

Objetivo: Principais mensagens para o tratamento de informações da ou fornecidas em nome da Lilly.

Para fins do nosso trabalho, o termo informações engloba tanto informações confidenciais quanto pessoais que usamos para objetivos comerciais. As informações pessoais incluem aquelas que, quando usadas de modo independente ou em combinação, identificam um indivíduo. As informações confidenciais são definidas como aquelas consideradas sigilosas ou proprietárias pela parte divulgadora.

Análise e faça o encadeamento na sua organização para os indivíduos atualmente tratando as informações da Lilly ou fornecidas pela Lilly e para aqueles que vão lidar com essas informações no futuro.

Por que isso é importante?

- Sua organização e sua força de trabalho são colaboradores valiosos para a Lilly e as ações que você e sua força de trabalho executam fazem parte da primeira e melhor linha de defesa contra o comprometimento de informações.
- A proteção de informações é essencial para a Lilly e os pacientes que atendemos.

As principais mensagens a seguir, que são informadas pelas práticas recomendadas do setor, incluindo a NIST Cybersecurity Framework, devem ser incorporadas nas práticas atuais para continuar a reduzir o risco durante o tratamento de informações.

Em geral:

- Evitar fazer cópias eletrônicas ou impressas de documentos contendo informações, a menos que seja absolutamente necessário.

Armazenamento de dados eletrônicos:

- Arquivos eletrônicos que incluem informações devem ser armazenados com segurança.
 - Trabalhe com seu Contato da Lilly se armazenamento externo ou serviços de nuvem não previamente divulgados ou estabelecidos com a Lilly forem utilizados pela sua organização para informações da Lilly ou fornecidas em nome da Lilly.
 - O acesso a arquivos eletrônicos que incluem informações só deve ser concedido às pessoas que precisarem, não mais do que elas e apenas pelo tempo necessário (privilegio mínimo).
 - O acesso deve ser analisado proporcional ao nível de confidencialidade. Isso inclui os locais de armazenamento que você gerencia e aqueles administrados por subcontratados.
 - A desativação só deve ocorrer oportunamente após uma saída da empresa ou quando os indivíduos não tiverem mais a necessidade de negócio de acesso à informação.
- As informações NÃO devem ser armazenadas nos seguintes locais sem a aprovação da Lilly:
 - Qualquer dispositivo de armazenamento removível, como discos rígidos externos ou USBs.
 - Dispositivos pessoais dos funcionários, como laptops ou iPads.

Transferência de dados eletrônicos:

- Arquivos eletrônicos que incluem informações devem ser transferidos com segurança (proporcional ao nível de confidencialidade). Trabalhe com seu Contato da Lilly para estabelecer o método de transferência a ser usado.
- Confirme os endereços de e-mail dos destinatários antes de enviar e assegurar que eles incluem apenas aqueles com necessidades de negócios.
- As informações NÃO devem ser transferidas via:
 - Dispositivos de armazenamento externo, como disco rígido externo ou USB (sem aprovação da Lilly).
 - E-mail pessoal.

Impressão:

- Não é recomendável imprimir informações em impressoras residenciais/pessoais ou em locais públicos. Se for necessário imprimir em sua residência ou em um local externo, conecte um laptop ou outro dispositivo autorizado (por exemplo, um iPad) à impressora por meio de um cabo ou rede sem fio.

Teleconferências:

- Devem ser realizadas com o Skype for Business, Cisco WebEx ou Citrix GoToMeeting. Trabalhe com seu Contato da Lilly se não houver uma dessas opções disponível.
- As reuniões on-line não são gravadas sem aprovação e aviso prévios da Lilly.
- Esteja consciente de seu entorno e seja cauteloso ao discutir as informações.

Segurança física:

- Mantenha um espaço de trabalho seguro:
 - Bloqueie o acesso ao seu computador SEMPRE que se distanciar de sua mesa.
 - Assegure-se de que os laptops e iPads estejam protegidos em um armário com chave ou o cabo bloqueado ou leve-os consigo quando você for embora.
 - Tranque sua mesa, gabinetes e armário/escritório quando for embora.
 - Não deixe as impressões nas impressoras.
 - Use os métodos de transferência eletrônica estabelecidos sempre que possível, em vez de expedições, remessa ou fax.
 - Descarte as informações com segurança (por exemplo, destruindo-as).

Mensagens de texto:

- As informações fornecidas por/em nome da Lilly não são incluídas nas mensagens de texto

Relatórios de incidentes de segurança de informações:

- Se houver um incidente de segurança de informações, entre em contato com o gerente de relacionamento da Lilly ou patrocinador E informe uma preocupação por meio da Linha Direta de Conformidade e Ética se tiver acesso interno da Lilly ou EthicsPoint se o seu acesso for externo.

Os incidentes podem incluir, sem limitação:

- E-mails com informações enviados acidentalmente a um destinatário não pretendido.
- Laptops, discos rígidos ou dispositivos de mídia removível que contêm informações perdidos ou roubados.
- Um subcontratado com acesso às informações alerta sua empresa sobre um incidente.
- Ransomware

Se for exibida uma tela semelhante à que é mostrada abaixo, executar as etapas a seguir pode ajudar a reduzir o risco:

- Desconecte o cabo de rede ou desative o adaptador sem fio.
- Coloque o dispositivo para hibernar.



Tome cuidado com o Phishing!

- O phishing é uma abordagem usada por intrusos mal-intencionados para adquirir Informações fingindo ser uma entidade confiável. Depois que você clicar em um anexo ou link desconhecido em um e-mail, seu computador e toda a rede poderão ser comprometidos.
- Uma tentativa de phishing é uma mensagem inesperada e quase sempre tem:
 - Uma chamada à ação alarmante (por exemplo, seu pagamento do cartão de crédito está atrasado).
 - Um elemento de tempo (por exemplo, algo que vence em dois dias).
 - Uma consequência (por exemplo, resolva o problema ou algo de ruim vai acontecer com você).
 - Gramática ruim ou má ortografia.
 - E sempre é preciso clicar em algo, como um link ou anexo.
- **Faça uma pausa e Inspeção.** Use sua intuição. Se um e-mail parecer suspeito, pare um instante para examinar a mensagem com atenção. Não clique em links, nem abra anexos que não estava esperando.
- As pessoas que têm um endereço de e-mail da Lilly farão parte de um programa de phishing educativo formal da Lilly. Os nomes dos clicadores frequentes serão informados ao terceiro com uma expectativa de coaching de acompanhamento. Trabalhe com seu Contato da Lilly se você tiver dúvidas sobre o programa educativo de phishing formal da Lilly. Se você clicar em um link ou abrir um anexo em uma mensagem que considerar suspeita de seu e-mail da Lilly, informe via [Operation Screen Door](#).

Em caso de dúvidas ou preocupações:

- Trabalhe com seu Contato da Lilly se você tiver dúvidas ou preocupações relacionadas a qualquer um dos itens discutidos acima.
- Essas informações também podem ser encontradas no [Portal do Fornecedor](#) na Protect Lilly.