VERS UNE APPROCHE PROPORTIONNELLE FONDÉE SUR LE RISQUE POUR L'ACCÈS AUX DONNÉES FÉDÉRÉES AU CANADA

TANIA BUBELA
REGIANE GARCIA
IVAN BESCHASTNIKH
ALINE TALHOUK

JUILLET 2023

CIFAR
Réflexions sur l'IA

À PROPOS DES AUTEURS

TANIA BUBELA

B. Sc. (Hons), Ph. D., JD, FCAHS, FRSC. Professeure et doyenne, Faculté des sciences de la santé, Université Simon Fraser

IVAN BESCHASTNIKH

B. Sc., M. Sc., Ph. D. Professeur agrégé, Département d'informatique, Université de la Colombie-Britannique

REGIANE GARCIA

LLB, LLM, Ph. D. Associée de recherche, Faculté des sciences de la santé, Université Simon Fraser

ALINE TALHOUK

B.A., M. Sc., Ph. D. Professeure adjointe et boursière Michael Smith en recherche en santé, Département d'obstétrique et de gynécologie, Faculté de médecine, Université de la Colombie-Britannique et Programme de recherche sur le cancer gynécologique et ovarien de la Colombie-Britannique (OVCARE).

REMERCIEMENTS

Les autrices et l'auteur souhaitent remercier les 47 spécialistes en éthique, protection de la vie privée, gouvernance et sécurité des données qui ont pris le temps, malgré leur horaire chargé, d'accorder un entretien dans le cadre de cette étude, ainsi que ceux et celles qui ont participé à l'atelier de validation et répondu au sondage en ligne. Nous souhaitons également remercier les assistantes et assistants de recherche qui ont participé aux entretiens, à l'analyse documentaire et à la préparation de cette note de breffage : Elise Abi Khalil (Université de la Colombie-Britannique), Mishaal Kazmi (Université de la Colombie-Britannique), Kalli Leung (Université de la Colombie-Britannique), Matheus Stolet (Université de la Colombie-Britannique) et Howard Zhang (Université Simon-Fraser).

RECONNAISSANCE DES TERRES

Nous reconnaissons les droits territoriaux des Autochtones sur les terres où le CIFAR est présent. Pendant des milliers d'années, ces terres ont été le territoire ancestral d'un grand nombre de peuples tels que les Mississaugas de la Credit, les Anishnabeg, les Chippewa, les Haudenosaunee et les Wendat, et abritent aujourd'hui diverses Premières Nations et populations inuit et métis. Nous sommes reconnaissants de pouvoir y établir le siège de nos activités. Nous sommes aussi conscients que la réconciliation est l'affaire de tous et de toutes. Le programme IA et société du CIFAR vise à enrichir notre compréhension des retombées sociétales de l'IA dans le but de poser les jalons d'une IA responsable. Et l'avenir de l'IA responsable passe par la prise en compte des préoccupations des communautés autochtones. Le CIFAR s'engage à privilégier le point de vue des peuples autochtones dans le développement et la conception d'une IA responsable.

TABLE DES MATIÈRES

Correspondance à
Aline Talhouk: a.talhouk@ubc.ca

RÉSUMÉ

Des algorithmes d'intelligence artificielle et d'apprentissage automatique sont en cours de développement pour une série d'applications dans le domaine de la santé, mais ils nécessitent des quantités massives de données pour reconnaître des formes cachées. Ces données sont souvent isolées dans différents sites et territoires, et il peut être difficile de les regrouper, de les conserver et d'y accéder en raison de préoccupations en matière d'éthique, de protection de la vie privée et de sécurité. L'apprentissage fédéré est un type émergent d'apprentissage automatique qui permet à plusieurs parties de collaborer à l'entraînement de modèles sans partager leurs données. L'apprentissage fédéré peut ainsi atténuer certains des problèmes de confidentialité, de sécurité et d'éthique généralement associés à la mise en commun des données pour l'apprentissage.

Dans cette note de breffage, nous explorons la manière dont l'apprentissage fédéré peut être mis en oeuvre. Notre analyse des 12 défis techniques et éthico-socio-juridiques et des possibilités d'action pour les consortiums d'apprentissage fédéré découle de la synthèse des analyses de quatre sources de données : une analyse documentaire, des entretiens avec des spécialistes, un atelier de validation et un sondage sur les solutions aux problèmes d'éthique, de sécurité et de protection de la vie privée soulevés par l'apprentissage fédéré. Nous formulons des possibilités d'action pour relever chaque défi.

Nous espérons ainsi aider les responsables politiques à comprendre les subtilités techniques et l'impact sociétal de l'apprentissage fédéré, une compréhension qui pourrait être améliorée par des discussions régulières avec des technologues, des spécialistes de l'éthique et du droit, et d'autres parties prenantes. Il sera essentiel qu'ils s'engagent auprès du public et des communautés concernées afin d'instaurer la confiance, d'obtenir de précieux commentaires et de veiller à ce que les bénéfices de l'apprentissage fédéré soient répartis équitablement. Nous soutenons que la mise en oeuvre des actions esquissées devrait faire l'objet d'une approche proportionnelle de l'évaluation des risques et des avantages potentiels des applications de l'apprentissage fédéré. Les responsables politiques devraient faciliter le développement d'un écosystème qui encourage l'innovation dans ce domaine tout en garantissant la protection de la vie privée des individus et la promotion du bien commun. Cela implique l'adoption d'une approche de la réglementation et de la gouvernance fondée sur le risque, c'est-à-dire que seules les applications à risque élevé feront l'objet d'un examen et d'une surveillance plus stricts. Les responsables politiques devront envisager des mécanismes pour favoriser la collaboration entre les secteurs public et privé, promouvoir la recherche technique et politique, et offrir des possibilités de formation et de dialogue à toutes les parties prenantes. La collaboration, aux niveaux national et international, sera cruciale pour partager l'expertise, atténuer les risques et établir des normes communes. Enfin, il est important de noter que l'apprentissage fédéré est un domaine qui évolue rapidement et que, par conséquent, les politiques et les cadres réglementaires devront être régulièrement réévalués et mis à jour pour les adapter aux avancées technologiques et aux nouveaux défis.

PRINCIPALES PRÉOCCUPATIONS POUR L'ÉLABORATION DE POLITIQUES

Dans cette note de breffage, nous examinons 12 défis techniques et éthico-socio-juridiques ainsi que des possibilités d'action pour les consortiums d'apprentissage fédéré. Nous abordons d'abord les questions liées à l'éthique, à la protection de la vie privée et à la gouvernance des données, puis les problèmes de sécurité.

ÉTHIQUE, PROTECTION DE LA VIE PRIVÉE ET GOUVERNANCE DES DONNÉES

1 PRÉOCCUPATIONS EN MATIÈRE DE PROTECTION DE LA VIE PRIVÉE DANS LE CADRE DE L'APPRENTISSAGE FÉDÉRÉ

Les données relatives à la santé sont protégées par un ensemble de lois sur la protection de la vie privée, ainsi que par les politiques et les pratiques des établissements ou des organisations qui reflètent les obligations fiduciaires des dépositaires de données à l'égard des personnes concernées. L'apprentissage fédéré pourrait atténuer les préoccupations en matière de protection de la vie privée, car seuls les modèles sont partagés, et les données ne quittent pas leur environnement sécurisé. Les possibilités d'action comprennent : élaborer des modèles de convention d'accès aux données pour l'apprentissage fédéré; mettre en oeuvre des procédures de plainte, de signalement, de décision et d'audit; adapter l'évaluation des facteurs relatifs à la vie privée et des préjudices éventuels en fonction d'une approche proportionnelle et fondée sur les principes; mettre à jour l'environnement législatif; mettre en oeuvre des régimes d'assurance ou d'indemnisation sans égard à la responsabilité pour les atteintes à la vie privée.

2 PROCÉDURES D'APPROBATION EN MATIÈRE D'ÉTHIQUE, DE PROTECTION DE LA VIE PRIVÉE ET D'ACCÈS AUX DONNÉES

Comme l'apprentissage fédéré est une technologie nouvelle et potentiellement perturbatrice, les lacunes des chercheurs et chercheuses relatives aux lois, aux politiques et aux pratiques peuvent altérer leur évaluation des risques des technologies en développement. De même, les personnes responsables des décisions en matière d'éthique, de protection de la vie privée et d'approbation opérationnelle peuvent ne pas disposer des compétences techniques et des

processus nécessaires pour évaluer les risques selon l'approche proportionnelle et atténuer les préjudices potentiels. Les possibilités d'action sont les suivantes : harmoniser les processus d'approbation; mettre en place des formations sur l'apprentissage fédéré pour les personnes responsables des décisions et sur les questions politiques, juridiques et éthiques pour la communauté de recherche; faciliter l'accès à l'expertise technique pour les personnes responsables des décisions; mettre en place des contrôles préalables et des certifications pour les solutions technologiques.

3 ENGAGEMENT DES PATIENTS, RESPONSABILISATION DES COMMUNAUTÉS ET ÉTABLISSEMENT OU MAINTIEN DE LA CONFIANCE

Une question déterminante pour l'avenir des modèles fédérés est leur capacité à assurer la souveraineté des données ainsi que l'autonomisation et la gouvernance des communautés, tout en atténuant les préjudices éventuels. Étant donné que les données ne quittent pas leur environnement local, il est possible d'engager davantage les patients et le public dans la gouvernance et l'utilisation des données. Des actions potentielles dans ce sens consistent à encourager les patients et les communautés à participer à la gouvernance des réseaux et des consortiums d'apprentissage fédéré et à échanger sur l'apprentissage fédéré, ses applications, ses risques et ses avantages. Il faudrait également examiner si l'apprentissage fédéré peut s'aligner sur les initiatives visant à renforcer la souveraineté des données pour les communautés et les organisations autochtones, mais cela nécessiterait un engagement et un renforcement des capacités des communautés et des organisations autochtones.

4 GOUVERNANCE DE L'INFRASTRUCTURE DE DONNÉES POUR L'APPRENTISSAGE FÉDÉRÉ

L'apprentissage fédéré implique l'utilisation de divers types de données anonymisées présentant différents niveaux de risque de réidentification. Le consentement est l'option privilégiée pour permettre l'utilisation et le partage de données à l'échelle interprovinciale ou internationale, car il offre la possibilité de retirer son consentement. Le consentement est un processus continu, et non une transaction ponctuelle, ce qui permet d'établir et de maintenir des relations de confiance. Nous abordons différents modèles de consentement en fonction de leur applicabilité : le consentement à la gouvernance, le consentement général, le consentement dynamique, le consentement de la communauté, la possibilité de retrait du consentement, la dispense de consentement, le consentement spécifique, le consentement historique et l'absence de consentement.

5 GOVERNANCE OF DATA INFRASTRUCTURE FOR FL

L'apprentissage fédéré pose des problèmes de gouvernance propres à la nature distribuée des données, mais il a le potentiel d'en régler d'autres. Les réseaux fédérés permettent à chaque site participant d'exercer un contrôle total sur ses données et de révoquer l'accès à tout moment. Les réseaux fédérés peuvent également faciliter la collaboration internationale, en permettant de surmonter certaines restrictions législatives et politiques sur la migration des données hors du Canada, mais seulement si rien n'empêche les utilisateurs hors d'un territoire d'accéder aux environnements locaux de données sécurisées. Les défis

de gouvernance suivants ont été abordés : les rôles et les responsabilités en matière de contrôle des données, la confidentialité des données, le couplage des données, la propriété des modèles et la validation des modèles. Les possibilités d'action sont les suivantes : être transparent dans le traitement des données et mettre en place des processus de responsabilisation; harmoniser les conventions sur le contrôle, l'accès et l'utilisation des données ainsi que les politiques et procédures dans tous les sites; élaborer des accords sur les possibilités d'exploitation commerciale ou de partenariat; déterminer à l'avance la contribution de chaque site.

6 SPECTRE DE L'ANONYMISATION ET DE L'IDENTIFIABILITÉ

La réidentification des données d'un site est un défi propre à l'apprentissage fédéré. Il s'agit de la possibilité de déterminer si un site particulier a participé à l'entraînement d'un modèle et de voir si les données de personnes déterminées sont utilisées par un site. La réidentification des données d'un site peut potentiellement compromettre la protection de la vie privée et la confidentialité des renseignements personnels des individus dont les données sont utilisées pour l'entraînement. Les possibilités d'action sont les suivantes : établir un guide des pratiques exemplaires d'anonymisation des données ainsi que des normes de classification et de traitement des données basées sur les risques liés à l'anonymisation; harmoniser les pratiques d'anonymisation des sites pour maintenir un risque proportionnel; élaborer et utiliser des clauses dans les contrats et les accords de licence, de collaboration ou de consortium qui interdisent l'utilisation des données à des fins de réidentification; légiférer sur les interdictions en établissant des sanctions; définir des mesures pour l'anonymisation des données et des modèles; exiger une taille minimale de cohorte pour la communication des résultats.

DÉFIS EN MATIÈRE DE SÉCURITÉ

1 CÉCITÉ DES DONNÉES

En apprentissage fédéré, le serveur central et les sites participants ont une visibilité limitée des données d'entraînement utilisées, ce qui peut compliquer le diagnostic et la résolution de problèmes liés à la qualité des données ou aux biais qui peuvent être induits. Faire collaborer et harmoniser des ensembles et structures de données distincts provenant de différents sites dans un modèle unique constituent également un défi, car il existe un risque accru que des données erronées soient utilisées. Les possibilités d'action sont les suivantes : harmoniser avec un modèle ou une norme de données commune au moyen de normes de gouvernance et de clauses contractuelles; collaborer avec des partenaires de confiance; mettre en oeuvre des contrôles de qualité locaux et mondiaux; auditer régulièrement les modèles; générer des résumés et des visualisations de données fédérées; partager des métadonnées; partager des données synthétiques différentiellement privées.

2 CYBERSÉCURITÉ

Une violation de sécurité se produit lorsque des personnes non autorisées accèdent à un système ou à des données sans permission, à la suite d'un piratage, de l'utilisation d'un logiciel malveillant, d'un hameçonnage ou de toute autre activité malveillante. Les violations de sécurité peuvent entraîner des atteintes à la vie privée. Les menaces liées à la cybersécurité sont réelles et peuvent avoir d'importantes répercussions sur les finances et la réputation des organisations. Les violations de sécurité dans le cadre de l'apprentissage fédéré peuvent être dues à trois causes, soit la sécurité du réseau, le contrôle des accès et la sécurité des modèles. Les possibilités d'action sont les suivantes : renforcer la sécurité du réseau; restreindre les accès non autorisés au modèle et utiliser des technologies de contrôle des utilisateurs; repérer les maillons faibles; créer des environnements de recherche sécurisés; surveiller et tester régulièrement la sécurité; utiliser des méthodes de chiffrement.

CONCLUSION

Alors que les menaces qui pèsent sur la sécurité, la protection de la vie privée et l'éthique de la recherche nécessiteront inévitablement certains développements techniques, nous soutenons que, pour les systèmes d'apprentissage fédéré, une approche proportionnelle et basée sur la gouvernance devrait prévaloir.

1.0 INTRODUCTION

Des algorithmes d'intelligence artificielle (IA) et d'apprentissage automatique sont en cours de développement pour une série d'applications dans le domaine de la santé. L'IA ouvre la porte à la médecine de précision, qui utilise des données pour prédire le meilleur traitement en fonction du profil génomique ou moléculaire des patients. L'IA s'impose également en reconnaissance d'images, de vidéos, de sons et de textes, permettant d'effectuer un diagnostic en temps réel et de prédire la probabilité d'apparition d'une maladie dans un délai donné. Les applications diagnostiques de l'apprentissage automatique pourraient améliorer la reproductibilité de l'évaluation humaine des images, par exemple en aidant un pathologiste à analyser l'imagerie médicale. Les applications en cours de développement comprennent la détection des dommages causés à la rétine par le diabète à partir de photographies1 et l'aide à la pathologie de qualité clinique pour divers cancers à partir de diapositives de tumeurs.[2,3,4,5,6,7]

Le potentiel clinique de l'apprentissage automatique dépend de l'accès aux importantes quantités de données recueillies par les systèmes de santé. Ces données sont souvent isolées dans différents sites et territoires, et il peut être difficile de les regrouper, de les conserver et d'y accéder en raison de préoccupations en matière d'éthique, de protection de la vie privée et de sécurité. L'apprentissage fédéré est une approche prometteuse en ce qui a trait à la gouvernance des données. Son utilisation pour entraîner des modèles peut atténuer certaines préoccupations, car il permet à plusieurs parties de collaborer à l'entraînement de modèles sans partager leurs données.[8] Plutôt que de regrouper les données dans un référentiel central, un algorithme d'apprentissage fédéré traite les données locales pour former un modèle global grâce à un réseau fédéré de centres de recherche.

Les conversations sur la fédération des données sont au coeur des aspirations canadiennes à accélérer l'amélioration des soins, de la performance des systèmes de santé et de la santé de la population dans le continuum des soins. Alors que le Canada vise à moderniser ses systèmes de santé avec des données sur la santé et des outils numériques normalisés[9], il est opportun de discuter de l'accès à ces données pour la recherche et l'innovation afin d'améliorer la santé des Canadiens. La fédération des sources de données est une étape importante pour maximiser la valeur des données, non seulement à des fins cliniques, mais aussi à des fins de recherche. Cela nécessitera l'élaboration de cadres politiques pour la collecte et le partage des données, la surveillance des données et la gouvernance dans les systèmes fédérés.

Dans cette note de breffage, nous explorons la manière de mettre en oeuvre l'apprentissage fédéré. Nous présentons les résultats de l'analyse documentaire, des entretiens avec des spécialistes, d'un atelier de validation et d'un sondage sur les solutions aux problèmes de protection de la vie privée, d'éthique et de sécurité soulevés par l'apprentissage fédéré. En évaluant les solutions aux défis potentiels, nous nous concentrons sur une réponse proportionnée aux risques avérés, en particulier la fréquence et l'ampleur des dommages causés par les atteintes à l'éthique, à la vie privée et à la sécurité des données sur la santé. Nous discutons des compromis entre les protections nécessaires et l'utilité des données dans le contexte de l'apprentissage fédéré et recommandons des modèles de gouvernance habilitants.

1.1

GOUVERNANCE DES MODÈLES REGROUPÉS ET DES MODÈLES FÉDÉRÉS

Actuellement, la plupart des algorithmes d'apprentissage automatique sont développés à l'aide de données regroupées dans un lieu central à partir de sites distribués (figure 1a). Ces données sont utilisées pour entraîner un modèle global, qui peut ensuite être partagé avec des collaborateurs pour être validé avec d'autres ensembles de données.[10] La gouvernance est centralisée et hiérarchique; l'établissement ou l'organisation responsable de l'hébergement établit les conditions d'entrée, d'accès et d'utilisation, car elle assume les risques associés à la protection des données contre les menaces à la vie privée et à la sécurité. Le regroupement des données est nécessaire, car il accroît la puissance de l'apprentissage automatique.

Cependant, une fois partagé, l'accès aux données est difficile à révoquer. Le regroupement de données peut s'avérer complexe d'un point de vue juridique.[11] Il nécessite des accords de partage de données ainsi que le respect du consentement et des lois sur la protection de la vie privée. De plus, sur le plan de la sécurité, il exige l'anonymisation des données sans perte d'exactitude, le contrôle de l'accès et la sécurité du transfert. Les intérêts commerciaux peuvent également limiter le regroupement de données, en particulier si l'agrégation ou la conservation des données leur donne une valeur ajoutée.

En revanche, avec l'apprentissage fédéré, un établissement ou une organisation coordonne la génération du modèle global (figure 1c). Les modèles peuvent être aussi performants que ceux entraînés avec des données regroupées ou encore partagés de pair à pair à plus petite échelle.[12] Le processus d'entraînement collaboratif du modèle global est itératif; il est développé à partir de modèles partiellement entraînés, développés localement, qui sont envoyés au coordonnateur central par intermittence à des fins d'agrégation. Seules les caractéristiques du modèle, telles que les paramètres et les gradients, sont partagées. L'entraînement du modèle global se poursuit jusqu'à ce que le modèle converge vers les données de l'ensemble des sites. Les données ne quittent jamais les sites protégés par des pare-feu, et aucune copie n'en est faite. Cependant, la coordination nécessite une structure de gouvernance hiérarchique pour le processus consensuel de développement du modèle global par les sites en réseau. L'apprentissage fédéré nécessite une capacité de calcul sur tous les sites, il peut y avoir des fuites renseignements personnels, et l'entraînement itératif peut prendre plus de temps. Les ententes juridiques peuvent être difficiles à négocier, et le champ d'application de la recherche et du développement reste incertain pour ce nouveau mode de développement technologique.

En résumé, l'apprentissage fédéré présente des avantages par rapport aux données regroupées, utilisées en apprentissage automatique.[13] Le principal avantage est que les données ne sont pas transférées ni partagées. L'apprentissage fédéré permet aux organisations d'exercer un plus grand contrôle sur la révocation de l'accès aux données, ce qui est difficile lorsque les données sont partagées. L'apprentissage fédéré est plus sûr et protège mieux la vie privée, car il est plus difficile pour des personnes malveillantes d'attaquer un système distribué, mais les fuites de renseignements ne peuvent jamais être totalement évitées. Les modèles partagés peuvent indirectement exposer des renseignements personnels sur la santé ou d'autres renseignements si des adversaires utilisent des processus de rétro-ingénierie. Les réseaux fédérés nécessitent des accords de consortium entre tous les sites participants, ce qui est plus difficile à négocier que les accords de partage de données entre pairs.

2.0

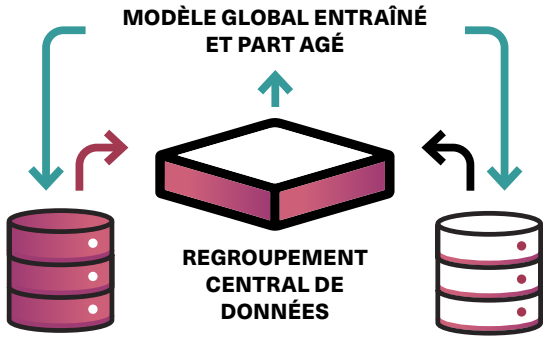
NOTRE APPROCHE ANALYTIQUE

Nous avons combiné trois méthodes de collecte de données pour analyser les défis techniques et éthico-socio-juridiques des consortiums d'apprentissage fédéré et les meilleures pratiques potentielles pour leur gouvernance.[i]

1. 43 entretiens avec des spécialistes en éthique de la recherche, en protection de la vie privée, en sécurité des réseaux et en gouvernance des données au Canada et dans le nord-ouest des États-Unis.[ii]
2. Une analyse documentaire des lois, des politiques, des dossiers juridiques et de la documentation.
3. Un atelier de validation virtuel avec 19 personnes et un sondage en ligne auprès de toutes les personnes interrogées.

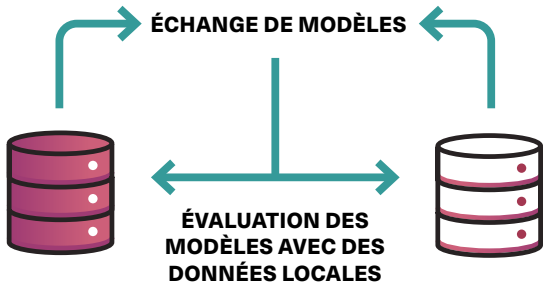
Alors que notre analyse s'appuie sur les avis de spécialistes et sur de la documentation, et non sur des délibérations publiques, nous recommandons toutefois de renforcer l'engagement du public. Par ailleurs, nos activités auprès de chercheurs et chercheuses autochtones ou de porte-parole des organisations autochtones de santé, de recherche et de données ont été minimales. Nous prenons note des problèmes importants liés à la souveraineté des données autochtones, mais il ne nous appartient pas de formuler des recommandations à ce sujet.

FIGURE 1A: REGROUPEMENT DES DONNÉES (ÉTAT ACTUEL DE LA PRATIQUE)



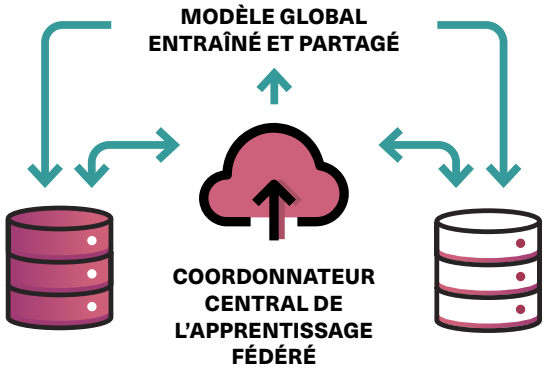
1. Regroupement des données des sites.
2. Accès à toutes les données du site commun.
3. Entraînement d'un modèle unique à partir des données regroupées.
4. Partage du modèle avec les collaborateurs.
   - Transfert de données des sites d'origine.
   - Gouvernance hiérarchique.

FIGURE 1B: PARTAGE DE MODÈLES DE PAIR À PAIR



1. Entraînement des modèles locaux avec des données locales.
2. Échange des modèles entraînés avec des collaborateurs.
3. Évaluation des modèles entraînés à partir des données locales de chaque site.
   - Pas de transfert des données des sites locaux.
   - Gouvernance distribuée.

FIGURE 1C: APPRENTISSAGE FÉDÉRÉ – SERVEUR D'AGRÉGATION



1. Sélection d'un coordonnateur central (par exemple, dans le nuage) qui développe unmodèle global et le distribue aux sites d'entraînement.
2. Envoi par intermittence des modèles partiellement formés par les sites au coordonnateur central pour agrégation.
3. Poursuite de l'entraînement itératif du modèle global renvoyé par le serveur central aux sites.
   - Pas de transfert des données des sites locaux
   - Gouvernance du réseau/consortium : le coordonnateur central, qui court le plus grand risque, devrait gérer les accords et leur négociation.

Veuillez noter qu'il peut y avoir plus de deux sites de données.

FIGURE 1

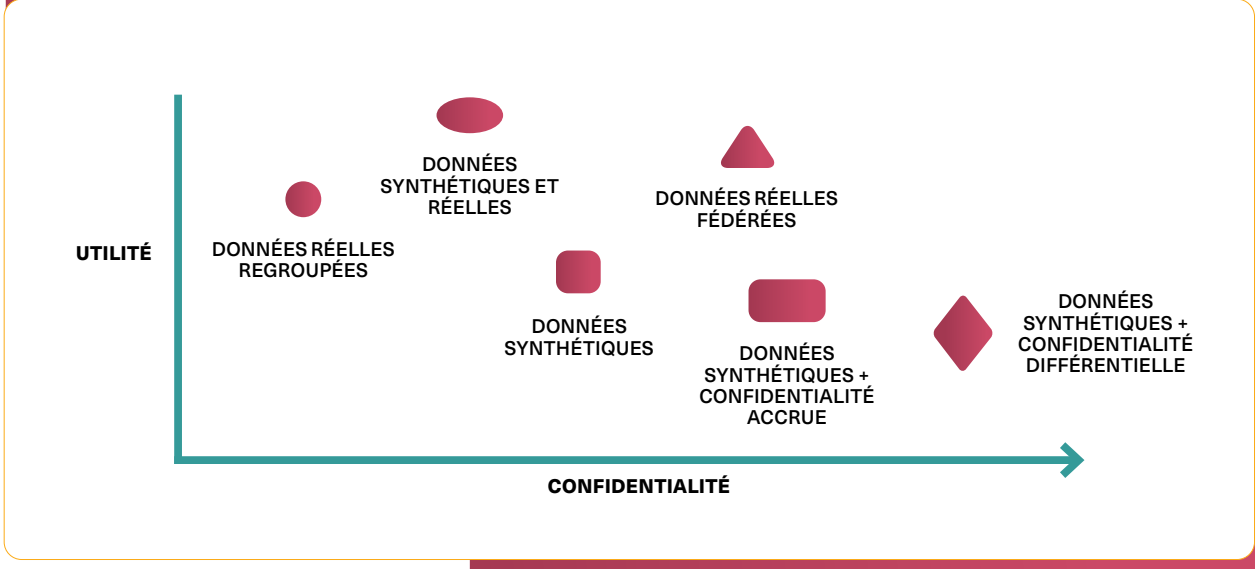
Trois modèles pour la formation des algorithmes d'apprentissage automatique : (a) le regroupement des données, où les accords de partage des données sont négociées avec le regroupement central de données; (b) le partage de modèles de pair à pair, où les accords de partage des modèles sont négociées entre les sites; (c) l'apprentissage fédéré, qui fonctionne mieux dans le cadre d'accords de réseaux ou de consortiums entre tous les sites; le coordonnateur central de l'apprentissage fédéré prend la direction des opérations, car il court le plus grand risque. Les flèches bleues représentent les modèles entraînés. Les flèches noires et blanches représentent le partage des données. Les silos représentent les sites locaux qui détiennent les données.

i Voir Notre approche analytique en détail Supplemental Methods pour une description complète de nos méthodes de collecte de données
ii Nous avons révisé les citations pour des raisons de longueur et de grammaire.

3.0 DISCUSSION

De nombreuses approches de protection de la vie privée en apprentissage automatique et en apprentissage fédéré sont en cours de développement, mais elles exigent toutes de faire certains compromis entre l'utilité et la confidentialité des données (figure 2). Outre la gouvernance, les solutions techniques comprennent l'utilisation de données synthétiques, l'entraînement avec des données cryptées, les cadres de confidentialité différentielle ou la combinaison de ces éléments.[14,15,16] Les données synthétiques, qui sont générées artificiellement par des modèles, imitent les propriétés statistiques des données du monde réel.[17] Elles permettent d'analyser et de manipuler des données sans compromettre la vie privée des individus.

FIGURE 2



Compromis entre confidentialité et utilité pour différents types de données, modèles de gouvernance et approches de protection de la vie privée.

La confidentialité différentielle est un cadre mathématique qui permet l'analyse de données sensibles tout en offrant une garantie mesurable de confidentialité (figure 3). Elle consiste à ajouter du bruit aux résultats d'un calcul. Ainsi, même si un pirate accède aux résultats, il ne peut déterminer quelles personnes font partie de l'ensemble de données original. Le bruit ajouté assure une plus grande confidentialité, mais il peut compromettre la précision du modèle. Ces approches de protection de la vie privée peuvent être difficiles à mettre à l'échelle en apprentissage fédéré, car elles génèrent des frais de communication et de calcul à chaque itération.

FIGURE 3

PLUS DE BRUIT = PLUS DE CONFIDENTIALITÉ

La confidentialité différentielle consiste à ajouter du bruit statistique pour créer un déni plausible, mais elle peut compromettre la précision du modèle.

Notre analyse envisage une réponse qui tient compte des compromis entre les mécanismes de protection de la vie privée et l'utilité du modèle. Nous abordons d'abord l'éthique, la protection de la vie privée et la gouvernance des données, puis les défis en matière de sécurité déterminés par notre analyse.

3.1

ÉTHIQUE, PROTECTION DE LA VIE PRIVÉE ET GOUVERNANCE DES DONNÉES

3.1.1 PRÉOCCUPATIONS EN MATIÈRE DE PROTECTION DE LA VIE PRIVÉE DANS LE CADRE DE L'APPRENTISSAGE FÉDÉRÉ

Les données relatives à la santé sont protégées par un ensemble de lois sur la protection de la vie privée ainsi que par les politiques et les pratiques des établissements ou des organisations

qui reflètent les obligations fiduciaires des dépositaires de données à l'égard des personnes concernées.[18] L'apprentissage fédéré pourrait atténuer les préoccupations en matière de protection de la vie privée, car les données ne sont pas partagées et ne quittent pas les environnements locaux sécurisés.[19] Seuls les modèles sont partagés.

La législation sur la protection de la vie privée, dans sa forme actuelle, n'a pas été conçue pour l'apprentissage fédéré ou d'autres initiatives de santé fondées sur les données massives. Les projets impliquant l'apprentissage fédéré doivent aborder les mêmes problèmes que tous les projets impliquant des renseignements personnels, et les comités d'éthique de la recherche (CER), les comités d'examen d'établissement (CEE) et les personnes responsables des décisions doivent appliquer les mêmes normes juridiques pour protéger les données sur la santé. Ces normes suggèrent que, pour protéger les personnes, les données doivent être minimales et non exhaustives, mais l'approche axée sur les données massives, utilisée pour l'IA, l'apprentissage automatique et l'apprentissage fédéré, consiste à recueillir toutes les données possibles. L'anonymisation des données, dont il est question ci-dessous, devient alors le modèle étalon.

Si l'évaluation des risques en matière de protection de la vie privée et d'éthique doit considérer que les préjudices éventuels doivent être proportionnés aux bienfaits espérés, certains préjudices peuvent être difficiles à mesurer. Certains préjudices sont simples, comme l'usurpation d'identité qui entraîne des pertes financières, mais d'autres sont plus intangibles. Les atteintes à la vie privée peuvent provoquer une perte de confiance des citoyens envers le système et la recherche, ce qui est difficile à mesurer. Certains domaines de recherche, tels que la génomique, ont porté attention aux risques pour la vie privée liés au partage de l'information génétique.[20] Ces principes peuvent également s'appliquer à d'autres formes de partage et d'analyse de données, telles que l'imagerie médicale.

Certains problèmes de confidentialité sont propres à l'apprentissage fédéré. Tout d'abord, les modèles partagés peuvent contenir des renseignements identifiables, tels que des renseignements personnels sur la santé, ce qui peut être considéré comme une atteinte à la vie privée. Deuxièmement, si les données synthétiques – des données générées artificiellement qui imitent les propriétés statistiques des données réelles – peuvent représenter une solution pour améliorer la protection de la vie privée, les méthodes qui fonctionnent le mieux sont probablement celles qui comportent le moins de contrôles de la protection de la vie privée lors de la génération des données synthétiques. Cela soulève le risque de fuite de données de patients réels dans des ensembles de données synthétiques et la capacité de déduire les données inconnues de patients réels à partir des données synthétiques en utilisant la similitude entre les patients des données synthétiques et les patients réels.

POSSIBILITÉS D'ACTIONS POUR PROTÉGER LA VIE PRIVÉE TOUT EN PERMETTANT L'APPRENTISSAGE FÉDÉRÉ

Élaborer des modèles de convention d'accès aux données pour l'apprentissage fédéré. Ces modèles pourraient faciliter l'utilisation et l'accès aux données locales en temps opportun. Ils devraient inclure des clauses de non-divulgation et de confidentialité des données, et interdire la réidentification. Les modèles pourraient accélérer les négociations et la conclusion d'accords de consortium ou de réseau et devraient avoir une portée internationale.

Mettre en oeuvre des procédures de dépôt de plainte des patients ou du public auprès d'un responsable déterminé, ainsi qu'un mécanisme de signalement et de décision en cas d'atteinte à la vie privée, conformément à

la loi. Les plaintes relatives aux atteintes à la vie privée peuvent être traitées différemment selon les organisations et les établissements, mais il doit exister une procédure claire quant au signalement des atteintes à la vie privée et au respect de la législation applicable en matière de protection de la vie privée pour informer les personnes concernées.

Adapter l'évaluation des facteurs relatifs à la vie privée de l'apprentissage fédéré en fonction d'une approche proportionnelle. Cela permettrait de passer d'une culture du protectionnisme à une culture de l'intendance des données en rendant les intendants de données responsables du cycle de vie entier des données, y compris leur utilisation et leur valeur.

Élaborer une approche fondée sur les principes pour les mesures de protection de la vie privée, en particulier pour les programmes de travail internationaux dont la législation en matière de protection de la vie privée est différente. Les préoccupations en matière de protection de la vie privée peuvent être atténuées si les données sont anonymisées, notamment en utilisant des principes de confidentialité différentielle[21,22] ou en générant des données synthétiques. La confidentialité différentielle dépend de la granularité des données et de la nature de la question posée. Cependant, les CER, les CEE et les personnes responsables des décisions en matière de protection de la vie privée ne sont pas encore familiers avec ces méthodes. L'autre solution consiste à instaurer la protection de la vie privée au moyen de la sécurité des données; dans cette optique, les modèles fédérés peuvent mieux protéger la vie privée.

Mettre à jour la législation et les politiques relatives aux applications de l'apprentissage automatique, de l'apprentissage fédéré et de l'intelligence artificielle, éventuellement avec une législation omnibus sur l'utilisation de la recherche et les sanctions en cas d'infraction. La législation sur la protection de la vie privée, dans sa forme actuelle, n'a pas été conçue pour l'apprentissage automatique ou d'autres initiatives en santé faisant appel aux données massives. Certaines lois provinciales font l'objet de réformes pour tenir compte de l'interaction entre les lois fédérales et provinciales et de la capacité à partager des données au-delà des limites de compétence, mais ces processus de réforme sont lents.

Réaliser des audits réguliers de la protection de la vie privée afin d'assurer la conformité aux cadres institutionnels et organisationnels de protection de la vie privée et de sécurité, combinés à un cadre de gestion et de déclaration des incidents. Les audits de protection de la vie privée constituent une pratique exemplaire et doivent permettre de retracer l'endroit où les chercheurs et chercheuses ont pris des données au fil de leurs déplacements d'un établissement à l'autre. À cela s'ajoutent des examens réguliers effectués par les commissaires à la protection de la vie privée des provinces ainsi que l'obligation de signaler au commissaire les atteintes non négligeables à la vie privée. Les commissaires à la protection de la vie privée peuvent fournir des conseils sur la manière de signaler et d'atténuer les atteintes à la vie privée et sur l'évaluation des facteurs relatifs à la vie privée.

Mettre en oeuvre des régimes d'assurance ou d'indemnisation sans égard à la responsabilité pour les atteintes à la vie privée. Les atteintes à la vie privée très médiatisées donnent lieu à des recours collectifs. La Cour d'appel de l'Ontario a statué en 2015 que la Loi sur la protection des renseignements personnels sur la santé[iii] n'était pas un code exhaustif quant aux mesures correctives en cas d'atteinte à la vie privée. Les plaignants pouvaient donc intenter un recours et

[iii] Loi sur la protection des renseignements personnels sur la santé, 2004, LO 2004, c 3, ann. A.
[iv] Hopkins v. Kay (2015) 124 O.R. (3d) 481.
[v] Jones v. Tsige (2012) 108 O.R. (3d) 241.

réclamer des dommages-intérêts en vertu de la common law pour le délit civil d'intrusion, qui comprend la violation du droit à la vie privée lors de l'accès non autorisé aux dossiers médicaux.[iv] Ce délit n'exige pas la preuve que les intérêts économiques du plaignant ont été affectés, ni que les renseignements personnels ont été publiés ou diffusés par le défendeur. Il se concentre sur l'acte d'intrusion par une conduite intentionnelle ou imprudente, sans justification légale, et sur le fait qu'une personne raisonnable considérerait l'intrusion comme un acte très offensant, qui cause de la détresse, de l'humiliation ou de l'angoisse.[v] Les règlements potentiels varient de 10 $ à 15 000 $ par personne. Pour éviter les procédures judiciaires, il serait possible d'établir un régime d'indemnisation progressif sans égard à la responsabilité pour les atteintes à la vie privée ou pour les instituts de recherche et les entreprises qui développent des modèles d'apprentissage fédéré afin de s'assurer contre les atteintes à la vie privée.

3.1.2 PROCÉDURES D'APPROBATION EN MATIÈRE D'ÉTHIQUE, DE PROTECTION DE LA VIE PRIVÉE ET D'ACCÈS AUX DONNÉES

L'apprentissage fédéré nécessite une collaboration entre différents sites ou territoires. Comme il s'agit d'une technologie nouvelle et potentiellement perturbatrice, les lacunes des chercheurs et chercheuses en ce qui a trait aux lois, aux politiques et aux pratiques peuvent altérer leur évaluation des risques des technologies en développement. De même, les personnes responsables des décisions en matière d'éthique, de protection de la vie privée et d'approbation opérationnelle peuvent ne pas disposer des compétences techniques et des processus nécessaires pour utiliser une approche proportionnelle de l'évaluation des risques et atténuer les préjudices potentiels.

POSSIBILITÉS D'ACTIONS POUR AMÉLIORER LES PROCESSUS D'APPROBATION

Harmonisation des processus. L'harmonisation des processus d'approbation est essentielle pour réduire les délais d'accès et d'utilisation des données qui comprennent des renseignements sur la santé.23 Si la question de l'harmonisation n'est pas propre à l'apprentissage fédéré, les structures fédérées amplifient la nécessité d'harmoniser les processus d'approbation et de prendre en compte l'interopérabilité juridique entre les institutions et/ou les territoires. Les processus d'approbation comprennent les approbations éthiques par les comités d'éthique de la recherche (CER) et les comités d'examen d'établissement (CEE), les évaluations des facteurs relatifs à la vie privée par les intendants de données et toutes les approbations opérationnelles pour l'utilisation des ressources des autorités de la santé. Des progrès ont été réalisés dans l'harmonisation des approbations éthiques, avec un CER responsable de l'évaluation, conformément à l'Énoncé de politique générale des trois conseils : Éthique de la recherche avec des êtres humains – EPTC-2 (2018). Les CER locaux prennent acte des conclusions et peuvent demander au CER responsable de reconsidérer sa décision à la lumière de circonstances locales ou de questions de fond non résolues.

Si l'harmonisation dans le domaine éthique progresse, l'examen des questions liées à la protection de la vie privée et à la sécurité est plus complexe. Les lois sur la protection de la vie privée ont été interprétées différemment par les organisations, et les travaux menés dans des contextes cliniques peuvent en outre nécessiter des approbations opérationnelles. La rationalisation et l'harmonisation des processus d'évaluation présentent l'avantage supplémentaire de permettre aux personnes responsables des décisions d'utiliser les mêmes renseignements et les mêmes critères d'évaluation.

Formation et éducation. L'apprentissage fédéré est une nouvelle technologie potentiellement perturbatrice et encore peu connue. Les personnes qui l'utilisent et celles qui sont responsables des décisions à son sujet n'ont pas toujours l'expertise nécessaire pour comprendre et gérer pleinement les risques. Le personnel en éthique et en recherche a besoin d'une formation continue sur les risques et les meilleures pratiques d'atténuation. Cette formation doit être adaptée aux différents contextes d'évaluation (éthique/protection de la vie privée/opérations). Il convient de s'attaquer aux mythes et aux idées fausses concernant la technologie. La formation peut aider la communauté de recherche à fournir de l'information claire et concise, rédigée de façon à être comprise des personnes responsables des décisions.

Accès à l'expertise technique. Les personnes responsables des décisions pourraient bénéficier de l'accès aux services-conseils de technologues. Les échanges avec des spécialistes qui connaissent le langage propre à différents domaines pourraient les aider à encourager une évaluation plus nuancée et plus complète de la technologie, à combler le fossé avec les différents protagonistes en protection de la vie privée et en sécurité, et à mieux comprendre les questions et les préoccupations auxquelles sont confrontés les intendants de données et les autorités sanitaires. Il convient de réfléchir à la manière de déployer ces technologues-conseils sans avoir à les nommer officiellement au sein des CER et des CEE.

Contrôles et certifications préalables. Une procédure d'évaluation préalable pour les comités d'éthique pourrait garantir que les détails et les points de détail ont été soigneusement examinés avant que la technologie ne soit présentée au CER ou au CEE. Une certification peut fournir une assurance supplémentaire que la technologie a été soumise à des tests rigoureux et qu'elle répond à certaines normes de sécurité. Les approches peuvent être vérifiées au préalable par un groupe de spécialistes, y compris une analyse de l'architecture proposée et de la manière dont elle sera gérée dans chacun des sites d'entraînement, car le comité d'éthique n'a pas besoin de comprendre ce niveau de détail. Enfin, il existe des méthodes formelles pour prouver que les systèmes ont été conçus et construits de manière sûre. Ces méthodes permettent de générer des certifications pour la mise en oeuvre des systèmes.

3.1.3 ENGAGER LES PATIENTS, RESPONSABILISER LES COMMUNAUTÉS ET ÉTABLIR OU MAINTENIR LA CONFIANCE

Une question déterminante pour l'avenir des modèles fédérés est leur capacité à assurer la souveraineté des données ainsi que l'autonomisation et la gouvernance des communautés, tout en atténuant les préjudices éventuels. Étant donné que les données ne quittent pas leur environnement local, il est possible d'engager davantage les patients et le public dans la gouvernance et l'utilisation des données.[24]

Il est essentiel de communiquer avec les patients et les communautés, et de leur donner les moyens d'agir, afin de favoriser « l'acceptabilité sociale » en faisant bon usage de leurs données et en établissant ou en maintenant la confiance.[25,26] La confiance est difficile à gagner, et encore plus difficile à regagner une fois perdue. Cette situation est exacerbée par un climat de méfiance à l'égard de la science, une perception qui a été amplifiée par la pandémie et les médias sociaux. Les processus d'engagement doivent donc rester apolitiques ou non partisans.

Jusqu'à présent, la collecte et l'utilisation des données massives ont été essentiellement le fait d'un petit groupe à la tête du secteur de la santé. Les patients et le public sont généralement favorables à l'utilisation des données à des fins de recherche. Par exemple, un sondage réalisé en décembre 2013 indique qu'« une grande majorité de la population de la Colombie-Britannique est prête à consentir aux recherches sur leurs renseignements sur la santé, à la condition que les dossiers soient anonymes ». [27] Il est temps de mettre en place des plateformes inclusives pour les délibérations publiques et d'inclure des voix diverses dans les structures de gouvernance des données.

POSSIBILITÉS D'ACTIONS POUR ENGAGER LE PUBLIC

Encourager les patients et les communautés à participer à la gouvernance. Nous devons responsabiliser les personnes représentées dans les ensembles de données, comme les communautés de personnes atteintes de maladies rares. Les partenaires, qu'ils soient citoyens ou patients, peuvent participer aux comités de données et de recherche ou à la recherche elle-même, et certains peuvent avoir une compréhension suffisante des technologies pour apporter des contributions significatives.[28] Dans son document de consultation, la Stratégie pancanadienne de données sur la santé réclame une assemblée citoyenne et d'autres délibérations publiques, et les agences et réseaux de santé fédéraux connexes disposent de conseils consultatifs publics. Il existe des modèles d'engagement public ou citoyen et de forum de délibération, et leur nécessité est devenue évidente partout au Canada. Toutefois, l'approche est

désorganisée et non collaborative, et les questions posées sont parfois trop pointues ou trop axées sur la protection de la vie privée. L'engagement a l'avantage de joindre les intérêts des patients et de les amener à contribuer à l'élaboration de cadres et de processus appropriés. Les patients et les communautés peuvent en outre être consultés dans le cadre de développements législatifs ou de réformes réglementaires concernant la recherche et d'autres utilisations des données.[29,30,31,32]

Favoriser les échanges sur l'apprentissage fédéré, ses applications, ses risques et ses avantages. Quelle que soit la manière dont les données sont partagées, y compris au moyen de systèmes fédérés, il est nécessaire de faire preuve de transparence au sujet des normes d'anonymisation et de mettre en place des mesures dissuasives importantes contre la réidentification afin d'instaurer et de maintenir la confiance. De même, il est nécessaire de faire preuve de transparence au sujet des utilisations commerciales potentielles des données, des conflits d'intérêts et des retombées, le cas échéant. Les patients et les membres du public peuvent hésiter davantage à permettre l'utilisation de leurs données à des entités commerciales ou transfrontalières. Les utilisations commerciales font craindre que la technologie soit exclusive, coûteuse ou accessible uniquement à certains segments de la population. Ces questions, liées à la justice distributive, réduisent la confiance.[33,34,35,36]

Il est également nécessaire de faire preuve de transparence au sujet des hypothèses et des performances des modèles sous-jacents, qui peuvent ne pas être validés et qui sont susceptibles de générer des inégalités ou des stéréotypes.[37,38,39,40,41] Les biais inhérents aux points de collecte de données et de partage des données, au type de données partagées et à leur granularité, aux algorithmes eux-mêmes et à l'utilisation de ces algorithmes peuvent entraîner des risques éthiques à chaque étape du processus.

Examiner si l'apprentissage fédéré peut s'aligner sur les initiatives visant à renforcer la souveraineté des données pour les communautés et les organisations autochtones. Cet examen nécessitera un engagement et une reconnaissance des concepts fondamentaux des droits inhérents et collectifs, protégés par la Constitution et de plus en plus reconnus par les lois et les traités internationaux (Haut-Commissariat des Nations Unies pour les réfugiés, non daté), ainsi que des principes de propriété, de contrôle, d'accès et de possession, connus sous le nom de PCAP®, qui « affirment que les Premières Nations sont les seules à contrôler les processus de collecte de données dans leurs communautés, et qu'elles possèdent et contrôlent la manière dont ces informations peuvent être stockées, interprétées, utilisées et partagées ».[42]

3.1.4 CONSENTEMENT À L'APPRENTISSAGE FÉDÉRÉ

L'apprentissage fédéré implique l'utilisation de vastes ensembles de données disparates et anonymisées qui présentent des risques variables de réidentification.43 Les renseignements personnels sur la santé auxquels il est possible d'accéder pour l'apprentissage fédéré peuvent généralement être classés en deux catégories : certaines données font l'objet d'un consentement pour leur collecte, leur accès et leur utilisation alors que d'autres sont accessibles à des fins de recherche en vertu de la loi. Le consentement est l'un des mécanismes qui permettent la circulation ou l'utilisation des données à l'échelle interprovinciale ou internationale. Toutefois, le processus de consentement pose des problèmes en raison de la complexité du langage utilisé et de l'ambiguïté des risques énoncés.44 Malgré la nécessité de simplifier les documents de consentement, la demande de consentement est privilégiée, car elle offre une possibilité de retrait du consentement. Le consentement est un processus continu, et non une transaction ponctuelle, ce qui permet d'établir et de maintenir des relations de confiance.

TABLEAU 1

MODÈLES DE CONSENTEMENT CLASSÉS PAR ORDRE D'APPLICABILITÉ À L'APPRENTISSAGE FÉDÉRÉ

1

CONSENTEMENT À LA GOUVERNANCE

Les personnes consentent à ce que leurs données soient gérées par l'établissement ou l'organisation qui les héberge. Le modèle de gouvernance et le cadre décisionnel relatifs à l'accès aux données et à leur utilisation sont décrits dans le formulaire de consentement, qui comprend également de l'information sur la collecte et le stockage des données ainsi que sur la structure et la représentation du comité qui prend les décisions relatives à l'accès aux données et à leur utilisation. Le comité peut comprendre des membres du public ou des patients. Les individus peuvent retirer leurs données préalablement, mais ils ne sont pas contactés à chaque nouvelle utilisation.

2

CONSENTEMENT GÉNÉRAL

Les personnes consentent à un large éventail d'utilisations futures des données, et ce, par divers acteurs, y compris ceux de l'industrie. L'EPTC-2 a récemment entrepris une consultation sur la question du consentement général, notamment sur la quantité de renseignements nécessaires pour obtenir le consentement et sur les limites éventuelles des utilisations futures des données.

3

CONSENTEMENT DYNAMIQUE

Les personnes ont la possibilité de consentir à des projets de recherche particuliers et de retirer leur consentement. Cette option optimise l'autonomie du participant et crée une relation continue. Cette approche est la plus transparente et permet d'instaurer la confiance. Le consentement dynamique peut être mis en oeuvre à l'aide de technologies telles que la chaîne de blocs, notamment pour les biobanques qui contiennent des données omiques.[45,46,47]

4

CONSENTEMENT DE LA COMMUNAUTÉ

Dans certaines circonstances, il peut être plus approprié de demander le consentement des communautés ou des organisations communautaires qui représentent les intérêts des individus au sein de ces communautés.[48]

5

RETRAIT DU CONSENTEMENT

Les données sur la santé des individus sont recueillies régulièrement et utilisées à des fins de recherche, à moins que les individus ne décident expressément de les exclure. Ce type de consentement permet d'accroître la participation et la représentativité, mais diminue l'autonomie des patients. Dans un système de santé publique, on s'attend à ce que les données des patients soient utilisées pour améliorer le système. Certains hôpitaux disposent d'un programme de retrait et en informent les patients lors de leur inscription à l'hôpital.

6 DISPENSE DE CONSENTEMENT

Les chercheurs peuvent demander une dispense de consentement pour l'utilisation secondaire de données sur la santé, ce qui peut impliquer un transfert d'autorité du responsable de la recherche au dépositaire/intendant des données de l'établissement ou de l'organisation. Les demandes de dispense sont évaluées par les comités d'éthique et les dépositaires/intendants des données, conformément à la législation et aux politiques. Souvent, les données ne peuvent pas quitter le site où elles sont stockées, et les analyses doivent être effectuées en toute sécurité. Seules les analyses peuvent quitter le site, et non les données d'origine. Dans certains endroits, les données peuvent être consultées dans plusieurs territoires, mais elles sont gérées de façon centralisée dans une installation sécurisée, et une équipe interne nettoie les données.[49]

7 CONSENTEMENT SPÉCIFIQUE

Certaines études reposent sur un consentement spécifique. Ce dernier ne s'étend pas au-delà de l'utilisation des données dans le cadre d'une étude particulière ou d'activités spécifiques dans le cadre d'une initiative plus large de production de données. Par exemple, les personnes qui participent à un essai clinique peuvent donner leur accord pour que leurs données soient couplées à des données administratives sur la santé.

8 CONSENTEMENT HISTORIQUE

Les données patrimoniales doivent être gérées conformément aux consentements spécifiques obtenus au moment de leur collecte, ce qui peut nuire à leur utilité et à la possibilité de couplage ou d'utilisation dans des contextes fédérés. Les contraintes historiques peuvent être surmontées dans certains cas si l'utilisation secondaire des données peut justifier la dispense de consentement. Les consentements historiques peuvent limiter l'utilisation internationale ou commerciale des données, qui doit faire l'objet d'un consentement spécifique.

9 ABSENCE DE CONSENTEMENT

Il est nécessaire de clarifier la distinction entre l'utilisation des données pour l'amélioration du système de santé ou l'évaluation des programmes et la recherche. Les données peuvent également être recueillies et utilisées sans consentement à des fins légales comme la surveillance de la santé publique, mais l'absence de consentement et les contraintes juridiques limitent leur utilisation. L'utilisation de certaines données qui sont accessibles au grand public ne nécessite pas de consentement.

3.1.5 GOUVERNANCE DE L'INFRASTRUCTURE DE DONNÉES POUR L'APPRENTISSAGE FÉDÉRÉ

L'apprentissage fédéré pose des problèmes de gouvernance propres à la nature distribuée des données, mais il a le potentiel d'en régler d'autres.[50] L'approche fédérée permet la création de fiducies de données virtuelles sans qu'il soit nécessaire de regrouper les données dans des plateformes en silos qui attirent les pirates informatiques (figure 1). Elle pourrait aussi faciliter la collaboration internationale, en permettant de surmonter certaines restrictions législatives et politiques sur la migration des données sur la santé hors du Canada, mais seulement si l'accès aux environnements locaux de données sécurisées n'est pas limité. Les obstacles à l'accès aux données sont dus aux multiples niveaux de responsabilité et à la complexité des mécanismes d'approbation.

De nombreuses initiatives sont en cours pour améliorer l'infrastructure numérique de la santé au Canada et faciliter l'accès aux données. Dans le présent document, la discussion est limitée aux défis de gouvernance propres à l'apprentissage fédéré, qui comprennent les éléments suivants.

Rôles et responsabilités en matière de contrôle des données. Pour l'apprentissage fédéré, les données sont réparties entre plusieurs sites, qui peuvent avoir des structures de gouvernance différentes et être soumis à des régimes juridiques différents (figure 1c).[51] Par conséquent, les rôles et les responsabilités en matière de contrôle des données et de leur utilisation pour l'entraînement, ainsi que le champ d'application et la responsabilisation peuvent être mal définis ou contradictoires. Le rôle des intendants de données ne devrait pas être d'évaluer la valeur de la recherche, mais de déterminer si les données peuvent être diffusées en toute sécurité, parce que d'autres organes de gouvernance et d'approbation de l'évaluation de la qualité ont déterminé que des protections étaient en place.

Confidentialité des données. Étant donné que l'apprentissage fédéré implique l'entraînement de modèles à partir de données réparties entre plusieurs sites, il est important de veiller à ce que la confidentialité des données soit protégée, mais que cette protection soit équilibrée par rapport à l'utilisation des données à des fins de santé publique ou d'utilité sociale. La protection de la vie privée peut être assurée par des mécanismes de gouvernance appropriés, mais aussi par les moyens technologiques évoqués plus loin. Les défis en matière de gouvernance peuvent découler d'une culture du protectionnisme dans un contexte de protection de la vie privée. Toutefois, des contrôles peuvent être mis en place au niveau des données; ces dernières pourraient être soumises à différents critères d'accès en fonction de leur sensibilité et des modalités de consentement.

Couplage des données. La mise en relation des données est confrontée à de nombreux défis, dont de multiples lois habilitantes, accords et niveaux de responsabilité, une infrastructure inadéquate pour le partage, le transfert ou le couplage des données entre le milieu de la recherche et le milieu clinique, et le manque de financement, aggravé par la lourdeur des processus.

Propriété des modèles. Dans le cas de l'apprentissage fédéré, comme plusieurs parties contribuent à l'entraînement du modèle, il peut être difficile de déterminer l'identité du propriétaire du produit final, ce qui soulève d'autres difficultés en ce qui a trait aux droits de propriété intellectuelle et aux contrats de licence.

Validation des modèles. Étant donné que l'apprentissage fédéré implique l'entraînement de modèles à partir de données distribuées, il peut être difficile de valider la précision et la fiabilité des modèles obtenus. Cela nécessite donc de nouvelles techniques de validation et de test des modèles.

POSSIBILITÉS D'ACTIONS

Être transparent et informer les patients et le public. Les systèmes d'apprentissage fédéré qui utilisent des données sensibles doivent être transparents quant à leurs pratiques de traitement des données et mettre en place des processus de responsabilité appropriés. Il est important d'informer les patients et le public au sujet des données recueillies, de leur utilisation et de la protection de la vie privée.[52]

Harmoniser les conventions de contrôle, d'accès et d'utilisation des données. L'harmonisation des conventions permet de garantir que les données sont accessibles et utilisées de manière cohérente et sûre dans tous les sites. Les conventions d'utilisation et de transfert des données devraient prévoir des contrôles distincts en matière de confidentialité selon le type et la sensibilité des données. Dans le cadre d'une évaluation de la protection de la vie privée, les données devraient être divisées en niveaux d'identifiabilité auxquels seraient associés des types d'accès, avec des règles claires établissant qui peut y avoir accès et dans quelles conditions.[53] Les plans normalisés de gestion de l'accès aux données permettent à différents groupes d'appliquer différentes approches d'apprentissage automatique au même ensemble de données et de comparer les modèles, mais ces plans peuvent être difficiles à négocier entre différentes compétences territoriales. Toutefois, il est possible d'utiliser un langage hybride pour tenir compte des variations dans les dispositions relatives à la protection de la vie privée et des références à ces dispositions. L'accord doit être rédigé dans l'intérêt de la partie sur laquelle pèse le risque le plus élevé.

Adopter des politiques et des procédures harmonisées dans tous les sites. Il importe d'élaborer et de mettre en oeuvre des politiques et des procédures normalisées pour le développement des modèles dans tous les sites participants, y compris des lignes directrices pour la collecte et le partage des données, ainsi que pour l'entraînement des modèles. Cette normalisation peut être soumise à certaines contraintes découlant de la nécessité de prendre en compte les politiques et procédures locales conformes aux lois.

Élaborer des accords en vue d'une utilisation commerciale potentielle ou de l'établissement de partenariats. Ces accords comprennent des directives en matière de conflits d'intérêts, de propriété intellectuelle, de stratégies de commercialisation et de retombées pour les individus ou la communauté, sinon pour le système.

Déterminer à l'avance les contributions de chaque sites. Afin de s'assurer que chaque site est rémunéré de manière appropriée pour ses contributions, ce qui favorise la confiance et la coopération.

3.1.6 SPECTRE DE L'ANONYMISATION ET DE L'IDENTIFIABILITÉ

La réidentification des données d'un site est un défi propre à l'apprentissage fédéré. Il s'agit de la possibilité de déterminer si un site particulier a participé à l'entraînement d'un modèle et de voir si les données de personnes déterminées sont utilisées par un site.54 La réidentification des données d'un site peut potentiellement compromettre la protection de la vie privée et la confidentialité des rensei-

gnements personnels des individus dont les données sont utilisées pour l'entraînement. Les questions qui se posent sont les suivantes : que signifie l'anonymisation dans un système fédéré de gouvernance des données? L'approche fédérée atténue-t-elle ou augmente-t-elle les risques, par exemple en raison d'incohérences dans les normes d'anonymisation ou encore de possibilités accrues de combiner des données de manière à favoriser la réidentification? Quel niveau d'anonymisation est approprié pour que les données puissent convenir aux utilisations proposées?

POSSIBILITÉS D'ACTIONS

Établir un guide des pratiques exemplaires d'anonymisation des données ainsi que des normes de classification et de traitement des données basées sur les risques liés à l'anonymisation. L'anonymisation des données est une bonne pratique, mais les sites ne le font pas tous de la même manière. Les incohérences peuvent créer des problèmes si des données qui proviennent de différents endroits sont combinées. Les CER peuvent leur venir en aide, car ils appliquent des lignes directrices et des règles normalisées pour la recherche avec des êtres humains en fonction du niveau d'identifiabilité des données et déterminent s'il est possible d'avoir une dispense de consentement.

La plupart des centres déploient des efforts considérables pour anonymiser les données, par exemple en supprimant l'en-tête des images médicales et les noms des patients, en brouillant les visages des IRM par un traitement élaboré des images. Malgré ces mesures, l'accès à de multiples variables peut permettre une réidentification.

Les métadonnées peuvent poser des problèmes supplémentaires d'anonymisation. Par exemple, les images comprennent des champs de données qui peuvent contenir de l'information sensible en raison d'une erreur humaine. Des systèmes doivent être mis en place pour détecter ces erreurs.

Harmoniser les pratiques d'anonymisation des sites pour maintenir un risque proportionnel. Les pratiques au sein des réseaux fédérés doivent équilibrer le rapport entre le risque et l'utilité de l'anonymisation, ce qui peut nécessiter de nouvelles méthodes d'anonymisation, notamment :

- La suppression des renseignements personnels permettant l'identification;
- L'application de méthodes de confidentialité différentielle en ajoutant du bruit aux données, ce qui complique l'établissement d'un lien entre des points de données individuels et des personnes précises (figure 2). On ne sait pas encore comment les CER et les CEE ainsi que les évaluations des exigences en matière de confidentialité tiendront compte de ces méthodes;
- L'utilisation de contrôles des données à la sortie, qui peuvent être plus utiles pour les statistiques descriptives et les produits statistiques tels que les modèles de régression;
- Des méthodes d'analyse du risque de réidentification permettant d'évaluer si les données sont sûres et de documenter la justification de ce jugement avant que les produits ne quittent l'environnement;
- La suppression de l'information sensible qui peut être associée à des personnes;
- L'exigence d'une taille minimale de cohorte pour la communication des résultats;
- La définition de paramètres pour mesurer la probabilité d'une réidentification potentielle par un pirate..

Élaborer et utiliser des clauses dans les contrats et les accords de licence, de collaboration et de consortium qui interdisent l'utilisation des données à des

fins de réidentification afin de renforcer les interdictions législatives existantes ou améliorées en matière de réidentification.

3.2

DÉFIS EN MATIÈRE DE SÉCURITÉ

3.2.1 CÉCITÉ DES DONNÉES

En raison de la nature distribuée de l'apprentissage fédéré, il peut être difficile de garantir la qualité et l'intégrité des données. En apprentissage fédéré, le serveur central et les sites participants n'ont aucune visibilité de l'ensemble des données utilisées pour entraîner le modèle (cécité des données).55 Les sites ne sont donc pas en mesure d'accéder directement aux données d'entraînement des autres sites ou de les analyser, ce qui complique le diagnostic et la résolution des problèmes liés à la qualité des données ou aux biais qui peuvent être induits. Comme les sites participants ont des ensembles et des structures de données distinctes, la collaboration en vue d'harmoniser les données dans un modèle unique est plus difficile. En outre, la répartition des sites augmente le risque que des données erronées soient introduites dans le système..[56,57]

POSSIBILITÉS D'ACTIONS

Harmoniser avec un modèle ou une norme de données commune au moyen de normes de gouvernance et de clauses contractuelles..

Collaborer avec des partenaires de confiance afin d'atténuer le risque d'empoisonnement des données.

Mettre en oeuvre des contrôles de qualité locaux et mondiaux qui peuvent analyser les données sans les observer directement.

Auditer régulièrement les modèles pour en évaluer la qualité.

Générer des résumés et des visualisations de données fédérées, qui peuvent donner un aperçu de la distribution des données et aider à repérer les biais potentiels ou les problèmes de qualité des données. [58]

Partager les métadonnées, qui peuvent éclairer la conception du modèle et les questions de qualité.

Partager des données synthétiques différentiellement privées. Les données synthétiques, qui sont générées artificiellement par des modèles, imitent les propriétés statistiques des données du monde réel. Toute fuite de renseignements personnels peut être atténuée par une confidentialité différentielle.59,60 Bien que ces techniques puissent réduire l'utilité des données, elles devraient toujours permettre l'exploration de données, l'harmonisation et d'autres actions de haut niveau.

3.2.2 CYBERSÉCURITÉ

Une violation de sécurité se produit lorsque des personnes non autorisées accèdent à un système ou à des données sans permission, à la suite d'un piratage, de l'utilisation d'un logiciel malveillant, d'un hameçonnage ou de toute autre activité malveillante. Les violations de sécurité peuvent entraîner des atteintes à la vie privée.61 Les menaces à la cybersécurité sont réelles et peuvent avoir d'importances répercussions sur les finances et la réputation des organisations. Certaines formes de menaces, telles que les attaques par rançongiciel contre les établissements de santé, ont plus que doublé de 2016 à 2021 aux États-Unis.62,63 Cependant, la plupart des violations de sécurité sont dues à des erreurs humaines, comme un accès aux données ou un stockage inapproprié, ou une mauvaise configuration du système. Dans le contexte de l'apprentissage fédéré, les violations de sécurité peuvent être causées par :

- Sécurité du réseau : En apprentissage fédéré, l'entraînement des modèles se fait à travers un réseau. À chaque itération du processus d'entraînement, des données sont partagées entre les sites participants et le coordonnateur central. Le risque de violation n'est pas plus élevé que dans d'autres variantes de l'apprentissage automatique; en fait, l'apprentissage

fédéré peut atténuer le risque de violation grâce à l'utilisation de protocoles de communication sécurisés. Toutefois, les risques peuvent découler des problèmes suivants :

- Accès non autorisés au modèle : Il se peut que le modèle final entraîné par apprentissage fédéré doive être déplacé sur un autre site du réseau, ce qui augmente le risque de fuites ou d'accès non autorisés. Pendant l'entraînement, le modèle peut être partagé avec les sites participants, et il faut avoir confiance que les sites ne compromettront pas le modèle ou ne feront pas d'ingénierie inverse des données personnelles au moyen du processus d'inversion de modèle.[64]

- Coût de l'entraînement sur un réseau fédéré de plusieurs sites en raison d'une largeur de bande ou d'une puissance de calcul insuffisante.[65]

- Maillon faible : L'apprentissage fédéré implique de nombreuses parties, que ce soit les propriétaires de données, les clients et le serveur central, qui doivent toutes coopérer pour garantir la sécurité du système. La sécurité de l'ensemble du réseau fédéré peut être compromise par un seul maillon faible. [66]

POSSIBILITÉS D'ACTIONS

Contrôle des accès et authentifications. En apprentissage fédéré, les sites collaborateurs n'accèdent pas directement aux données, mais soumettent une requête qui est distribuée aux sites, exécutée localement sur chaque site et dont les résultats sont ensuite publiés. Un aspect essentiel de la gouvernance consiste à déterminer qui peut soumettre des requêtes et accéder aux résultats, et à évaluer le niveau de risque que représentent ces collaborateurs. Les niveaux de confiance sont continuellement contrôlés et déterminés au moyen d'un modèle de gouvernance convenu au départ, qui dicte les procédures d'accès et leur application. Les contrôles d'accès, qui comportent une authentification multifactorielle, restreignent l'accès au modèle aux utilisateurs et sites autorisés. Les contrôles peuvent être ajustés pour permettre des utilisations particulières du modèle final qui atténuent le gain d'information sur le modèle sous-jacent.

Bac à sable et environnements de recherche sécurisés. Ces méthodes fournissent des contrôles à l'entrée et à la sortie, et ne permettent pas aux données de sortir si les vulnérabilités aux points d'entrée et de sortie des requêtes sont bien protégées.67 C'est le modèle employé par la plupart des centres de données fédéraux et provinciaux au Canada, tels que l'Institut canadien d'information sur la santé (ICIS), l'Institut de recherche en services de santé de l'Ontario (ICES) et le Population Data British Columbia (PopData BC).[vi]

Surveillance régulière. Cette pratique courante est essentielle pendant l'entraînement du modèle pour assurer sa sécurité et sa fiabilité, notamment lors d'un fonctionnement sans interruption pendant de longues périodes.68 De nombreux problèmes, tels que les pannes de réseau ou les problèmes de performance, peuvent être détectés par l'infrastructure de surveillance. Cependant, la surveillance de plusieurs sites est un défi, car les sites appartiennent à des administrations différentes. La surveillance permet de détecter les accès non autorisés et les activités suspectes et devrait se concentrer sur les points d'entrée du réseau.

Tests d'intrusion. Des concours et des événements au cours desquels des étudiants et des spécialistes tentent de percer le système peuvent aider à repérer les vulnérabilités, à améliorer la sécurité et à protéger les données sensibles.[69]

Chiffrement. Les méthodes de chiffrement, comme le chiffrement homomorphe, permettent d'effectuer des calculs sur des données chiffrées sans avoir à les déchiffrer, ce qui renforce la sécurité.[70]

[vi] CIHI - https://www.cihi.ca/
ICES - https://www.ices.on.ca/
PopulationData BC - https://www.popdata.bc.ca/

4.0 CONCLUSION

L'apprentissage fédéré s'annonce très prometteur pour le développement des technologies de la santé au bénéfice des patients, des systèmes de santé et de l'écosystème de l'innovation en matière de santé au Canada. Il permet à plusieurs parties de collaborer à l'entraînement de modèles sans partager les données ni les regrouper dans un référentiel central. Jusqu'à présent, le débat public a surtout porté sur la protection des données. Il est temps d'entamer des délibérations publiques sérieuses sur l'équilibre approprié entre les risques pour la vie privée et les inconvénients de la non-utilisation des données pour la recherche et l'innovation dans le domaine de la santé. Les délibérations devraient également porter sur les limites éthiques des modèles qui orientent les décisions en matière de santé, en tenant compte des possibilités de stigmatisation et d'inégalités lors de l'élaboration des modèles et de leur accès.

Il existe des solutions pour gouverner les consortiums d'apprentissage fédéré où de multiples parties prenantes participent à la prise de décision. Le développement technologique lié au consentement dynamique permet à des individus de déterminer leur niveau de participation; d'autres peuvent donner un consentement plus large à des organes de gouvernance correctement constitués. L'apprentissage fédéré simplifie la gouvernance avec une organisation responsable qui assume les risques liés au développement du modèle global.

Toutefois, le développement et la mise en oeuvre de l'apprentissage fédéré exigeront que tous les partenaires et responsables impliqués dans les approbations et la gouvernance suivent une formation. La collaboration avec des technologues sera essentielle pour bien comprendre les progrès de la recherche en matière de sécurité. Cela favorisera le développement de l'apprentissage fédéré et de ses applications pour la santé ainsi que celui des prototypes de recherche existants qui ont fait l'objet d'évaluations à petite échelle. Une application en situation réelle sera nécessaire pour démontrer l'efficacité de ces techniques et leur utilité pour relever les défis en matière d'éthique, de protection de la vie privée et de sécurité liés à l'utilisation des données sur la santé.

5.0 RÉFÉRENCES

[1] Gulshan, V., Peng, L., Coram, M., Stumpe, M. C., Wu, D., Narayanaswamy, A., Venugopalan, S., Widner, K., Madams, T., Cuadros, J., Kim, R., Raman, R., Nelson, P. C., Mega, J. L., & Webster, D. A. (2016). Development and Validation of a Deep Learning Algorithm for Detection of Diabetic Retinopathy in Retinal Fundus Photographs. JAMA, 316(22), 2402. https://doi.org/10.1001/jama.2016.17216

[2] Campanella, G., Hanna, M. G., Geneslaw, L., Miraflor, A. P., Silva, V., Busam, K. J., Brogi, E., Reuter, V. E., Klimstra, D. S., & Fuchs, T. (2019). Clinical-grade computational pathology using weakly supervised deep learning on whole slide images. Nature Medicine, 25(8), 1301–1309. https://doi.org/10.1038/s41591-019-0508-1

[3] Coudray, N., Ocampo, P. S., Sakellaropoulos, T., Narula, N., Snuderl, M., Fenyö, D., Moreira, A. L., Razavian, N., & Tsirigos, A. (2018). Classification and mutation prediction from non–small cell lung cancer histopathology images using deep learning. Nature Medicine, 24(10), 1559–1567. https://doi.org/10.1038/s41591-018-0177-5

[4] Bejnordi, B. E., Veta, M., Van Diest, P. J., Van Ginneken, B., Karssemeijer, N., Litjens, G., Van Der Laak, J. a. W. M., Hermsen, M., Manson, Q. F., Balkenhol, M., Geessink, O., Stathonikos, N., Van Dijk, M. C., Bult, P., Beca, F., Beck, A. H., Wang, D., Khosla, A., Gargeya, R., . . . Venâncio, R. (2017). Diagnostic Assessment of Deep Learning Algorithms for Detection of Lymph Node Metastases in Women With Breast Cancer. JAMA, 318(22), 2199. https://doi.org/10.1001/jama.2017.14585

[5] Esteva, A., Kuprel, B., Novoa, R. A., Ko, J. S., Swetter, S. M., Blau, H. M., & Thrun, S. (2017). Dermatologist-level classification of skin cancer with deep neural networks. Nature, 542(7639), 115–118. https://doi.org/10.1038/nature21056

[6] Mobadersany, P., Yousefi, S., Amgad, M., Gutman, D. A., Barnholtz-Sloan, J. S., Vega, J. A., Brat, D. J., & Cooper, L. (2018). Predicting cancer outcomes from histology and genomics using convolutional networks. Proceedings of the National Academy of Sciences of the United States of America, 115(13). https://doi.org/10.1073/pnas.1717139115

[7] Halpern, A. C., Janda, M., Lallas, A., Longo, C., Malvehy, J., Paoli, J., Puig, S., Rosendahl, C., Soyer, H. P., Zalaudek, I., & Kittler, H. (2020). Human–computer collaboration for skin cancer recognition. Nature Medicine, 26(8), 1229–1234. https://doi.org/10.1038/s41591-020-0942-0

[8] Rieke, N., Hancox, J., Li, W., Milletari, F., Roth, H. R., Albarqouni, S., Bakas, S., Galtier, M., Landman, B. A., Maier-Hein, K. H., Ourselin, S., Sheller, M. J., Zhang, D., Trask, A., Xu, D., Baust, M., & Cardoso, M. J. (2020). The future of digital health with federated learning. Npj Digital Medicine, 3(1). https://doi.org/10.1038/s41746-020-00323-1

[9] Health Canada (2023, February) Working together to improve health care for Canadians. https://www.canada.ca/en/health-canada/news/2023/02/working-together-to-improve-health-care-for-canadians.html

[10] Rieke, N., Hancox, J., Li, W., Milletari, F., Roth, H. R., Albarqouni, S., Bakas, S., Galtier, M., Landman, B. A., Maier-Hein, K. H., Ourselin, S., Sheller, M. J., Zhang, D., Trask, A., Xu, D., Baust, M., & Cardoso, M. J.

(2020). The future of digital health with federated learning. Npj Digital Medicine, 3(1). https://doi.org/10.1038/s41746-020-00323-1

[11] Agence de la santé publique du Canada (novembre 2021). Bâtir la Fondation canadienne des données sur la santé : Rapport 2 du Comité consultatif d'experts de la Stratégie pancanadienne de données sur la santé. Canada.ca. https://www.canada.ca/fr/sante-publique/organisation/mandat/a-propos-agence/organismes-consultatifs-externes/liste/strategie-pancanadienne-sante-rapports-sommaires/rapport-02-comite-consultatif-experts-batir-fondation-canadienne-donnees-sante.html

[12] Rieke, N., Hancox, J., Li, W., Milletari, F., Roth, H. R., Albarqouni, S., Bakas, S., Galtier, M., Landman, B. A., Maier-Hein, K. H., Ourselin, S., Sheller, M. J., Zhang, D., Trask, A., Xu, D., Baust, M., & Cardoso, M. J. (2020). The future of digital health with federated learning. Npj Digital Medicine, 3(1). https://doi.org/10.1038/s41746-020-00323-1

[13] Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (2019). Federated Learning: Challenges, Methods, and Future Directions. IEEE Signal Processing Magazine, 37(3), 50–60. https://doi.org/10.1109/msp.2020.2975749

[14] Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (2019). Federated Learning: Challenges, Methods, and Future Directions. IEEE Signal Processing Magazine, 37(3), 50–60. https://doi.org/10.1109/msp.2020.2975749

[15] Wood, A., Altman, M., Bembenek, A., Bun, M., Gaboardi, M., Honaker, J., . . . Vadhan, S. (2018). Differential Privacy: A Primer for a Non-Technical Audience. Vanderbilt Journal of Entertainment & Technology Law, 21(1), 209. Retrieved from https://scholarship.law.vanderbilt.edu/cgi/viewcontent.cgi?article=1058&context=jetlaw

[16] Zhao, Y., & Chen, J. (2022). A Survey on Differential Privacy for Unstructured Data Content. ACM Computing Surveys, 54(10s), 1–28. https://doi.org/10.1145/3490237

[17] Kokosi, T., & Harron, K. (2022). Synthetic data in medical research. BMJ Medicine, 1(1), e000167. https://doi.org/10.1136/bmjmed-2022-000167

[18] Gstrein, O. J., & Beaulieu, A. (2022). How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches. Philosophy & Technology, 35(1). https://doi.org/10.1007/s13347-022-00497-4

[19] World Economic Forum. (2020) Sharing Sensitive Health Data in a Federated Data Consortium Model: An Eight-Step Guide. https://www.weforum.org/reports/sharing-sensitive-health-data-in-a-federated-data-consortium-model-an-eight-step-guide/

[20] Wan, Z., Hazel, J. W. G., Clayton, E. W., Vorobeychik, Y., Kantarcioglu, M., & Malin, B. A. (2022). Sociotechnical safeguards for genomic data privacy. Nature Reviews Genetics, 23(7), 429–445. https://doi.org/10.1038/s41576-022-00455-y

[21] Commissaire à l'information et à la protection de la vie privée de l'Ontario (2011) Privacy by Design – The 7 Foundational Principles – Implementation and Mapping of Fair Information Practices. https://www.ipc.on.ca/wp-content/uploads/resources/pbd-implement-7found-principles.pdf

[22] Wood, A., Altman, M., Bembenek, A., Bun, M., Gaboardi, M., Honaker, J., . . . Vadhan, S. (2018). Differential Privacy: A Primer for a Non-Technical Audience. Vanderbilt Journal of Entertainment & Technology Law, 21(1), 209. Retrieved from https://scholarship.law.vanderbilt.edu/jetlaw/vol21/iss1/4/

[23] Agence de la santé publique du Canada (novembre 2021). Bâtir la Fondation canadienne des données sur la santé : Rapport 2 du Comité consultatif d'experts de la Stratégie pancanadienne de données sur la santé. Canada.ca. https://www.canada.ca/fr/sante-publique/organisation/mandat/a-propos-agence/organismes-consultatifs-externes/liste/strategie-pancanadienne-sante-rapports-sommaires/rapport-02-comite-consultatif-experts-batir-fondation-canadienne-donnees-sante.html

[24] Rieke, N., Hancox, J., Li, W., Milletari, F., Roth, H. R., Albarqouni, S., Bakas, S., Galtier, M., Landman, B. A., Maier-Hein, K. H., Ourselin, S., Sheller, M. J., Zhang, D., Trask, A., Xu, D., Baust, M., & Cardoso, M. J. (2020). The future of digital health with federated learning. Npj Digital Medicine, 3(1). https://doi.org/10.1038/s41746-020-00323-1

[25] Kalkman, S., Van Delden, J. J. M., Banerjee, A., Tyl, B., Mostert, M., & Van Thiel, G. J. M. W. (2019). Patients' and public views and attitudes towards the sharing of health data for research: a narrative review of the empirical evidence. Journal of Medical Ethics, 48(1), 3–13. https://doi.org/10.1136/medethics-2019-105651

[26] Teng, J., Bentley, C., Burgess, M. M., O'Doherty, K. C., & McGrail, K. (2019). Sharing linked data sets for research: results from a deliberative public engagement event in British Columbia, Canada. International Journal for Population Data Science, 4(1). https://doi.org/10.23889/ijpds.v4i1.1103

[27] Culbert, L. Would you let researchers access your health care data?; B.C.'s ‚medical database cited as a treasure trove of information. Vancouver Sun (5 December 2013).

[28] Velarde, M. R., Tsantoulis, P., Burton-Jeangros, C., Aceti, M., Chappuis, P. O., & Hurst-Majno, S. (2021). Citizens' views on sharing their health data: the role of competence, reliability and pursuing the common good. BMC Medical Ethics, 22, 62. https://doi.org/10.1186/s12910-021-00633-3

[29] Aitken, M., de St Jorre, J., Pagliari, C., Jepson, R., & Cunningham-Burley, S. (2016). Public responses to the sharing and linkage of health data for research purposes: a systematic review and thematic synthesis of qualitative studies. BMC Medical Ethics, 17(1), 73. https://doi:10.1186/s12910-016-0153-x

[30] Harrison, J., Auerbach, A. D., Anderson, W. G., Fagan, M., Carnie, M. B., Hanson, C., Banta, J. E., Symczak, G., Robinson, E. J., Schnipper, J. L., Wong, C., & Weiss, R. B. (2019). Patient stakeholder engagement in research: A narrative review to describe foundational principles and best practice activities. Health Expectations, 22(3), 307–316. https://doi.org/10.1111/hex.12873

[31] Teng, J., Bentley, C., Burgess, M. M., O'Doherty, K. C., & McGrail, K. (2019). Sharing linked data sets for research: results from a deliberative public engagement event in British Columbia, Canada. International Journal for Population Data Science, 4(1). https://doi.

org/10.23889/ijpds.v4i1.1103

[32] Tripp, L., Vanstone, M., Canfield, C., Leslie, M., Levasseur, M. A., Panday, J., Rowland, P., Wilson, G. A., You, J., & Abelson, J. (2022). The impact of COVID-19 on patient engagement in the health system: Results from a Pan-Canadian survey of patient, family and caregiver partners. Health Expectations, 25(2), 744–753. https://doi.org/10.1111/hex.13421

[33] Lysaght, T., Ballantyne, A., Xafis, V., Ong, S., Schaefer, G., Ling, J., Newson, A. J., Khor, I. W., & Tai, E. S. (2020). "Who is watching the watchdog?": ethical perspectives of sharing health-related data for precision medicine in Singapore. BMC Medical Ethics, 21, 118. https://doi.org/10.1186/s12910-020-00561-8

[34] McCradden, M. D., Sarker, T., & Paprica, P. A. (2020). Conditionally positive: a qualitative study of public perceptions about using health data for artificial intelligence research. BMJ Open, 10(10), e039798. https://doi.org/10.1136/bmjopen-2020-039798

[35] Paprica, P. A., De Melo, M. N., & Schull, M. J. (2019). Social licence and the general public's attitudes toward research based on linked administrative health data: a qualitative study. CMAJ Open, 7(1), E40–E46. https://doi.org/10.9778/cmajo.20180099

[36] Teng, J., Bentley, C., Burgess, M. M., O'Doherty, K. C., & McGrail, K. (2019). Sharing linked data sets for research: results from a deliberative public engagement event in British Columbia, Canada. International Journal for Population Data Science, 4(1). https://doi.org/10.23889/ijpds.v4i1.1103

[37] Carter, S. M., Rogers, W. A., Win, K. T., Frazer, H., Richards, B., & Houssami, N. (2020). The ethical, legal and social implications of using artificial intelligence systems in breast cancer care. The Breast, 49, 25–32. https://doi.org/10.1016/j.breast.2019.10.001

[38] Mantelero, A. (2022). Regulating AI. In A. Mantelero (Ed.), Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI (pp. 139-183). Springer Nature.

[39] Naik, N., Hameed, B.M.Z., Shetty, D. K., Swain, D., Shah, M., Paul, R., Aggarwal, K., Ibrahim, S., Patil, V., Smriti, K., Shetty, S., Rai, B. P., Chlosta, P., & Somani, B. K. (2022). Legal and Ethical Consideration in Artificial Intelligence in Healthcare: Who Takes Responsibility? Frontiers in Surgery, 9. https://doi.org/10.3389/fsurg.2022.862322

[40] UNESCO. (2023) https://en.unesco.org/artificial-intelligence/ethics

[41] Cooley, O., Pestrue, J., Phillips, M., Konye, J., Penoza, C., Ghous, M., & Singh, K. (2021). External Validation of a Widely Implemented Proprietary Sepsis Prediction Model in Hospitalized Patients. JAMA Internal Medicine. https://doi.org/10.1001/jamainternmed.2021.2626

[42] First Nations Information Governance Centre. (2014). Ownership, Control, Access and Possession (OCAP™): The Path to First Nations Information Governance. https://achh.ca/wp-content/uploads/2018/07/OCAP_FNIGC.pdf

[43] World Health Organization. (2021) Ethics and governance of artificial intelligence for health: WHO guidance. https://www.who.int/publications/i/item/9789240029200

[44] Kassam, I., Ilkina, D., Kemp, J., Roble, H., Carter-Langford, A., & Shen, N. (2022). Patient Perspectives and Preferences for Consent in the Digital Health Context: State-of-the-art Literature Review. Journal of Medical Internet Research, 25, e42507. https://doi.org/10.2196/42507

[45] Alghazwi, M., Turkmen, F., Van Der Velde, K. J., & Karastoyanova, D. (2021). Blockchain for Genomics: A Systematic Literature Review. Distributed Ledger Technologies: Research and Practice, 1(2), 1–28. https://doi.org/10.1145/3563044

[46] Mamo, N., Martin, G. M., Desira, M., Ellul, B., & Ebejer, J. (2020). Dwarna: a blockchain solution for dynamic consent in biobanking. European Journal of Human Genetics, 28(5), 609–626. https://doi.org/10.1038/s41431-019-0560-9

[47] Teare, H., Prictor, M., & Kaye, J. (2021). Reflections on dynamic consent in biomedical research: the story so far. European Journal of Human Genetics, 29(4), 649–656. https://doi.org/10.1038/s41431-020-00771-z

[48] ten Have, H., & Patrão Neves, M. d. C. (2021). Community Consent. In ten Have, H., & Patrão Neves, M. D. C. (2021). Dictionary of Global Bioethics. Springer Nature.

[49] Cumyn, A., Barton, A., Dault, R., Cloutier, A., Jalbert, R., & Ethier, J. (2020). Informed consent within a learning health system: A scoping review. Learning Health Systems, 4(2). https://doi.org/10.1002/lrh2.10206

[50] Broes, S., Lacombe, D., Verlinden, M., & Huys, I. (2018). Toward a Tiered Model to Share Clinical Trial Data and Samples in Precision Oncology. Frontiers in Medicine, 5. https://doi.org/10.3389/fmed.2018.00006

[51] Wolf, L. E., Hammack, C. M., Brown, E. G., Brelsford, K. M., & Beskow, L. M. (2020). Protecting Participants in Genomic Research: Understanding the "Web of Protections" Afforded by Federal and State Law. Journal of Law Medicine & Ethics, 48(1), 126–141. https://doi.org/10.1177/1073110520917000

[52] World Economic Forum. (2020) Sharing Sensitive Health Data in a Federated Data Consortium Model: An Eight-Step Guide. https://www.weforum.org/reports/sharing-sensitive-health-data-in-a-federated-data-consortium-model-an-eight-step-guide/

[53] Broes, S., Lacombe, D., Verlinden, M., & Huys, I. (2018). Toward a Tiered Model to Share Clinical Trial Data and Samples in Precision Oncology. Frontiers in Medicine, 5. https://doi.org/10.3389/fmed.2018.00006

[54] Mothukuri, V., Parizi, R. M., Pouriyeh, S., Huang, Y., Dehghantanha, A., & Srivastava, G. (2021). A survey on security and privacy of federated learning. Future Generation Computer Systems, 115, 619–640. https://doi.org/10.1016/j.future.2020.10.007

[55] Mothukuri, V., Parizi, R. M., Pouriyeh, S., Huang, Y., Dehghantanha, A., & Srivastava, G. (2021). A survey on security and privacy of federated learning. Future Generation Computer Systems, 115, 619–640. https://doi.org/10.1016/j.future.2020.10.007

[56] Nguyen, T. V., Dakka, M. A., Diakiw, S., VerMilyea, M. D., Perugini, M., Hall, J. M. M., & Perugini, D. (2022). A novel decentralized federated learning approach to train on globally distributed, poor quality, and protected private medical data. Scientific Reports, 12, 8888. https://doi.org/10.1038/s41598-022-12833-x

[57] Scheibner, J., Sleigh, Ienca, M J., & Vayena, E. (2021). Benefits, challenges, and contributors to success for national eHealth systems implementation: a scoping review. Journal of the American Medical Informatics Association, 28(9), 2039–2049. https://doi.org/10.1093/jamia/ocab096

[58] Rieke, N., Hancox, J., Li, W., Milletari, F., Roth, H. R., Albarqouni, S., Bakas, S., Galtier, M., Landman, B. A., Maier-Hein, K. H., Ourselin, S., Sheller, M. J., Zhang, D., Trask, A., Xu, D., Baust, M., & Cardoso, M. J. (2020). The future of digital health with federated learning. Npj Digital Medicine, 3(1). https://doi.org/10.1038/s41746-020-00323-1

[59] Behera, M. R., Upadhyay, S. K., Shetty, S. K. B., Priyadarshini, S., Patel, P., & Lee, K. F. (2022). FedSyn: Synthetic Data Generation using Federated Learning. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2203.05931

[60] Chen, H., Tu, C., Li, Z., Shen, H., & Chao, W. (2022). On the Importance and Applicability of Pre-Training for Federated Learning. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2206.11488

[61] Ghimire, B. K., & Rawat, D. B. (2022). Recent Advances on Federated Learning for Cybersecurity and Cybersecurity for Federated Learning for Internet of Things. IEEE Internet of Things Journal, 9(11), 8229–8249. https://doi.org/10.1109/jiot.2022.3150363

[62] Al Kinoon, M., Omar, M., Mohaisen, M., & Mohaisen, A. (2021). Security Breaches in the Healthcare Domain: A Spatiotemporal Analysis. In Lecture Notes in Computer Science (pp. 171–183). Springer Science+Business Media. https://doi.org/10.1007/978-3-030-91434-9_16

[63] Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Healthcare Data Breaches: Insights and Implications. Healthcare, 8(2), 133. https://doi.org/10.3390/healthcare8020133

[64] Fredrikson, M., Jha, S., & Ristenpart, T. (2015). Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures. CCS '15: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, 1322-1333. https://doi.org/10.1145/2810103.2813677

[65] Kairouz, P., et al. (2021) Advances and Open Problems in Federated Learning. Now Foundations and Trends Books | IEEE Xplore. https://ieeexplore.ieee.org/document/9464278

[66] Rieke, N., Hancox, J., Li, W., Milletari, F., Roth, H. R., Albarqouni, S., Bakas, S., Galtier, M., Landman, B. A., Maier-Hein, K. H., Ourselin, S., Sheller, M. J., Zhang, D., Trask, A., Xu, D., Baust, M., & Cardoso, M. J. (2020). The future of digital health with federated learning. Npj Digital Medicine, 3(1). https://doi.org/10.1038/s41746-020-00323-1

[67] Banner, N. (2022). NHS data breaches: a further erosion of trust. BMJ, o1187. https://doi.org/10.1136/bmj.o1187

[68] Mothukuri, V., Parizi, R. M., Pouriyeh, S., Huang, Y., Dehghantanha, A., & Srivastava, G. (2021). A survey on security and privacy of federated learning. Future Generation Computer Systems, 115, 619–640. https://doi.org/10.1016/j.future.2020.10.007

[69] Rieke, N., Hancox, J., Li, W., Milletari, F., Roth, H. R., Albarqouni, S., Bakas, S., Galtier, M., Landman, B. A., Maier-Hein, K. H., Ourselin, S., Sheller, M. J., Summers, R.M., Trask, A., Xu, D., Baust, M., & Cardoso, M. J. (2020). The future of digital health with federated learning. npj Digital Medicine, 3, 119. https://doi.org/10.1038/s41746-020-00323-1

[70] Phong, L. T., Aono, Y., Hayashi, T., Wang, L. et Moriai, S. (2017). Privacy-preserving deep learning: Revisited and enhanced. In Batten, L., Kim, D. S., Zhang, X. et Li, G (éd.). Applications and Techniques in Information Security. ATIS 2017. Communications in Computer and Information Science, vol. 719, Springer, Singapore. https://doi.org/10.1007/978-981-10-5421-1_9