Objectif : messages clés pour la gestion des informations de ou fournies au nom de Lilly.

Pour les besoins de notre travail, les informations incluent à la fois des informations confidentielles et des informations personnelles que nous utilisons pour nos activités professionnelles. Les informations personnelles incluent toute information qui, utilisée seule ou avec d'autres informations, identifie un individu. Les informations confidentielles représentent toute information considérée comme confidentielle ou propriétaire par la partie divulguant.

Veuillez lire ce document et le transférer au sein de votre organisation aux personnes gérant actuellement les informations de ou fournies au nom de Lilly, ainsi qu'aux autres personnes qui rejoindront l'organisation à l'avenir.

Pourquoi est-ce important ?

- Votre organisation et son personnel sont des collaborateurs importants pour Lilly, et les mesures prises par vous-même et vos employés constituent la meilleure ligne de défense contre toute mise en péril des informations.
- La protection des informations est vitale pour Lilly et ses patients.

Les messages clés suivants, qui s'appuient sur les meilleures pratiques du secteur, dont le Cybersecurity Framework de NIST, doivent être incorporés aux pratiques actuelles pour continuer à réduire les risques liés à la gestion des informations.

En général :

- Évitez les copies redondantes au format papier ou électronique de documents contenant des informations, sauf en cas de nécessité absolue.

Stockage électronique des données

- Les fichiers électroniques contenant des informations doivent être stockés de façon sécurisée.
    - Étudiez la situation avec votre contact Lilly si un stockage externe ou des services cloud qui n'ont pas précédemment été mentionnés ou fait l'objet d'une autorisation de Lilly sont utilisés par votre organisation pour les informations de ou fournies au nom de Lilly.
    - L'accès aux fichiers électroniques qui incluent des informations ne doit être accordé qu'aux personnes devant être informées, pour le contenu minimal nécessaire et uniquement pendant la durée requise (privilège minimal).
    - L'accès doit être revu en fonction du degré de sensibilité. Cela inclut les emplacements de stockage que vous gérez, mais également ceux gérés par vos sous-traitants.
    - La désactivation doit se produire dans les meilleurs délais après la fin de contrat d'un employé ou lorsque les personnes n'ont plus besoin d'avoir accès aux informations pour leur travail.
- Les informations ne doivent pas être stockées aux emplacements suivants sans approbation de Lilly :
    - Tout dispositif de stockage amovible tel qu'un disque dur externe, une clé USB.
    - Appareils personnels des employés tels qu'ordinateur portable ou iPad.

Transfert électronique des données :

- Les fichiers électroniques contenant des informations doivent être transférés de façon sécurisée (en fonction du degré de sensibilité). Étudiez la situation avec votre contact Lilly pour trouver un accord sur la méthode de transfert à utiliser.
- Confirmez les adresses électroniques des destinataires avant l'envoi, et assurez-vous que seules les personnes ayant besoin de savoir dans le cadre de leur travail sont incluses.
- Les informations ne doivent PAS être transférées via :
    - Des dispositifs de stockage externes tels qu'un disque dur externe ou une clé USB (sans approbation de Lilly).
    - Des e-mails personnels.

Impression :

- L'impression d'informations sur des imprimantes personnelles ou dans des lieux publics est déconseillée. Si vous devez imprimer à domicile ou à l'extérieur, connectez un ordinateur portable ou tout autre appareil autorisé (par ex. iPad) à l'imprimante via un câble ou un réseau sans fil.

Téléconférences :

- Elles doivent être effectuées à l'aide de Skype for Business, Cisco WebEx ou Citrix GoToMeeting. Étudiez la situation avec votre contact Lilly si les options ci-dessus ne sont pas possibles.
- Les réunions en ligne ne sont pas enregistrées sans préavis ni approbation de Lilly.
- Faites attention à l'entourage et prenez les précautions nécessaires quand des informations sont au cœur de la discussion.

Sécurité physique :

- Conserver un espace de travail sécurisé :
    - Verrouillez l'accès à votre ordinateur DÈS que vous vous en éloignez.
    - Les ordinateurs portables et les iPads doivent être placés dans une armoire verrouillée, ou protégés à l'aide d'un câble antivol ou emportés avec vous lorsque vous terminez votre journée de travail.
    - Une fois votre journée de travail terminée, fermez à clé votre bureau, les armoires et les casiers.
    - Ne laissez pas les copies papier sur les imprimantes.
    - Dans la mesure du possible, utilisez les méthodes de transfert électronique convenues plutôt que les courriers papier, les envois postaux ou les télécopies.
    - Éliminez les informations de façon sécurisée (par ex., déchiquetage).

SMS :

- Les informations fournies par ou au nom de Lilly ne sont pas incluses dans des SMS.

Signalement d'incidents liés à la sécurité des informations :

- En cas d'incident lié à la sécurité des informations, contactez votre responsable des relations Lilly ou sponsor ET signalez un problème via la ligne d'assistance téléphonique consacrée aux questions d'éthique et de conformité pour un accès interne à Lilly ou EthicsPoint pour un accès externe.
  Les incidents peuvent inclure, sans s'y limiter, les éléments suivants :
    - Un e-mail contenant des informations a été envoyé accidentellement à un destinataire imprévu.
    - Vol ou perte d'un ordinateur portable, disque dur ou dispositif de stockage amovible contenant des informations.
    - Un sous-traitant doté d'un accès aux informations prévient votre société d'un incident.
    - Ransomware
      Si un écran similaire à celui illustré ci-dessous s'affiche, la mise en œuvre des actions suivantes peut aider à limiter les risques :
        - Débranchez le câble réseau ou désactivez l'adaptateur sans fil.
        - Mettez l'appareil en veille prolongée.

Attention au phishing !

- Le phishing est une technique utilisée par des tiers malveillants pour obtenir des informations en se faisant passer pour des entités dignes de confiance. Dès que vous cliquez sur une pièce jointe inconnue ou un lien contenu dans un e-mail, votre ordinateur et le réseau tout entier peuvent être compromis.

- Une tentative de phishing est un message inattendu qui possède presque toujours les caractéristiques suivantes :

    - Un appel urgent à accomplir une action (par exemple, retard de paiement de votre carte de crédit).
    - Un élément de temps (par exemple, action requise sous deux jours).
    - Une conséquence (par exemple, si vous ne réglez pas ce problème, vous aurez de graves ennuis).
    - Fautes de grammaire ou d'orthographe.
    - ET toujours un élément sur lequel il faut cliquer tel qu'un lien ou une pièce jointe.

- Effectuez une **P**ause et une **I**nspection. Fiez-vous à votre intuition. Si un e-mail semble suspect, prenez le temps d'examiner le message. Ne cliquez pas sur les liens et n'ouvrez pas les pièces jointes si vous ne les attendiez pas.

- Les personnes possédant une adresse e-mail Lilly feront partie du programme éducatif officiel de Lilly sur le phishing. Les noms des cliqueurs excessifs seront communiqués au tiers avec l'attente qu'ils suivent la formation. Étudiez la situation avec votre contact Lilly si vous avez des questions sur le programme éducatif officiel de Lilly sur le phishing. Si vous cliquez sur un lien ou ouvrez une pièce jointe dans un message que vous suspectez dans votre messagerie Lilly, signalez le problème via le site Operation Screen Door.

Si vous avez des questions ou des préoccupations :

- Étudiez la situation avec votre contact Lilly si vous avez des questions ou des préoccupations concernant les éléments traités dans ce document.
- Ces informations sont également disponibles sur le Supplier Porta (Portale fornitori) sous Protect Lilly.