planification stratégique des investissements. De plus, ce domaine souligne l'importance de l'apprentissage par les pairs entre les différentes provinces et différents territoires et de la coordination nationale menée par l'ACAPC, le PCQR et les parties prenantes provinciales. Les mesures d'amélioration continue comprennent également l'évaluation du soutien apporté par les fournisseurs, le perfectionnement des processus hors ligne, le renforcement des pratiques de communication et la garantie d'un suivi à long terme des patients touchés par des interruptions de traitement. Collectivement, ces mesures garantissent que les services de radiothérapie ne se contentent pas de revenir à leur état initial après une interruption de service, mais qu'ils évoluent pour devenir plus résilients et plus réactifs.

N°	**Mesure d'action**	Catégorie
DC0 — Réunion de compte rendu et amélioration continue en général		
DC0.1	**Recommandation** • Utiliser les connaissances et les enseignements tirés des événements précédents pour élaborer des recommandations visant à renforcer la gestion des interruptions imprévues et prolongées en radiothérapie.	Organisationnelle
DC0.2	**Réunion de compte rendu après l'incident et enseignements tirés** • Organiser une réunion de compte rendu structurée après la reprise des activités, rassemblant les membres de l'équipe d'intervention en cas d'incident (EII) et les principaux intervenants qui ont participé directement aux activités du centre de commandement et à l'intervention opérationnelle. • L'objectif de cette réunion de compte rendu est de passer en revue les événements, d'évaluer ce qui a bien fonctionné, d'identifier les lacunes ou les inefficacités, et d'évaluer les	Organisationnelle + Axée sur l'humain

	mesures relatives à la communication, à la gouvernance, à l'intervention technique et à la continuité des soins cliniques. • Consigner les enseignements tirés et les traduire en mises à jour concrètes du PCA, des manuels de gestion des interruptions de service, des modèles de communication, des protocoles de triage et des mesures de sécurité techniques. • Le cas échéant, partager les principales conclusions avec la direction de l'établissement, les partenaires régionaux ou les réseaux professionnels afin de favoriser l'apprentissage à l'échelle du système, tout en respectant les considérations de confidentialité et de sécurité.	
DC0.3	**Préparation continue** • Mettre en place une procédure de mises à jour et de tests réguliers à toutes les étapes d'une interruption imprévue ou prolongée, en veillant à ce que les plans de détection, de réaction, d'intervention et de rétablissement restent robustes et adaptés à l'évolution des menaces, et à ce que des améliorations continues soient mises en œuvre.	Organisationnelle
DC0.4	**Soutien au personnel** • Reconnaître et saluer officiellement les contributions du personnel pendant l'incident. Exprimer votre gratitude pour la flexibilité, le professionnalisme et l'esprit d'équipe dont le personnel a fait preuve dans des conditions difficiles. • Mener des discussions constructives pour réfléchir aux points positifs et mettre en avant des exemples de collaboration, de leadership et de résolution de problèmes efficaces. Le renforcement positif favorise la résilience et la culture organisationnelle. • Reconnaître que l'esprit d'équipe a pu être mis à rude épreuve en fonction de la nature de l'événement et de la manière dont il a été géré. Offrir des occasions de dialogue ouvert, de sécurité psychologique et de retour d'information constructif. • Surveiller les signes d'épuisement professionnel ou de détresse morale et garantir l'accès aux ressources de bien-être, aux programmes de soutien par les pairs ou aux services d'aide aux employés proposés par l'établissement. • Profiter de la période après l'incident pour renforcer la cohésion de l'équipe grâce à une mobilisation continue, à l'apprentissage et à des efforts communs d'amélioration.	Axée sur l'humain, Organisationnelle
DC1 — Examen des événements passés		
DC1.1	**Examen général** • Créer une liste exhaustive de tous les défis et problèmes survenus pendant l'interruption imprévue/prolongée.	Technologique
DC1.2	**Gestion des risques et vulnérabilité** • Identifier les faiblesses de l'hôpital et de son concept de cybersécurité. Analyser si la gestion des risques de cybersécurité a été efficace.	Organisationnelle + Technologique

DC1.3	**Communication** • Résumer la manière dont la communication a fonctionné avec les patients, le personnel, les prestataires et les fournisseurs. Évaluer la transparence de la communication et dans quelle mesure les parties prenantes se sont senties informées.	Axée sur l'humain
DC1.4	**Fournisseurs** • Réaliser une analyse après incident de l'implication des fournisseurs pendant les phases d'intervention et de rétablissement, y compris la disponibilité et l'efficacité de leur assistance, le cas échéant.	Organisationnelle + Technologique
DC1.5	**Phase de prévention** • En collaboration avec le service informatique, les responsables de la cybersécurité et la direction de l'établissement, identifier les mesures qui auraient pu prévenir ou atténuer l'incident, y compris les mesures au sein du programme de radiothérapie et les contrôles plus larges à l'échelle de l'établissement.	Technologique
DC1.6	**Phase d'intervention** • Analyser les mesures à prendre de manière urgente par rapport à une intervention par étapes.	Organisationnelle
DC1.7	**Données hors ligne disponibles** • Évaluer la disponibilité, la facilité d'utilisation, l'exhaustivité et la qualité des données hors ligne, ainsi que l'efficacité des modèles préparés pour les processus sur papier.	Organisationnelle + Technologique
DC1.8	**Priorité des patients** • Analyser le fonctionnement du triage et de la priorisation des patients, ainsi que toute incidence éventuelle sur la prise en charge des patients.	Organisationnelle + Axée sur l'humain
DC1.9	**Traitement hors ligne** • Analyser le fonctionnement de l'administration de la RT sans SIO ni système R&V, le fonctionnement de l'AQ et le degré de sécurité avec lequel le traitement a pu être administré.	Technologique
DC1.10	**Orientation des patients** • Analyser dans quelle mesure l'orientation des patients vers d'autres hôpitaux a fonctionné, c'est-à-dire la logistique des patients, le transfert des données et la continuité des soins.	Organisationnelle + Technologique
DC1.11	**Sauvegardes et rétablissement** • Vérifier l'état et l'utilité des sauvegardes hors ligne ainsi que des serveurs et du réseau hors ligne/redondants, le cas échéant.	Technologique
DC1.12	**Phase de rétablissement** • Analyser le déroulement du rétablissement, la manière dont les données restaurées et les données sur papier ont été intégrées et le processus de retour à la normale.	Organisationnelle + Technologique
DC1.13	**Résultats des traitements** • Surveiller les patients ayant reçu un traitement inhabituel à la suite de l'incident (par exemple, interruptions prolongées, séances manquées).	Organisationnelle

	• Consigner toute incidence potentielle sur les résultats des traitements.	
DC2 — Adaptation du plan d'intervention en cas d'incident		
DC2.1	**Protocole en cas de sinistre** • Les résultats de l'analyse et de l'examen des événements passés ainsi que des procédures associées doivent être intégrés dans une adaptation des plans d'intervention en cas d'incident pour la détection, l'intervention et le rétablissement.	Organisationnelle + Technologique
DC2.2	**Investissements futurs** • Tirer les enseignements des analyses des événements passés afin d'identifier les investissements financiers, techniques et en ressources humaines nécessaires pour être mieux préparés aux événements futurs.	Organisationnelle + Axée sur l'humain
DC3 — Diffuser les enseignements tirés par l'organisme à chaque phase de la gestion de l'incident		
DC3.1	**Partage d'expériences** • Encourager le partage des expériences liées à l'incident et des solutions pratiques, non seulement au sein des services et des hôpitaux, mais aussi par l'intermédiaire de plateformes pancanadiennes, telles que le PCQR, ainsi que des comités ou forums provinciaux de radiothérapie. Le transfert de connaissances entre pairs peut contribuer à renforcer la préparation dans les différentes provinces et différents territoires.	Organisationnelle
DC3.2	**Déclaration des incidents** • À la suite de toute interruption de service importante ou de tout cyberincident, veiller à ce que tous les centres concernés rédigent des rapports d'incident officiels en utilisant les systèmes de déclaration provinciaux ou nationaux existants (par exemple, le SNDAI-RT, les portails provinciaux dédiés aux incidents de santé numérique). Ces rapports doivent alimenter des analyses d'apprentissage structurées qui favorisent l'amélioration de la qualité.	Organisationnelle + Technologique
DC3.3	**Relations avec le service informatique** • Favoriser une intégration plus étroite entre les services de radiothérapie et les services informatiques grâce à des réunions régulières et à la création de comités de gouvernance conjoints, incluant la définition des objectifs communs (en mettant l'accent sur les soins aux patients), des canaux de communication transparents et bien définis, des examens de cybersécurité et des évaluations communes des risques. • Dans les grandes régions disposant de systèmes intégrés, cette relation est essentielle pour garantir que les besoins spécifiques à la radiothérapie soient prioritaires.	Organisationnelle

6. Facteurs habilitants généraux du système

Outre les six phases opérationnelles de la préparation et de l'intervention en cas d'urgence, le *Cadre pancanadien de préparation aux situations d'urgence en cas d'interruption des activités des centres de radiothérapie* intègre un ensemble de facteurs habilitants généraux qui favorisent la viabilité à long terme, l'harmonisation organisationnelle et le changement de culture. Ces éléments systémiques comprennent l'implication active de la haute direction dans la prise en charge des risques et l'allocation des ressources, l'établissement de partenariats solides avec les fournisseurs du secteur et des systèmes, un leadership visible et responsable en cas de crise, ainsi que l'intégration de normes reconnues et d'initiatives éducatives dans le perfectionnement professionnel. En intégrant ces éléments habilitants interdisciplinaires, les programmes de radiothérapie peuvent garantir que la préparation ne se limite pas aux aspects techniques, mais qu'elle soit reconnue comme une responsabilité stratégique partagée à tous les échelons de l'établissement et au sein des réseaux intersectoriels.

N°	**Mesure d'action**	Catégorie
OT1 — Implication de la direction générale		
OT1.1	**Responsabilité partagée et transfert de connaissances** • Reconnaître que la préparation aux interruptions de service implique plusieurs domaines de la direction de l'hôpital, notamment la radiothérapie, l'informatique, la cybersécurité, la direction clinique et la gestion des risques. • Soutenir la coordination et la planification entre les services, en veillant à ce que les perspectives opérationnelles, cliniques et techniques pertinentes soient intégrées dans les efforts de préparation et d'intervention. • Maintenir des mécanismes de partage continu des connaissances et de communication entre les équipes de radiothérapie, la direction du DPI et des services informatiques, et les fonctions de gestion des risques de l'établissement, afin de favoriser la maîtrise de la situation et une prise de décision coordonnée.	Organisationnelle + Axée sur l'humain
OT1.2	**Coûts** • Allouer des fonds aux initiatives de préparation aux interruptions de service et de cybersécurité, notamment en matière de personnel, d'infrastructure, de formation et de collaboration avec les fournisseurs. • Les demandes de financement doivent être liées à la continuité des activités, à l'atténuation des risques cliniques et aux priorités en matière de qualité et de sécurité déjà suivies dans les hôpitaux canadiens.	Organisationnelle
OT2 — Implication du secteur et des prestataires		

OT2.1	**Partenariat avec le secteur** • Tirer parti des partenariats existants avec les fournisseurs, les prestataires de services infonuagiques et les fabricants de dispositifs médicaux afin de renforcer la résilience des systèmes, de coordonner les interventions en cas d'incident et de faciliter les activités de rétablissement. • Le cas échéant, intégrer des exercices de mise à l'essai (par exemple, des simulations sur table) dans les contrats de service des fournisseurs et dans les initiatives de collaboration visant à renforcer la préparation à l'échelle du secteur et à favoriser l'apprentissage partagé.	Organisationnelle + Axée sur l'humain
OT3 — Leadership en situation de crise		
OT3.1	**Présence visible et responsabilité des dirigeants** • La préparation aux situations d'urgence en radiothérapie doit s'appuyer sur un leadership visible et responsable en cas de perturbations du système, renforçant ainsi l'engagement de l'organisme en faveur de la sécurité des patients et de la continuité des soins. Les établissements doivent définir des attentes selon lesquelles les responsables cliniques et opérationnels maintiennent une présence active et visible lors de pannes prolongées afin de faciliter la communication coordonnée, les décisions de triage et la collaboration entre les équipes. L'intégration de cette visibilité du leadership au sein de la gouvernance organisationnelle des situations d'urgence permet de garantir que les équipes de première ligne sont soutenues et que les efforts d'intervention restent coordonnés entre les groupes cliniques, opérationnels et techniques.	Organisationnelle + Axée sur l'humain
OT3.2	**Bien-être du personnel et des patients** • Intégrer des contrôles du bien-être du personnel dans les flux de travail d'urgence, en particulier lors de perturbations prolongées des services. Cela inclut la rotation des tâches, les comptes rendus et la mise à disposition de ressources liées au bien-être. Les équipes des ressources humaines et de la santé au travail doivent être intégrées au système de gestion des incidents (SGI). • Les discussions animées par les cliniciens et le soutien psychosocial doivent aller au-delà des aspects logistiques afin d'aborder le stress des patients lié à l'interruption du système ou des soins. Ces mesures contribuent à réduire l'anxiété pendant les perturbations et favorisent le regain de confiance à mesure que les services sont rétablis.	Axée sur l'humain
OT4 — Normes et formation		
OT4.1	**Normes informatiques** • Les programmes de radiothérapie doivent travailler en collaboration avec les experts en informatique et en cybersécurité de l'établissement afin de garantir que les	Organisationnelle + Axée sur l'humain

	cadres de cybersécurité pertinents soient intégrés aux normes de santé numérique et aux pratiques opérationnelles de l'organisme. • Les équipes de radiothérapie doivent également participer aux formations et aux activités de préparation pertinentes afin de s'assurer qu'elles sont sensibilisées aux risques liés à la cybersécurité et aux procédures d'intervention.	
OT4.2	**Modélisation des risques** • Les systèmes de santé et les équipes informatiques et de cybersécurité des établissements devraient intégrer les flux de travail et les interdépendances spécifiques à la radiothérapie dans leurs processus plus larges de modélisation des menaces et d'évaluation des risques. • La collaboration avec les responsables cliniques et les fournisseurs de systèmes peut contribuer à garantir que les vulnérabilités potentielles, les risques d'interruptions de service et les répercussions opérationnelles sur les services de radiothérapie soient correctement identifiés et pris en compte dans les processus organisationnels de gestion des risques.	Organisationnelle + Technologique
OT4.3	**Formation** • Les programmes de formation canadiens devraient inclure la gestion des interruptions de service, la consignation sur papier, les ordonnances verbales et la prise de décision en matière de traitements d'urgence dans les cours cliniques destinés aux radiothérapeutes, aux EPM et aux résidents.	Organisationnelle + Axée sur l'humain

7. Conclusion

Le Cadre pancanadien de préparation aux situations d'urgence en cas d'interruption des activités des centres de radiothérapie marque une étape importante dans le renforcement de la résilience du secteur de la radiothérapie à l'échelle du Canada. Élaboré à partir d'analyses comparatives internationales, d'enquêtes pancanadiennes et des contributions conjointes d'experts cliniques, techniques et en matière de politiques, il propose un modèle structuré, fondé sur le cycle de vie, qui intègre la cybersécurité et la préparation aux situations d'urgence en une stratégie cohérente.

Ce cadre est conçu pour être à la fois normalisé et adaptable ; il s'aligne sur les normes internationales tout en tenant compte du contexte, de la législation et des structures du système de santé canadiens. Organisé en six domaines opérationnels — préparation, prévention, détection, intervention, rétablissement et amélioration continue — et soutenu par des facilitateurs généraux portant sur le leadership, les partenariats avec le secteur et la formation, ce cadre garantit une approche globale couvrant la gouvernance, la technologie et la préparation du personnel.

Grâce à ses mesures d'action multidisciplinaires, ce cadre fournit aux centres de radiothérapie des orientations claires pour améliorer leur préparation aux interruptions de service, garantir la sécurité des patients et assurer la continuité des opérations en cas de perturbations, d'origine cyber ou non. Sa conception met l'accent sur la collaboration entre les équipes informatiques, cliniques et administratives, garantissant ainsi que la préparation ne soit pas considérée comme un effort technique isolé, mais comme une responsabilité partagée par l'ensemble de l'établissement.

8. Prochaines étapes

La prochaine phase vise à traduire ce cadre en outils de mise en œuvre concrets et en initiatives d'essai. Les principales mesures sont les suivantes :

- Mener des activités de mobilisation des connaissances afin de faire connaître les travaux et de favoriser leur diffusion et leur déploiement à grande échelle.
- Soutenir l'adoption de modèles, de listes de contrôle et de protocoles de simulation pancanadiens afin de mettre en œuvre les domaines du cadre.
- Explorer les possibilités d'intégrer ce cadre dans les programmes de qualité existants du PCQR, les parcours d'agrément et les programmes de formation.
- Mettre en place un mécanisme de retour d'information continu afin d'évaluer l'adoption du cadre, de recueillir les enseignements tirés et d'assurer des mises à jour itératives en fonction de l'évolution des menaces et des technologies.

À long terme, ce cadre jette les bases d'une approche coordonnée à l'échelle nationale en matière de résilience de la radiothérapie en cas d'interruption imprévue et prolongée de service.

9. Références

[1] CityNews Toronto. *Flooding damages London, Ontario hospital equipment* [Internet]. 24 juillet 2021. Disponible à l'adresse : 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]. 17 novembre 2021. Disponible à l'adresse : 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]. Irlande; 2021. Disponible à l'adresse : 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]. 24 novembre 2023. Disponible à l'adresse : 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]. 20 février 2024. Disponible à l'adresse : 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]. 1 novembre 2021. Disponible à l'adresse : https://globalnews.ca/news/8341284/newfoundland-labrador-healthcare-cyberattack/

[7] Centre canadien pour la cybersécurité. Centre canadien pour la cybersécurité. *Utiliser la gestion des informations et des événements de sécurité pour gérer les risques de cybersécurité (ITSM.80.024)* [Internet]. Gouvernement du Canada. Disponible à l'adresse : https://www.cyber.gc.ca/fr/orientation/utiliser-gestion-informations-evenements-securite-gerer-risques-cybersecurite-itsm80024

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

[9] Peters S, O'Donovan A, Bellini M, et coll. *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. Disponible à l'adresse : 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. Disponible à l'adresse : https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[12] Organisation mondiale de la Santé (2018). WHO guidance for business continuity planning. Organisation mondiale de la Santé. https://iris.who.int/handle/10665/324850. Licence : CC BY-NC-SA 3.0 IGO

[13] NHS England. *NHS England business continuity management toolkit*. Date de publication : 20 avril 2023; dernière mise à jour : 18 mai 2023. NHS England. *Business continuity management toolkit* [Internet]. 2023. Disponible à l'adresse : https://www.england.nhs.uk/publication/business-continuity-management-toolkit/

[14] Organisation internationale de normalisation (ISO). *ISO 22301:2019 Sécurité et résilience — Systèmes de management de la continuité d'activité — Exigences*. Genève : ISO; 2019. Disponible à l'adresse : https://www.bsigroup.com/fr-CA/products-and-services/standards/iso-22301-business-continuity-management/

[15] Groupe CSA. *CSA Z1600-17 (R2022): Programme de gestion des urgences et de la continuité* Toronto: Groupe CSA; 2017. Disponible à l'adresse : https://www.csagroup.org/fr/store/product/Z1600-17/

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

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

[18] Santé Ontario (Action Cancer Ontario). *Radiation Treatment Centres Emergency Preparedness MoU Checklist (v1.2)*. Toronto, Canada; mars 2023.

[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; mai 2020.

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

[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; décembre 2020.

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

[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;

13 mai 2021.

[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 [consulté le 1er juillet 2025] p. NIST SP 800-94. Numéro de rapport : NIST SP 800-94. Disponible à l'adresse : 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. Disponible à l'adresse : https://attack.mitre.org