

Doel: belangrijke berichten voor de behandeling van gegevens van of geleverd namens Lilly.

Ten behoeve van onze werkzaamheden verstaan we onder informatie zowel vertrouwelijke informatie als persoonlijke gegevens die we voor zakelijke doeleinden gebruiken. Persoonlijke gegevens omvatten alle gegevens die, apart of in combinatie met andere gegevens, een persoon kunnen identificeren. Vertrouwelijke informatie wordt gedefinieerd als informatie die door de onthullende partij als vertrouwelijk of bedrijfseigen wordt beschouwd.

Bespreek dit binnen uw organisatie en meld dit aan personen die momenteel informatie van of geleverd namens Lilly behandelen en aan mensen die in de toekomst in dienst komen.

Waarom is dit belangrijk?

- Wij waarderen de bijdragen van uw organisatie en uw werknemers aan Lilly en de acties van u en uw werknemers zijn onderdeel van onze eerste en beste verdedigingslinie tegen aantasting van gegevens.
- Het is essentieel voor Lilly en de patiënten die we dienen dat we informatie beschermen.

Neem de volgende belangrijke principes, op basis van best practices uit de sector zoals het Cybersecurity Framework van NIST, op in uw huidige praktijken om risico's bij de behandeling van gegevens verder te beperken.

Algemeen:

- Maak geen dubbele elektronische of gedrukte kopieën van documenten met vertrouwelijke informatie, tenzij dit absoluut nodig is.

Elektronische gegevensopslag:

- Elektronische bestanden met informatie moeten veilig worden opgeslagen.
 - Overleg met uw Lilly-contactpersoon als niet eerder bekendgemaakte of met Lilly afgesproken externe opslagmiddelen of cloudservices worden door uw organisatie gebruikt voor informatie van of geleverd namens Lilly.
 - Toegang tot elektronische bestanden met informatie moet alleen worden verleend aan degenen die de informatie nodig hebben voor hun werk. Zij mogen uitsluitend toegang tot de hoognodige informatie hebben en alleen gedurende de benodigde periode (beperkte rechten).
 - Bij de verlening van toegang moet worden gekeken naar de mate van vertrouwelijkheid. Hieronder vallen opslaglocaties die u beheert en locaties die worden beheerd door uw onderaannemers.
 - Wanneer een persoon vertrekt bij het bedrijf of voor het werk geen toegang tot de gegevens meer hoeft te hebben, moet de toegang meteen worden ingetrokken.
- Zonder goedkeuring van Lilly mogen er geen gegevens worden opgeslagen op de volgende locaties:
 - Verwisselbare opslagmedia, zoals externe harde schijven of USB-schijven.
 - Persoonlijke apparaten van werknemers, zoals laptops of iPads.

Elektronische gegevensoverdracht:

- Elektronische bestanden met informatie moeten veilig worden overgedragen (conform het niveau van vertrouwelijkheid). Maak met uw Lilly-contactpersoon afspraken over de te gebruiken overdrachtsmethode.
- Controleer voor verzending de e-mailadressen van de beoogde ontvangers en zorg ervoor dat alleen die personen het bericht krijgen die het bericht nodig hebben voor hun werk.
- Gegevens mogen NIET worden overgedragen via:
 - Externe opslagapparaten, zoals een externe harde schijf of een USB-schijf (zonder goedkeuring van Lilly).
 - Persoonlijke e-mail.

Afdrukken:

- Druk bij voorkeur geen informatie af op thuis-/privéprinters of op openbare locaties. Als u thuis of bij een extern printbedrijf moet afdrukken, moet u uw Lilly-laptop of een ander door Lilly goedgekeurd apparaat (bijvoorbeeld een iPad) met een kabel of via een draadloos netwerk met de printer verbinden.

Teleconferenties:

- Gebruik hiervoor Skype voor Bedrijven, Cisco WebEx of Citrix GoToMeeting. Overleg met uw Lilly-contactpersoon als deze geen optie voor u zijn.
- Online vergaderingen mogen alleen worden geregistreerd na kennisgeving aan en voorafgaande toestemming van Lilly.
- Wees u bewust van uw omgeving en wees voorzichtig wanneer u vertrouwelijke informatie bespreekt.

Fysieke beveiliging:

- Zorg voor een veilige werkplek:
 - Blokkeer de toegang tot uw computer ALTIJD wanneer u uw computer onbeheerd achterlaat.
 - Wanneer u aan het eind van de dag uw werkplek verlaat, moet u laptops en iPads in een afgesloten kast leggen, met een kabel vastmaken of met u meenemen.
 - Sluit uw bureau, kasten en locker/kantoor af wanneer u aan het eind van de dag vertrekt.
 - Laat geen afdrukken op printers liggen.
 - Gebruik zoveel mogelijk afgesproken methoden voor elektronische verzending in plaats van reguliere postverzending of faxen.
 - Zorg voor een veilige vernietiging van vertrouwelijke gegevens (bijvoorbeeld door versnipperen).

Sms-berichten:

- Informatie die door of namens Lilly wordt verstrekt, wordt niet via sms-berichten verzonden.

Incidenten met beveiliging van informatie melden:

- Neem in het geval van een incident met de beveiliging van informatie contact op met uw Lilly-relatiemanager of sponsor EN meld een zorg via de hotline voor Ethics and Compliance als u een Lilly-werknemer bent of via EthicsPoint als u geen Lilly-werknemer bent.

Voorbeelden van incidenten zijn:

- U hebt per ongeluk een e-mail met vertrouwelijke informatie naar een ongewenste ontvanger gestuurd.
- Een laptop, harde schijf of verwisselbaar opslagapparaat met vertrouwelijke informatie is verloren of gestolen.
- Een onderaannemer met toegang tot vertrouwelijke informatie waarschuwt uw bedrijf voor een incident.
- Ransomware

Als u een scherm zoals hieronder ziet, kunt u met de volgende stappen mogelijk de risico's beperken:

- Koppel de netwerkkabel los of schakel de wifi-adapter uit.
- Activeer de slaapstand.



Wees bedacht op phishing

- Phishing is een methode die kwaadwillende outsiders gebruiken om vertrouwelijke bedrijfsinformatie te verkrijgen door zich voor te doen als een betrouwbare eenheid. Als u op een onbekende bijlage of koppeling in een e-mail klikt, brengt u uw computer en het volledige Lilly-netwerk in gevaar.
- Een phishing-poging is een onverwacht bericht en heeft vrijwel altijd de volgende elementen
 - Een alarmerende oproep (bijvoorbeeld dat uw creditcardbetaling te laat is).
 - Een tijdselement (iets gebeurt bijvoorbeeld binnen twee dagen).
 - Een gevolg (bijvoorbeeld dat u het probleem moet oplossen omdat er anders iets naars met u gebeurt).
 - Slecht gestelde zinnen of taal- en schrijffouten.
 - EN altijd iets waarop u moet klikken, zoals een koppeling of een bijlage.
- **Pauzeer en Inspecteer.** Gebruik uw intuïtie. Bekijk een e-mail extra goed als deze verdacht lijkt. Klik niet op koppelingen of bijlagen als u die niet verwacht.
- Personen met een Lilly-mailadres maken deel uit van het formele educatieve programma over phishing van Lilly. De namen van mensen die vaker op koppelingen klikken, worden aan de externe partij doorgegeven waarbij wordt verwacht dat deze personen nadere coaching krijgen. Overleg met uw Lilly-contactpersoon bij vragen over het formele educatieve programma over phishing van Lilly. Als u op een koppeling hebt geklikt of een bijlage hebt geopend in een verdacht bericht in uw Lilly-mail, meldt u dit via [Operation Screen Door](#).

Bij vragen of zorgen:

- Overleg met uw Lilly-contactpersoon als u vragen of zorgen hebt met betrekking tot de hiervoor beschreven punten.
- U kunt deze informatie ook vinden op het [leveranciersportal](#) onder Protect Lilly.