FAQ sur les accès à EpicCare Link et Hyperspace

Mon organisation n'a pas besoin de consentement pour consulter et collecter les données. Pourquoi dois-je signer l'accord?

Nous reconnaissons que certaines des organisations auxquelles nous fournissons l'accès n'ont pas besoin de consentement pour accéder aux données. Cependant, nous sommes tenus, dans notre accord avec Epic, propriétaire des licences de la solution, d'imposer des conditions générales aux organisations accédant aux données via Epic. Il s'agit notamment de conditions générales telles que le respect de la propriété intellectuelle d'Epic et d'autres conditions similaires. De plus, l'entente clarifie la relation entre les parties et comprend les modalités qui se trouvent normalement dans une entente de partage de données entre deux organisations.

L'accord est-il négociable ??

Généralement non. Nous avons élaboré l'accord avec l'aide de conseillers juridiques internes et externes. Nous avons développé des conditions raisonnables qui sont pertinentes pour la variété de relations et d'organisations auxquelles nous donnons accès à notre système. En raison du volume d'organisations avec lesquelles nous entretenons une relation, nous ne sommes généralement pas en mesure de négocier les termes de l'accord. Toutefois, s'il y a des conditions auxquelles une organisation n'est pas en mesure de s'engager en vertu de la loi, l'organisation devrait proposer un autre libellé et une justification du changement.

Mon organisation n'est pas un dépositaire de renseignements sur la santé (HIC) en vertu de la LPRPS. Cet accord est-il toujours approprié?

Oui. L'entente a été élaborée pour tenir compte de la diversité des organisations auxquelles nous fournissons l'accès et de la variété des fins pour lesquelles elles accèdent aux données. L'entente comporte un certain nombre de modalités qui ne s'appliquent pas si l'autre partie n'est pas un HIC en vertu de la Loi sur la protection des renseignements personnels sur la santé (LPRPS). Cependant, nous demandons de ne pas les rayer parce que nous avons une capacité très limitée d'examiner les changements apportés par chaque organisation.

Mon organisation a-t-elle vraiment besoin de 5 000 000 $ de cyberassurance?

Oui. Nous avons inclus cette exigence d’après les conseils de nos assureurs. La cyberassurance couvre une organisation pour les atteintes à la vie privée et à la sécurité qui ne sont pas couvertes par d'autres polices d'assurance. Le montant de 5 000 000 $ pour une atteinte grave est réaliste pour couvrir le coût du confinement, de l'enquête, de la déclaration, de la rectification, des amendes ou pénalités potentielles et des poursuites judiciaires éventuelles.

Pourquoi l'entente accorde-t-elle à L'Hôpital d'Ottawa le droit de retirer l'accès sans préavis?

Nous nous efforcerions d'aviser et de travailler avec l'organisation ou les organisations touchées avant de retirer l'accès à leur personnel. Cependant, il peut y avoir des cas, par exemple dans le cas d'une atteinte à la vie privée ou à la sécurité, où nous devons immédiatement suspendre l'accès pour contenir le bris sans préavis.

Qui de notre organisation devrait signer l'accord?

L'accord doit être signé par:

a. Quelqu'un de l'organisation qui demande l'accès. Une organisation ne peut pas signer au nom des utilisateurs finaux d'une autre organisation ou parrainer l'accès pour ceux-ci; et

b. Quelqu'un qui a le pouvoir d'engager l'organisation. Dans une grande organisation, il s'agit probablement d'un membre de l'équipe de direction (p. ex., PDG, directeur financier). Dans une pratique communautaire, il s'agit probablement du médecin chef ou du directeur de la clinique. Cependant, vous devrez identifier qui, au sein de votre organisation, a le pouvoir de signer l'accord.

Que dois-je inclure dans la colonne de description de l'attestation?

En un ou deux points, décrivez comment vous répondez à l'exigence. Notez également si votre organisation dispose d'une stratégie existante qui répond à cette exigence.

Nos utilisateurs finaux utilisent l'équipement Atlas Alliance pour accéder aux informations sur les patients, car ils travaillent sur place chez l'un des membres d'Alliance Atlas. Comment devrions-nous remplir les éléments de l'attestation qui font référence à la sécurité de nos appareils?

Si vos utilisateurs finaux travaillent sur place et utilisent l'équipement Atlas Alliance, veuillez répondre « N/A » aux questions où un membre d'Atlas Alliance fournit la technologie. Veuillez également noter dans la colonne de description pourquoi il n'est pas applicable (par exemple, « Nos utilisateurs utiliseront exclusivement les appareils et les réseaux fournis par les membres d'Atlas Alliance. Les utilisateurs ont été éduqués et sont conscients de cette exigence.

Pourquoi le chiffrement du disque dur est-il requis sur les appareils qui accèdent à des renseignements personnels sur la santé?

Il est possible pour un utilisateur final d'enregistrer des informations sur ses ordinateurs via une capture d'écran ou un autre mécanisme. Les fichiers temporaires peuvent également être automatiquement enregistrés sur l'ordinateur si l'utilisateur final imprime des documents. Le chiffrement du disque dur permet de s'assurer que les informations sont protégées en cas de perte ou de vol de l'appareil.