REGLAS COMERCIALES PARA EL MANEJO SEGURO DE LA INFORMACIÓN

Objetivo: Mensajes clave para el manejo de información de o proporcionada en nombre de Lilly, en lo sucesivo denominada Información.

¿Porque es importante esto?

- Su organización y su personal son colaboradores valiosos de Lilly, y las acciones que usted y su personal toman son parte de la primera y mejor línea de defensa frente al compromiso de la Información.
- La protección de la información es esencial para Lilly y los pacientes a quienes atendemos.

Los siguientes mensajes clave, que se basan en las mejores prácticas de la industria, incluido el Marco de Ciberseguridad del NIST, deben incorporarse a las prácticas actuales para continuar reduciendo el riesgo cuando se maneja la información.

En general:

- Evite hacer copias duplicadas electrónicas o impresas de documentos que contengan información a menos que sea absolutamente necesario.

Almacenamiento de datos electrónicos:

- Los archivos electrónicos que incluyen información deben almacenarse de forma segura. Los dispositivos de almacenamiento extraíbles, como discos duros externos y USB, no se pueden utilizar sin la aprobación de Lilly.
    - Se debe aplicar el principio de privilegio mínimo para otorgar acceso a los archivos (es decir, el acceso a la información solo debe otorgarse a quienes lo necesiten, no más de lo necesario y solo durante el tiempo requerido). El acceso debe revisarse de acuerdo con el nivel de sensibilidad. Esto incluye las ubicaciones de almacenamiento que administra, así como las administradas por sus subcontratistas.
    - La desactivación oportuna del acceso debe ocurrir después de una salida de la empresa o cuando las personas ya no tengan la necesidad comercial de acceder a la información.
- La información NO debe almacenarse en los siguientes lugares sin la aprobación de Lilly:
    - Los dispositivos personales de los empleados, como computadoras portátiles, iPad, etc.
    - Servicios o sitios de almacenamiento externo.

Transferencia electrónica de datos:

- Los archivos electrónicos que incluyen información deben transferirse de forma segura. Consulte a su contacto de Lilly para establecer el método preferido para la transferencia de información. Los dispositivos de almacenamiento extraíbles, como discos duros externos, CD/DVD y USB, no se pueden utilizar sin el permiso de Lilly.
- La información NO debe transferirse a través de:
    - Correo electrónico no seguro (a menos que el nivel de confidencialidad no lo garantice).
    - Dispositivos de almacenamiento externo como disco duro externo o USB (sin el permiso de Lilly).
    - Correo electrónico personal.

Teleconferencias y reuniones en línea:

- Utilice los servicios de reuniones aprobados por Lilly para programar y realizar reuniones sobre los negocios de la empresa. Consulte a su contacto de Lilly si tiene preguntas relacionadas con teleconferencias o reuniones en línea.
- Sea consciente de su entorno y tenga cuidado al hablar de información.

Seguridad física:

- Mantenga un espacio de trabajo seguro:
  - Bloquee el acceso a sus dispositivos en CUALQUIER momento que se aleje de ellos.
  - Los dispositivos deben colocarse en un gabinete con cerradura, cerrarse con cable o llevarse consigo cuando salga por el día, esté fuera por viaje de negocios o de vacaciones.
  - Cierre con llave su escritorio, gabinetes y casillero, y la oficina cuando se vaya por el día, esté de viaje de negocios o de vacaciones.
  - No deje copias impresas en las impresoras.
  - Descarte información de forma confidencial (por ejemplo, triturar).

Mensaje instantáneo y texto:

- Utilice una herramienta aprobada por Lilly para mensajes instantáneos y mensajes de texto para los negocios de la empresa. Consulte a su contacto de Lilly si tiene preguntas relacionadas con la mensajería instantánea o la mensajería de texto.

Notificación de incidentes de seguridad de la información:

- Informe los incidentes a su contacto de Lilly de manera oportuna. Los incidentes incluyen, entre otros:
  - El correo electrónico que contiene información se envió accidentalmente a un destinatario no deseado.
  - Se perdió o robaron una computadora portátil, un disco duro o un dispositivo de almacenamiento extraíble que contiene información.
  - Un subcontratista con acceso a la información alerta a su empresa sobre un incidente.
  - Reciba Ransomware, un tipo de software malicioso diseñado para bloquear el acceso al dispositivo hasta que se pague una suma. Vea el ejemplo a continuación. La realización inmediata de los siguientes pasos puede ayudar a reducir el riesgo:
    - Desenchufe el cable de red o desactive el adaptador inalámbrico.
    - Hibernar.

¡Tenga cuidado con la ingeniería social *(p. ej., phishing, vishing, SMiShing)***!:**

- La ingeniería social es el uso del engaño para manipular a las personas para que divulguen información confidencial o personal que pueda utilizarse con fines fraudulentos. Los estafadores se hacen pasar por una fuente confiable en un esfuerzo por robar identidades o recuperar información, como contraseñas, datos bancarios y números de tarjetas de crédito, etc.

- **Phishing** (a través de correo electrónico)
  - Un intento de phishing es un mensaje inesperado y las características incluyen:
    - Una llamada a la acción alarmante (por ejemplo, el pago de su tarjeta de crédito se atrasa).
    - Un elemento de tiempo (por ejemplo, algo vence en dos días).
    - Una consecuencia (por ejemplo, resuelva este problema, o le pasará algo malo).
    - Gramática deficiente o palabras mal escritas.
    - Y siempre tiene algo en donde "hacer clic", como un enlace o un archivo adjunto.
  - Si hace clic en un archivo adjunto o enlace desconocido en un correo electrónico, su computadora y toda la red podrían verse comprometidas.

- **Vishing** (a través de llamadas telefónicas o mensajes de voz)
  - Un intento de vishing (como el phishing pero por voz) es una llamada telefónica inesperada que:
    - Busca confirmación de información o solicita información.
    - Puede usarse en combinación con un ataque de phishing.
- **SMiShing** (a través de mensajes de texto SMS)
  - Un intento de SMiShing es un texto inesperado que:
    - Busca confirmación de información o solicita información.
    - Puede usarse en combinación con un ataque de phishing.
    - Por lo general, tiene algo donde "hacer clic", como un enlace o un archivo adjunto.

- **Si tiene una dirección de correo electrónico de Lilly**, participará en el Programa educativo formal sobre phishing de Lilly.
  - Se informará al empleador externo de las personas que hacen clic repetidamente con la expectativa de recibir orientación de seguimiento. Consulte a su contacto de Lilly si tiene preguntas sobre el Programa educativo formal sobre phishing de Lilly.
  - Si está utilizando una cuenta de correo electrónico de Lilly o365, informe los correos electrónicos sospechosos a través del botón “Report Phishing” (Informar sobre phishing) en la barra de herramientas “Home” (Inicio) de Outlook.

  - Si está conectado a la red interna de Lilly a través de VPN o virtual.lilly.com, informe los mensajes sospechosos a través de cyber@lilly.com.

- **Haga una pausa e investigue. Use su intuición:**
  - Si un correo electrónico parece sospechoso, tómese un momento para analizar el mensaje.
  - No haga clic en enlaces ni abra archivos adjuntos si no los esperaba.
  - Si no tiene una dirección de correo electrónico de Lilly y hace clic en un enlace o abre un archivo adjunto en un mensaje que cree que es sospechoso, infórmelo a través del proceso de su empleador.

Si tiene preguntas o inquietudes:

- Consulte a su contacto de Lilly si tiene preguntas o inquietudes relacionadas con cualquiera de los puntos mencionados anteriormente.
- Esta información también está disponible en el Supplier Portal (Portal de proveedores) bajo Responsabilidad Operativa en los Recursos del Proveedor.