Objetivo: mensajes clave para manejar información recibida por parte de Lilly o proporcionada en nombre de ella.

A los fines de nuestro trabajo, la información abarca tanto información confidencial como personal que utilizamos para cuestiones comerciales. La información personal incluye toda la información que identifique a un individuo cuando se la utiliza de manera independiente o combinada con otra información. La información confidencial se define como toda la información que la parte divulgante considera confidencial.

Revise y difunda en su organización a individuos que, actualmente, manejan información brindada por Lilly o proporcionada en su nombre, y a quienes se incorporen en el futuro.

¿Por qué es importante?

- Su organización y su fuerza de trabajo son valiosos contribuyentes de Lilly, y las acciones que tanto usted como su fuerza de trabajo llevan a cabo forman parte de la primera, y mejor, línea de defensa a fin de evitar que la información se vea comprometida.
- Proteger la información resulta fundamental, para Lilly y para los pacientes a los que prestamos servicios.

Los siguientes mensajes clave, elaborados sobre la base de las prácticas recomendadas del sector, incluido el Marco de trabajo sobre la seguridad cibernética de NIST (Instituto Nacional de Estándares y Tecnología), deberían incorporarse en las prácticas actuales para, de esta manera, continuar reduciendo los riesgos en el momento de manejar información.

En general:

- Evite realizar copias electrónicas o duplicados de documentos que contienen Información, a menos que sea absolutamente necesario.

Almacenamiento electrónico de datos:

- Los archivos electrónicos que contienen Información deben almacenarse de manera segura.
    - Trabaje junto con su contacto de Lilly en caso de que se utilicen servicios de nube o almacenamiento externo, no informados previamente ni acordados con Lilly, para manejar información brindada por Lilly o proporcionada en su nombre.
    - Solo debería otorgarse acceso a archivos electrónicos que incluyan Información a quienes tengan la necesidad de conocer dicha información, en una medida que no supere lo necesario y únicamente por el tiempo requerido (privilegio mínimo).
    - Debería revisarse el acceso a fin de que guarde coherencia con el nivel de confidencialidad. Esto incluye las ubicaciones de almacenamiento que maneja, así como aquellas que manejan los subcontratistas.
    - La desactivación debería tener lugar de inmediato tras la salida de la empresa o cuando los individuos dejan de tener una necesidad comercial de acceder a la información.
- NO debe almacenarse información en las siguientes ubicaciones sin la aprobación de Lilly:
    - Dispositivos de almacenamiento extraíbles, como unidades de disco duro externo o USBs.
    - Dispositivos personales de los empleados, como ordenadores portátiles o iPads.

Transferencia electrónica de datos:

- Los archivos electrónicos que contienen Información deben transferirse de manera segura (en consonancia con el nivel de confidencialidad). Trabaje junto con su contacto de Lilly para acordar el método de transferencia que ha de utilizarse.
- Confirme las direcciones de correo electrónico de los receptores antes del envío y asegúrese de que incluya únicamente a aquellos que tienen una necesidad comercial de conocimiento.

- La información NO debe transferirse a través de los siguientes medios:
    - Dispositivos de almacenamiento externo, como unidades de disco duro externo o USB (sin la aprobación de Lilly).
    - Correo electrónico personal.

Impresión

- Imprimir Información en impresoras hogareñas o personales, o en ubicaciones públicas se desaconseja. Si debe imprimir desde su hogar u otro lugar externo, conecte su ordenador portátil o dispositivo autorizado (por ejemplo, un iPad) a la impresora mediante un cable o una conexión inalámbrica.

Teleconferencias:

- Deberían llevarse a cabo con Skype Empresarial, Cisco WebEx o Citrix GoToMeeting. Trabaje junto con su contacto de Lilly en caso de que ninguna de las anteriores sea una opción viable.
- No grabe las reuniones en línea sin avisar o sin obtener la autorización previa de Lilly.
- Preste atención a su alrededor y tenga cuidado cuando hable sobre la Información.

Seguridad física:

- Preserve la seguridad del lugar de trabajo:
    - Bloquee el acceso a su ordenador CADA VEZ que se aleje de él.
    - Asegúrese de que los ordenadores portátiles y los iPad estén guardados bajo llave en un gabinete o cajón, o cerrados con cable y candado, o bien, lléveselos con usted cuando termine su jornada laboral.
    - Cierre con llave su escritorio, gabinetes y casillero/oficina cuando termine su jornada de trabajo.
    - No deje hojas impresas en las impresoras.
    - Utilice métodos de transferencia electrónica autorizados siempre que sea posible en lugar de enviar por correo electrónico, correo postal o fax.
    - Descarte la Información de manera segura (por ejemplo, por medio de la trituración).

Mensajes de texto:

- La información proporcionada por o en nombre de Lilly no está incluida en los mensajes de texto

Denunciar incidentes relacionados con la seguridad de la Información:

- Si se produce un incidente relacionado con la seguridad de la Información, póngase en contacto con su gerente de relaciones o patrocinador de Lilly, E informe el hecho a través de la línea directa de Ética y Cumplimiento, en caso de que se trate de un acceso interno de Lilly, o a través de EthicsPoint, si es externo.
  Estos son solo algunos ejemplos de incidentes:
    - Correo electrónico con Información se envió por accidente a un destinatario no deseado.
    - Se perdió o robó un ordenador portátil, un disco duro o un dispositivo de almacenamiento extraíble que contiene Información.
    - Un subcontratista con acceso a Información alerta de la ocurrencia de un incidente a la empresa.
    - Ransomware
      Si le aparece una pantalla similar a la que se muestra abajo, siga estos pasos para contribuir a reducir el riesgo:
        - Desconecte el cable de red o desactive el adaptador inalámbrico.
        - Ponga el equipo a hibernar.

¡Tenga cuidado con el phishing!

- El phishing es un enfoque utilizado por ajenos con intencionalidad maliciosa de adquirir Información al hacerse pasar por una entidad confiable. Toda vez que hace clic en un adjunto o enlace desconocidos incluidos en un correo electrónico, tanto su ordenador como la totalidad de la red pueden verse afectados.

- Un intento de phishing es un mensaje inesperado y, por lo general, suele incluir lo siguiente:

    - Un llamado a la acción "urgente" (por ejemplo, el pago de su tarjeta de crédito está vencido).
    - Un elemento de tiempo (por ejemplo, algo que debe hacerse, como máximo, en dos días).
    - Una consecuencia (por ejemplo, solucione el problema o algo malo le ocurrirá).
    - Palabras mal escritas o con errores gramaticales.
    - Y, siempre, tiene algún lugar en el que debe hacerse "clic", como un enlace o un adjunto.

- **D**eténgase e **I**nspeccione. Recurra a su intuición. Si un correo electrónico parece sospechoso, tómese un momento para leer el mensaje con detenimiento. No haga clic en adjuntos, ni los abra, si no los espera.

- Todos aquellos que posean una dirección de correo electrónico de Lilly serán parte del programa formal y educativo sobre el phishing de Lilly. Los nombres de quienes hagan clic de manera reiterada se informarán al tercero a fin de que se realice una orientación de seguimiento. Trabaje junto con su contacto de Lilly si tiene alguna pregunta en relación con el programa formal y educativo sobre el phishing de Lilly. Si hace clic en un enlace o abre un adjunto en un mensaje que considera sospechoso en su correo electrónico de Lilly, informe el hecho a través de Operation Screen Door.

Si desea realizar alguna pregunta o tiene inquietudes:

- Trabaje junto con su contacto de Lilly si tiene alguna pregunta o inquietud en relación con alguno de los temas mencionados.
- Esta información también se encuentra disponible en Supplier Portal (Portal de proveedores) en Protect Lilly.

15 July 2017