



Les attestations de vaccination sont-elles le prochain vecteur de cyberrisques?

Pour faire contrepoids aux cyberrisques liés aux certificats de vaccination numériques, il importe de prendre en considération la manière dont nous pourrions d'emblée intégrer des mécanismes de protection en adoptant un système de régulation dans plusieurs secteurs cruciaux.

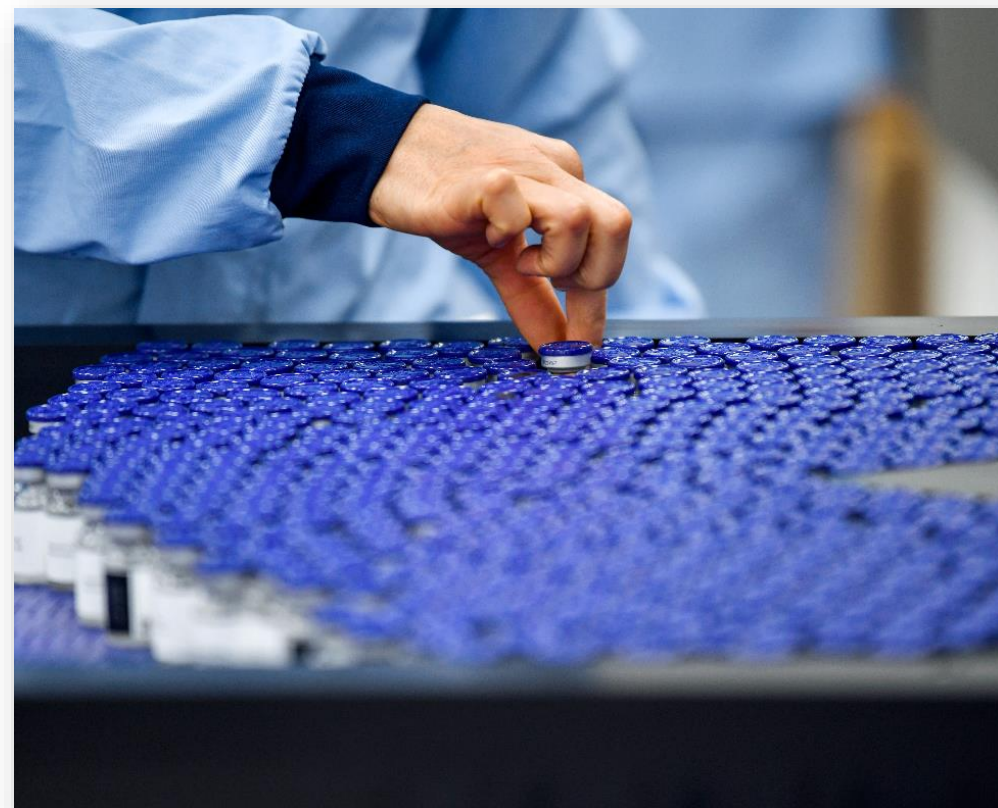
Dans la foulée de la mise au point par des sociétés pharmaceutiques de plusieurs vaccins viables contre la COVID-19, l'éventualité d'un retour à un semblant de normalité se profile. La capacité d'endiguer la propagation du virus fait naître l'espoir que, grâce à la vaccination, la population pourra retourner au travail, fréquenter de nouveau les restaurants et les commerces de détail, assister à des événements publics, et recommencer à voyager.

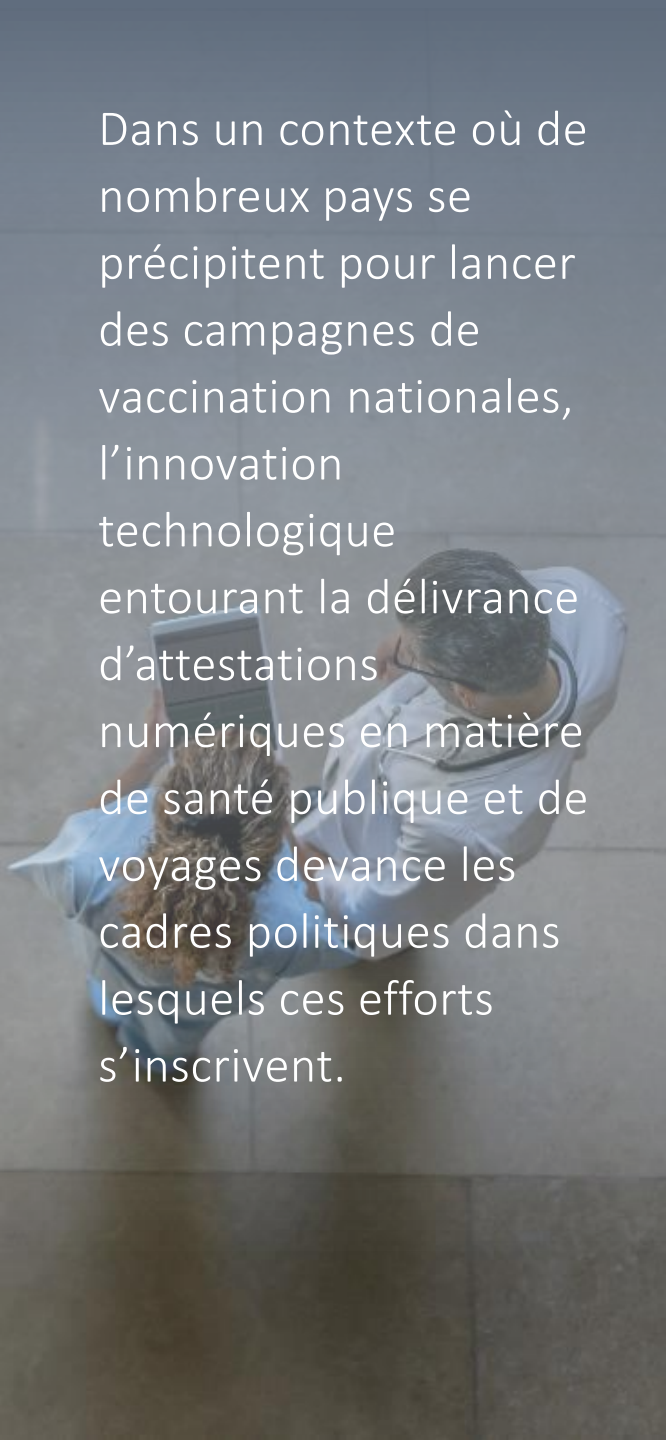
Cette perspective présuppose que des certificats de vaccination sous une forme ou une autre seront délivrés aux citoyens pour prouver leur statut vaccinal. Si cette idée paraît simple en théorie, il en va autrement dans la pratique : les attestations de vaccination comportent leur lot de complications, dont un grand nombre relèvent du domaine de la cybersécurité.

Quels sont les deux principaux enjeux? L'impératif de créer des versions numérisées des certificats de vaccination, en plus de produire des versions papier sécurisées; la nécessité d'assurer l'interopérabilité de ces attestations et leur transmissibilité à des tiers partout dans le monde.

En fait, cela signifie qu'une preuve de vaccination numérique délivrée à un voyageur du Royaume-Uni doit être acceptable et crédible pour les pouvoirs publics et les entreprises privées de Singapour ou d'Australie afin d'offrir les avantages nécessaires à la réouverture de l'économie mondiale.

Pour assurer à la fois la délivrance de certificats de vaccination et la protection de l'identité numérique des personnes vaccinées (sans parler de la confidentialité de leurs renseignements personnels), les gouvernements, les consortiums, les organisations du secteur des soins de santé et les entreprises privées mettent rapidement leurs efforts en commun afin de surmonter plusieurs obstacles dans la course à la montre qui s'est engagée. Cet article fait état de quelques-unes des problématiques qui devront être abordées à relativement brève échéance – étant entendu qu'il ne s'agit que d'une amorce de débat.





Dans un contexte où de nombreux pays se précipitent pour lancer des campagnes de vaccination nationales, l'innovation technologique entourant la délivrance d'attestations numériques en matière de santé publique et de voyages devance les cadres politiques dans lesquels ces efforts s'inscrivent.

Adopter des mécanismes régulateurs dans plusieurs secteurs cruciaux

Vue aérienne

Comme le bilan des décès attribués au coronavirus depuis un an a franchi la barre des 2,5 millions¹, il n'est pas étonnant que de nombreux pays se précipitent maintenant pour lancer des campagnes de vaccination nationales. Au 2 mars 2021, environ 247 millions de doses avaient été administrées dans le monde², et ce nombre augmente chaque jour.

La rapidité avec laquelle le monde se mobilise pour juguler la crise sanitaire est louable. Ce qui en ressort, cependant, c'est que des programmes et des systèmes sont parfois créés en l'espace de quelques jours et que la rigueur habituellement démontrée dans les initiatives de longue haleine fait défaut. Résultat : l'innovation technologique entourant la production d'attestations numériques en matière de santé publique et de voyages devance les cadres politiques dans lesquels ces efforts s'inscrivent.

En plus de faire croître le risque de faux-pas et d'une mauvaise utilisation des données, cette précipitation ouvre la voie à un autre enjeu de cybersécurité – un enjeu particulièrement pressant dans le domaine des soins de santé parce que les données médicales ne sont pas juste sensibles; elles sont inestimables. En fait, les données liées à la santé valent presque 50 fois plus sur le marché noir que les données relatives aux cartes de paiement³ puisque les renseignements de nature sanitaire comportent des éléments d'information qui permettent l'identification des personnes et peuvent être exploitées aux fins de vol d'identité et de fraude financière.

Pour faire contrepoids à ces cyberrisques, une technologie relativement récente qui permet la vérification des attestations et la gestion distribuée des identités fait l'unanimité à l'échelle mondiale. Parfois désigné sous le nom de « modèle d'identité autosouveraine » ou SSI, ce mode d'identification numérique diffère de ses cousins centralisés ou fédérés parce qu'il place le porteur (le citoyen) au centre du système d'interactions et permet aux parties qui s'y fient (p. ex. les compagnies aériennes) de valider la preuve de vaccination en regard d'un registre public d'émetteurs (en général, des chaînes de blocs) plutôt que d'avoir à traiter ou à stocker les renseignements personnels des porteurs.

Certes, les subtilités du mécanisme de vérification des preuves apportent des solutions à certains problèmes classiques des systèmes centralisés de gestion de l'identité, mais il est important de tenir compte des moyens à prendre pour intégrer dès le départ des mesures de protection en adoptant un système de régulation dans plusieurs secteurs cruciaux. En voici quelques-uns :

La gouvernance

Le nombre d'intervenants qui seront nécessaires pour établir efficacement les preuves de vaccination partout dans le monde est colossal. Un nombre incalculable d'organismes publics, d'organisations intergouvernementales (p. ex. l'Organisation mondiale de la santé), de consortiums et d'entreprises privées doivent travailler de concert pour arriver à une solution – et bien que ces parties prenantes soient peut-être motivées

actuellement à coopérer, des structures de gouvernance bien rodées seront nécessaires pour empêcher que la collaboration s'érode avec le temps. Pour que les rôles et les résultats escomptés de chaque partie à l'écosystème soient définis, des intervenants des secteurs public et privé se sont déjà réunis dans certains pays pour établir des cadres de confiance clairs tels que le Cadre de confiance pancanadien et le Digital Identity and Attributes Trust Framework au Royaume-Uni.

En plus de définir clairement les rôles, les responsabilités et les comportements acceptés, cependant, les cadres de gouvernance devront se prêter à la mise en commun des efforts des parties prenantes. Tout le monde tente de comprendre comment fonctionnerait une preuve de vaccination ou de dépistage, mais il est important que les considérations de cybersécurité soient rigoureusement enchâssées dans les travaux de mise au point. Le recours à des structures de gouvernance à maturité sera essentiel si les parties prenantes espèrent parvenir à énoncer des normes générales ou communes en matière de sécurité, d'authentification, de protection de la vie privée et d'échange de données.

La complexité de cette tâche est sans contredit exacerbée par la vitesse à laquelle le monde évolue. Cela signifie que des politiques gouvernementales régissant le contrôle des frontières exercé par les pays de même que leur position à l'égard des attestations de vaccination et de dépistage devront être énoncées aussi rapidement que de nouvelles technologies apparaîtront.

1. John Hopkins, « COVID-19 Dashboard by the Center for Systems Science and Engineering », <https://coronavirus.jhu.edu/map.html>.

2. *New York Times*, 2 mars, 2021, « Tracking Coronavirus Vaccinations Around the World », <https://www.nytimes.com/interactive/2021/world/covid-vaccinations-tracker.html>.

3. SecureLink, 5 février 2020, « Healthcare data: The new prize for hackers », par Ellen Neveux, <https://www.securelink.com/blog/healthcare-data-new-prize-hackers/>.

L'éthique et la confiance

L'une des principales difficultés inhérentes à la production d'un certificat de vaccination réside dans le fait qu'elle est conditionnelle à ce que les citoyens acceptent de communiquer leurs renseignements sanitaires aux autorités responsables. Leur acceptation est précaire même dans les pays où les populations font confiance aux organisations du secteur public. Dans les pays où la confiance fait défaut, l'idée même de communiquer des preuves de vaccination peut être d'emblée exclue.

Vu les dilemmes éthiques que suscite cette initiative, le recours à un cadre de confiance et à des méthodes technologiques qui intègrent les principes de la protection des renseignements personnels dès la conception est impérieux. Comment empêcher un gouvernement d'utiliser des dossiers de vaccination pour d'autres utilisations que l'autorisation de voyager? Comment faire intervenir l'utilisateur plutôt que l'organe gouvernemental dans la gestion et le contrôle du consentement? Nous découvrirons que, selon la région, des questions peuvent être soulevées quant au juste équilibre entre les libertés civiles et l'intérêt public. Est-on en train de créer un dangereux précédent en limitant l'accès des citoyens aux produits ou aux services en fonction de données sanitaires?

Il ne suffit pas de faire preuve de maturité à l'égard de la cybersécurité pour régler tous ces dilemmes, mais cela peut grandement contribuer à l'établissement d'un réseau de confiance propice à la concertation de multiples intervenants, même dans les territoires où il semble impossible de gagner la confiance des citoyens en raison de la complexité des facteurs en présence.

L'échange des données

Avant que les voyageurs puissent commencer à montrer leurs certificats de vaccination numériques dans les aéroports et les lieux publics, des normes devront être mises en place pour régir la manière dont les données sanitaires des voyageurs seront communiquées, leur accès, la période de conservation de ces renseignements et leur utilisation. Par exemple, en plus d'accorder aux citoyens le droit de consentir (ou de refuser leur consentement) à l'utilisation de leurs renseignements personnels, le Règlement général sur la protection des données (RGPD) dont l'Union européenne s'est dotée impose des restrictions strictes concernant les entités qui peuvent traiter les données sanitaires des citoyens et leur utilisation. Ces entités, en contrepartie, sont censées faire preuve d'une transparence absolue dans le traitement des données.

La complexité inhérente à l'échange des données est l'une des principales raisons pour lesquelles l'adoption d'un modèle distribué d'attestations vérifiables se répand rapidement en tant que cadre de référence pour les preuves de vaccination et de dépistage. Des protocoles techniques précis n'ont pas encore été mis en place pour les attestations de vaccination, mais on assiste à l'émergence de normes tenant compte de protocoles de validation (p. ex. W3C et HCL7). Des gouvernements et des consortiums du secteur privé s'alignent sur ces normes. Deloitte et d'autres cabinets collaborent à la résolution de ce problème mondial avec des groupes locaux et dans le cadre de vastes projets sectoriels tels que The Good Health Pass⁴.

Les gouvernements et les organisations autorisées à délivrer des certificats de vaccination et de dépistage doivent se porter garants de leur authenticité partout dans le monde. Des organisations du secteur privé, par exemple les aéroports et les compagnies aériennes, devront avoir la capacité de vérifier que les attestations électroniques ou imprimées présentées par les citoyens sont authentiques et qu'elles ont été délivrées par des sources sûres.

Si la raison d'être des registres de chaînes de blocs pouvait paraître relever d'un avenir plutôt lointain il y a quelques mois à peine, on commence maintenant à entrevoir leur nécessité en tant qu'éléments de la solution qui permettra la mise en place du type de plateforme mondiale en voie d'élaboration

La protection des données

Pour qu'il soit possible de confirmer qu'une personne a rempli (ou est en voie de remplir) les formalités de vaccination ou de dépistage, les certificats de vaccination ou de dépistage peuvent comporter des identifiants personnels – allant des noms et des adresses aux identifiants de santé, voire à des données biométriques. Compte tenu de la valeur de ces renseignements, des contrôles de sécurité doivent impérativement être utilisés. Les parties prenantes doivent réfléchir à la manière dont les données seront gérées, stockées et protégées.

Cette tâche est d'autant plus compliquée qu'elle exige une collaboration mondiale. Une pléthore de structures juridiques et réglementaires, qui ont été conçues pour protéger cette catégorie de données, ont déjà été mises en place partout dans le monde. Ces mécanismes de protection et ces directives rendent le problème beaucoup plus complexe.

Les quelques documents ci-dessous en font foi :

- [Règlement général sur la protection des données](#)
- [Vermont Act 171 of 2018 Data Broker Regulation](#)
- [California Consumer Privacy Act](#)
- [Brazilian General Data Protection Law \(LGPD\)](#)
- [India Personal Data Protection Bill](#)
- [Chile Privacy Bill Initiative](#)
- [New Zealand Privacy Bill](#)

Qu'on en juge : sur le strict plan de la confidentialité des données, chaque pays est doté de sa propre réglementation. Des normes qui sont perçues comme étant très rigoureuses dans un territoire peuvent être jugées laxistes ailleurs. Sans palliatif efficace en matière de cybersécurité, le risque de fuite de données et de violation de la vie privée s'accroît.

Cela explique probablement pourquoi le modèle décentralisé autosouverain, dans lequel le citoyen est le porteur de l'attestation dans le portefeuille de son choix, devient une nécessité logique, car ce modèle réduit sensiblement ou élimine la quantité de renseignements personnels sur la santé qui sont stockés ou traités par des tiers.

4. Good Health Pass Collaborative, « Good Health Pass: A Safe Path to Global Reopening ». <https://www.goodhealthpass.org/>

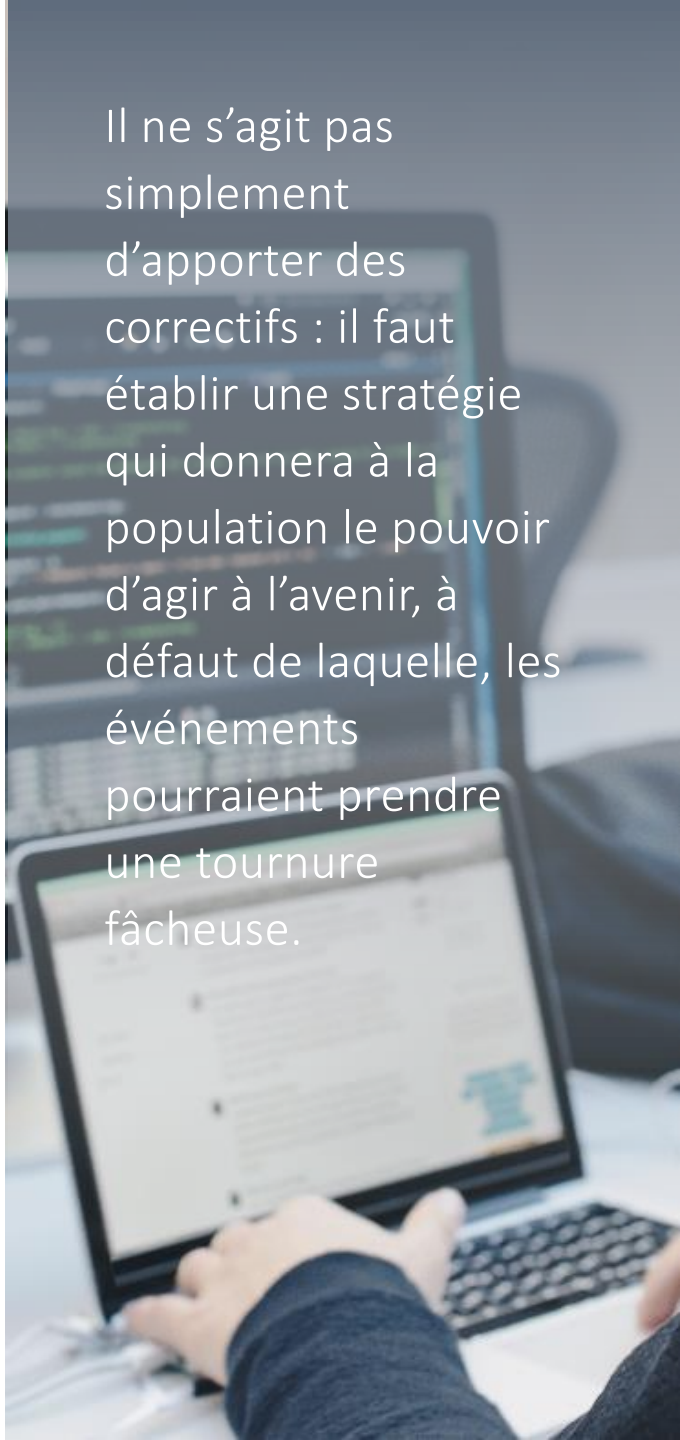
Enjamber le fossé

Ce survol d'une poignée de préoccupations liées à la cybersécurité fait ressortir clairement la nécessité de créer des assises solides dans un contexte où le monde se tourne vers l'adoption de certificats de vaccination numériques. Il ne s'agit pas simplement d'apporter des correctifs : il faut établir une stratégie complète et sécuritaire qui donnera à la population le pouvoir d'agir à l'avenir. À défaut d'une telle stratégie, les événements pourraient prendre une tournure fâcheuse.

Au cours des prochaines semaines, nous approfondirons les considérations de cybersécurité effleurées dans cet article, qu'il est nécessaire de peser pour assurer la délivrance de certificats de vaccination ou de dépistage sécuritaires. Entretemps, il y a matière à réflexion : l'un des obstacles à l'investissement public dans de vastes systèmes de gestion des identités numériques (l'identité citoyenne numérique) est l'adhésion publique à la création précoce de certificats. La nécessité de délivrer des attestations de vaccination ou de dépistage pour relancer l'économie dans des conditions sécuritaires change complètement ce paradigme.

Les gouvernements et les intervenants du secteur privé discutent de la question des identités citoyennes numériques et des certificats de même que de leurs rôles, mais la nécessité de produire des certificats de vaccination et de dépistage sécuritaires, utiles et inclusifs peut véritablement accélérer la mise au point d'identités citoyennes numériques d'utilisation générale et interexploitables mondialement.

Tout cela montre clairement que si les 12 derniers mois ont été extraordinairement difficiles, ils ont aussi mis en lumière l'ingéniosité et les ressources de la société à l'échelle mondiale. Maintenant que nous nous employons collectivement à faire en sorte que les économies et les populations renouent avec la prospérité, nous ne devons rien négliger pour assurer la collecte et la communication sécuritaires des données de même que la mise en application de politiques cohérentes et pour gagner la confiance nécessaire à notre réussite.



Il ne s'agit pas simplement d'apporter des correctifs : il faut établir une stratégie qui donnera à la population le pouvoir d'agir à l'avenir, à défaut de laquelle, les événements pourraient prendre une tournure fâcheuse.

Personne-ressource



Amir Belkhelladi | Leader canadien, Cybersécurité

abelkhelladi@deloitte.ca

Collaborateurs:

Esther Dryburgh | Conseils en gestion des risques – Deloitte Canada

Dan Shaver | Consultation – Deloitte Canada

À propos de Deloitte

Deloitte offre des services dans les domaines de l'audit et de la certification, de la consultation, des conseils financiers, des conseils en gestion des risques, de la fiscalité et d'autres services connexes à de nombreuses sociétés ouvertes et fermées dans différents secteurs. Deloitte sert quatre entreprises sur cinq du palmarès Fortune Global 500MD par l'intermédiaire de son réseau mondial de cabinets membres dans plus de 150 pays et territoires, qui offre les compétences de renommée mondiale, le savoir et les services dont les clients ont besoin pour surmonter les défis d'entreprise les plus complexes. Deloitte S.E.N.C.R.L./s.r.l., société à responsabilité limitée constituée en vertu des lois de l'Ontario, est le cabinet membre canadien de Deloitte Touche Tohmatsu Limited. Deloitte désigne une ou plusieurs entités parmi Deloitte Touche Tohmatsu Limited, société fermée à responsabilité limitée par garanties du Royaume-Uni, ainsi que son réseau de cabinets membres dont chacun constitue une entité juridique distincte et indépendante. Pour une description détaillée de la structure juridique de Deloitte Touche Tohmatsu Limited et de ses sociétés membres, voir www.deloitte.com/ca/apropos.

Notre raison d'être mondiale est d'avoir une influence marquante. Chez Deloitte Canada, cela se traduit par la création d'un avenir meilleur en accélérant et en élargissant l'accès au savoir. Nous croyons que nous pouvons concrétiser cette raison d'être en incarnant nos valeurs communes qui sont d'ouvrir la voie, de servir avec intégrité, de prendre soin les uns des autres, de favoriser l'inclusion et de collaborer pour avoir une influence mesurable.

Pour en apprendre davantage sur les quelque 330 000 professionnels de Deloitte, dont plus de 11 000 font partie du cabinet canadien, veuillez nous suivre sur [LinkedIn](#), [Twitter](#), [Instagram](#), ou [Facebook](#).