Finalità: messaggi chiave per la gestione delle informazioni fornite da o per conto di Lilly.

Ai fini dell'attività lavorativa, le informazioni comprendono sia le Informazioni riservate che le Informazioni personali utilizzate per scopi aziendali. Le informazioni personali comprendono tutte le informazioni che, se utilizzate autonomamente o in combinazione con altre, identificano una persona. Le Informazioni riservate si definiscono come qualsiasi informazione ritenuta riservata o proprietaria dalla parte che la rivela.

Riesaminate e trasmettete questa documentazione a tutte le persone all'interno della vostra organizzazione che gestiscono informazioni fornite da o per conto di Lilly e ai futuri assunti.

Perché questo è importante?

- La vostra organizzazione e la sua forza lavoro offrono un importante contributo a Lilly e le azioni intraprese da voi o dal vostro personale costituiscono la prima e miglior linea di difesa contro la compromissione delle Informazioni.
- La protezione delle informazioni è essenziale per Lilly e per i pazienti che serviamo.

I seguenti messaggi chiave, ispirati alle miglior prassi del settore, compreso il NIST Cybersecurity Framework, devono essere introdotti nelle pratiche correnti per permette di ridurre ulteriormente il rischio insito nella gestione delle Informazioni.

In generale:

- Evitate di effettuare copie elettroniche o su carta di documenti contenenti Informazioni se non assolutamente necessario.

Archiviazione elettronica dei file:

- I file elettronici che comprendono Informazioni devono essere archiviati in modo sicuro.
    - Rivolgetevi al vostro contatto interno di Lilly qualora la vostra organizzazione utilizzasse servizi di archiviazione esterna o cloud non precedentemente noti o concordati con Lilly per le Informazioni fornite da o per conto di Lilly.
    - L'accesso ai file elettronici che comprendono le Informazioni dovrebbe essere garantito solamente a coloro che necessitino di tali Informazioni, limitatamente a quanto necessario e solo per il periodo di tempo necessario (privilegio minimo).
    - L'accesso deve essere riesaminato in base al grado di sensibilità delle Informazioni. Questo comprende gli archivi gestiti da voi e quelli gestiti dai vostri subfornitori.
    - La disattivazione deve essere eseguita tempestivamente quando una persona lascia l'azienda oppure non ha più motivo di accedere alle Informazioni ai fini dell'attività svolta.
- Le informazioni NON devono essere archiviate come segue se non previa autorizzazione di Lilly:
    - Qualsiasi dispositivo di archiviazione mobile come hard drive esterni o chiavette USB.
    - Dispositivi personali dei dipendenti come computer portatili o iPad.

Trasferimento elettronico dei file:

- I file elettronici che comprendono Informazioni devono essere trasferiti in modo sicuro (adeguato al grado di sensibilità dell'informazione). Rivolgetevi al vostro contatto Lilly per concordare il metodo di trasferimento da utilizzare.
- Confermate l'indirizzo e-mail dei destinatari prima dell'invio e assicuratevi che siano compresi solo gli indirizzi delle persone effettivamente interessate ai fini dell'attività svolta.
- Le informazioni NON devono essere trasferite tramite:
    - Dispositivi di archiviazione esterni come hard drive esterno o USB (senza autorizzazione di Lilly).
    - E-mail privata.

Stampa:

- La stampa delle informazioni su stampanti personali/private o presso postazioni pubbliche è sconsigliata. Qualora occorra stampare a casa o in strutture esterne, collegare alla stampante il proprio portatile o un dispositivo autorizzato (ad esempio, iPad) con un cavo o una rete wireless.

Teleconferenze:

- Devono essere condotte tramite Skype for Business, Cisco WebEx o Citrix GoToMeeting. Se questi canali non sono disponibili, rivolgersi al proprio contatto Lilly.
- Le riunioni online non devono essere registrate senza preavviso e approvazione preventiva di Lilly.
- Prestate attenzione ai luoghi circostanti e usate cautela durante l'esame delle Informazioni.

Sicurezza fisica:

- Mantenete uno spazio di lavoro sicuro:
    - Bloccate SEMPRE l'accesso al computer quando vi allontanate.
    - Accertatevi che i computer portatili e gli iPad siano riposti in un armadio con serratura o siano provvisti di blocco cavi, oppure portateli via quando lasciate il posto di lavoro a fine giornata.
    - Chiudete a chiave la vostra scrivania, gli armadi e l'ufficio/armadietto quando lasciate il posto di lavoro a fine giornata.
    - Non lasciate documenti stampati sulle stampanti.
    - Ogni volta che è possibile, utilizzate i metodi di trasferimento dati elettronici concordati invece di usare la e-mail, la spedizione per posta tradizionale o il fax.
    - Eliminazione sicura delle Informazioni (es., distruggerle).

Messaggi di testo:

- Le informazioni fornite da o per conto di Lilly non sono incluse in messaggi di testo

Segnalazione di incidenti relativi alla sicurezza delle Informazioni:

- In caso di incidenti relativi alla sicurezza delle Informazioni, rivolgetevi al vostro responsabile delle relazioni Lilly o allo sponsor E segnalate il caso alla linea di assistenza per l'etica e la compliance, se dipendenti o all'EthicsPoint, se collaboratori esterni.
  Tali incidenti includono, ad esempio:
    - E-mail contenenti Informazioni inviate accidentalmente a un destinatario diverso da quello previsto.
    - Smarrimento o furto di computer portatile, hard drive o dispositivo di archiviazione esterno contenente le Informazioni.
    - Segnalazione ricevuta da un subfornitore con accesso alle Informazioni.
    - Ransomware
      Se viene visualizzata sullo schermo una videata simile a quella sotto riportata, la procedura di seguito descritta potrebbe contribuire a ridurre il rischio:
        - Scollegare il cavo di rete o disabilitare l'adattatore wireless.
        - Avviare l'ibernazione.

Attenzione al phishing!

- Il phishing è un approccio utilizzato da malintenzionati esterni all'azienda per acquisire Informazioni aziendali confidenziali apparendo come un'entità affidabile. Facendo clic su un allegato sconosciuto o un link contenuto in una e-mail, si potrebbero compromettere il proprio computer e l'intera rete.

- Un tentativo di phishing è un messaggio inatteso che contiene quasi sempre:

    - Una richiesta di intervento immediato (per esempio, un ritardo di un pagamento su carta di credito).
    - Una scadenza temporale (per esempio, una scadenza entro due giorni).
    - Una conseguenza (per esempio, si richiede di risolvere un problema altrimenti si verificheranno situazioni spiacevoli).
    - Testo grammaticalmente scorretto o errori di ortografia.
    - E richiede sempre di fare clic su un certo link o allegato.

- **F**ermatevi e **V**erificate. Utilizzate il vostro intuito. Se una e-mail vi appare sospetta, leggete attentamente il messaggio. Non fate clic su link né aprite allegati che non vi aspettavate.

- Coloro che hanno un indirizzo e-mail Lilly prenderanno parte ad un programma formale di istruzione sul phishing di Lilly. I nomi degli interessati saranno comunicati ai terzi per i quali si prevede un addestramento di follow-up. Rivolgetevi al vostro contatto Lilly se avete domande relative al programma formale di istruzione sul phishing di Lilly. Se avete fatto clic su di un link o aperto un allegato che ritenete sospetto tramite la vostra e-mail Lilly, vi preghiamo di segnalarlo tramite il sito Operation Screen Door.

In caso di domande o dubbi:

- Rivolgetevi al vostro contatto Lilly se avete domande o dubbi relativi agli argomenti trattati in precedenza.
- Queste informazioni sono anche reperibili sul Supplier Portal (Portale fornitori) in Protect Lilly.