LA SÉCURISATION DANS TOPAZ

Comment ça fonctionne ?

- Chaque utilisateur dispose d'une clé de chiffrement. Cette clé est un fichier de 2048 caractères (fichier *.key) qui correspond au standard actuel en matière de chiffrement. Ce fichier est stocké dans votre application sur votre poste de travail (en local). Il permet de chiffrer et déchiffrer (via un algorythme de chiffrement) toutes les données que vous enregistrez. Les données sont chiffrées en local sur votre machine puis envoyées chiffrées dans le cloud Topaz. Ainsi, personne d'autre ne peut les lire.

- Les identifiants (nom d'utilisateur et mot de passe) que vous utilisez pour entrer dans Topaz servent uniquement à vous identifier, pas à chiffrer les données.

Conséquences

- En cas de perte ou de dégât (matériel ou logiciel) de votre ordinateur sur lequel est installé Topaz, la clé est perdue et donc toutes vos données sont illisibles.

- Vous devez donc stocker cette clé dans un endroit sécurisé sur support informatique et l'imprimer (double stockage). Topaz organise une possibilité de sauvegarde chez un notaire, vous pouvez contacter notre support pour plus d'informations.

- Il ne faut pas stocker une clé de chiffrement sur un serveur. Par définition, un serveur reste en permanence connecté à internet, il est donc vulnérable aux attaques incessantes qui circulent sur le net. Votre clé peut alors être volée ou détruite (cryptovirus/ransomware).

Remarque : ces clés personnelles ne sont pas protégées par un mot de passe, car une fois volées, il est très rapide de découvrir un mot de passe de 8 ou 10 caractères (ex : attaque de force brute). Un mot de passe est une modalité d'identification plutôt qu'une modalité de sécurisation. La seule sécurisation valable est donc de rendre la clé innacessible: ordinateur éteint en dehors de l'utilisation quotidienne et double stockage dans un endroit sécurisé.

- Si on vole ou découvre vos identifiants (ex : attaque de force brute), on peut entrer dans Topaz, voir la liste des patients, mais pas lire les données.

- Le partage de dossier ne peut se faire que si plusieurs utilisateurs utilisent la même clé. Les membres d'une pratique de groupe utilisent donc tous la même clé appelée **clé de groupe**. Celle-ci chiffre les données accessibles aux membres de la pratique de groupe. **Cette clé de groupe doit également être stockée de manière sécurisée**. De plus chaque membre du groupe possède aussi sa propre clé personnelle, ce qui pourrait permettre éventuellement de chiffrer des données spécifiques pour cet utilisateur, mais cette fonctionnalité n'est pas encore activée (! On distingue le chiffrement du droit d'accès: même si il n'y a pas de chiffrement, ce n'est pas pour cela que l'utilisateur dispose du droit de lecture ou d'écriture.)

Pourquoi ?

Le chiffrement est le moyen le plus sécurisé de mettre des données dans un cloud (ou sur un serveur) afin de les partager. En effet, les serveurs sont devenus des cibles d'attaques fréquentes même avec les standards de sécurité actuels (firewall, antivirus professionnel, détection du niveau d'activité, équipe informatique formée, restrictions réseau...) et il ne se passe plus un mois sans que des attaques soient médiatisées. Le plus souvent simplement pour détruire les données et exiger une rançon, mais à l'avenir peut-être pour les exploiter aussi (actuellement, le cas le plus fréquent étant que les utilisateurs consentent plus ou moins sciemment au partage de leurs données: cf GAFAM...). Ce phénomène est un obstacle important au partage des données de santé informatisées.

En pratique

- La première fois que vous accédez à Topaz, vous devez entrer votre clé personnelle puis la clé de groupe. Celles-ci sont alors stockées sur votre ordinateur.

- Si vous désinstallez Topaz, cela supprime votre clé. Quand vous le réinstaller, Topaz vous demande à nouveau votre clé personnelle et votre clé de groupe.

- On ne le répétera jamais assez : **vous devez stocker cette clé dans un endroit sécurisé sur support informatique et l'imprimer (double stockage).**