情報の安全な取り扱いに関するビジネス ルール

目的:Lilly または Lilly の代理人から提供される情報を取り扱うための重要なメッセージ (以下、「情報」と呼びます)。

重要である理由

- あなたの組織とその従業員は Lilly にとって価値ある貢献者であり、あなたとその従業員が取る行動は、情報の侵害に対する最も重要で最善の自衛策の一部である。
- 情報の保護は、Lilly と私たちがサービスを提供する患者にとって不可欠なものである。

NIST サイバーセキュリティ フレームワークを含む業界のベスト プラクティスによって通知される次の重要なメッセージは、情報を取り扱う際のリスクを引き続き軽減するために、現在の行動に取り入れる必要があります。

一般情報:

- 絶対に必要な場合以外は、情報を含むドキュメントの電子コピーまたはハード コピーを複製しないでください。

電子データ ストレージ:

- 情報を含む電子ファイルは安全に保管する必要があります。Lilly の承認なしに、外付けハード ドライブや USB などのリムーバブル記憶装置を使用することはできません。
    - 最小特権の原則は、ファイルへのアクセス権を与えるために適用する必要があります (つまり、情報へのアクセス権は、情報を知る必要がある人にのみ、必要最小限の情報へのアクセスに限定し、必要な時間だけ与える必要があります)。アクセス権は、機密性に応じて確認する必要があります。これには、あなた自身が管理する保存場所と下請け業者が管理する保存場所が含まれます。
    - アクセス権の非アクティブ化は、個人が会社を離れた後または情報にアクセスする必要がなくなったときに適時に行う必要があります。
- Lilly の承認なしに、次の場所に情報を保存しないでください:
    - ラップトップや iPad などの従業員の私用デバイス
    - 外部のストレージ サービスまたはサイト

電子データ転送:

- 情報を含む電子ファイルは安全に転送する必要があります。Lilly に問い合わせて、優先する情報転送方法を確立してください。Lilly の承認なしに、外付けハード ドライブ、CD/DVD、USB などのリムーバブル記憶装置を使用することはできません。
- 以下の手段で情報を転送しないでください。
    - セキュリティで保護されていない電子メール (機密レベルを保証しない場合を除く)
    - 外付けハード ドライブや USB などの外部ストレージ デバイス (Lilly の承認を得てないもの)
    - 個人的な電子メール

電話会議/オンライン会議:

- 会社のビジネスに関する会議をスケジューリングおよび実施する際は、Lilly が承認した会議サービスを使用してください。電話会議/オンライン会議について不明な点がある場合は、Lilly まで問い合わせてください。
- 情報について話し合うときは、周囲の状況に気を配ってください。

物理的セキュリティ:

- 安全なワークスペースを維持します。
    - デバイスから離れるときは必ず、デバイスを利用できない状態にしてください。

- 一日中外出する際、出張中、または休暇中は、デバイスを施錠可能なキャビネットに収納したり、ケーブルをロックしたり、持ち返ったりする必要があります。
- 一日中外出する際、出張中、休暇中は、机、キャビネット、ロッカー/オフィスを施錠してください。
- プリンタにハード コピーを残さないでください。
- 情報は外に漏れないように破棄してください (例: 細断する)。

インスタント メッセージおよびテキスト:

- 会社のビジネス用のインスタント メッセージやテキスト メッセージには、Lilly が承認したツールを利用してください。インスタント メッセージングまたはテキスト メッセージングについて不明な点がある場合は、Lilly までお問い合わせください。

情報セキュリティ インシデントの報告:

- インシデントは適時に Lilly まで報告してください。インシデントには次のようなものがありますが、これらに限定されません。
  - 情報を含む電子メールが意図しない相手に誤って送信された。
  - 情報を含むラップトップ、ハード ドライブ、またはリムーバブル ストレージ デバイスの紛失または盗難が発生した。
  - 情報へのアクセス権を持つ下請け業者から、インシデントに対する注意を喚起された。
  - 金額が支払われるまでデバイスへのアクセスをブロックするように設計された悪意のあるソフトウェアの一種であるランサムウェアを受け取った。この場合は、以下の例を参照してください。次の手順をすぐに実行すると、リスクを軽減できる場合があります。
    - ネットワーク ケーブルを抜くか、またはワイヤレス アダプタを無効にする。
    - 休止状態にする。

ソーシャル エンジニアリングに注意してください *(例: フィッシング、ビッシング、スミッシング)* **!:**

- ソーシャル エンジニアリングとは、詐欺目的で使用される可能性のある機密情報や個人情報を漏らすよう個人を操作するために不正な手段を取ることです。詐欺師は、信頼できる情報源になりすまして、ID を盗んだり、パスワード、銀行の詳細情報、クレジット カード番号などの情報を取得したりします。
  - **フィッシング** (電子メール)
    - フィッシングの試みは予期しないメッセージによるものであり、次のような特徴があります。
      - 警戒を促すフレーズが含まれる (クレジット カードの支払いが遅れているなど)。
      - 時間的な要素が含まれる (2 日以内に期限が来るなど)。

        - もたらされる結果が含まれる (この問題を解決しないと悪いことが起こるなど)。
        - 文法や単語のつづりに間違いがある。
        - リンクや添付ファイルなど、必ず「クリック」するものがある。
      - 電子メール内の不明な添付ファイルまたはリンクをクリックすると、コンピューターとネットワーク全体が危険にさらされる可能性があります。

  - **ビッシング** (電話または音声メッセージ)
    - ビッシング (ボイス フィッシング) の試みは、次のような予期しない電話によるものです。
      - 情報の確認を求める、または情報を要求する。
      - フィッシング攻撃と組み合わせて使用されることもある。
  - **スミッシング** (SMS テキスト メッセージ)
    - スミッシングの試みは、次のような予期しないテキストによるものです。
      - 情報の確認を求める、または情報を要求する。
      - フィッシング攻撃と組み合わせて使用されることもある。
      - 通常、リンクや添付ファイルなど、「クリック」するものがある。

- **Lilly のメール アドレスをお持ちの場合は**、Lilly の正式な教育用フィッシング プログラムに参加できます。
  - 何度もクリックする人は、フォローアップ コーチングのために第三者に報告されます。Lilly の正式な教育用フィッシング プログラムに関するご質問は、Lilly までお問い合わせください。
  - Lilly o365 電子メール アカウントを使用している場合は、Outlook の [Home (ホーム)] リボンの [Report Phishing (フィッシングの報告)] ボタンから疑わしい電子メールを報告してください。

  - VPN または virtual.lilly.com を介して内部の Lilly ネットワークに接続している場合は、cyber@lilly.com

- **間を置いて調べてみてください。直感を働かしてください。**
  - 電子メールが疑わしい場合は、メッセージをよく見てください。
  - リンクをクリックしたり、受信を予想していない添付ファイルを開いたりしないでください。
  - Lilly のメール アドレスをお持ちでなく、疑わしいメッセージのリンクをクリックしたり、添付ファイルを開いたりした場合は、雇用主のプロセスに従って報告してください。

ご質問やご不明な点がある場合:

- 上記のいずれかの項目に関連する質問や不明な点がある場合は、Lilly までお問い合わせください。
- この情報は、「Supplier Resources (サプライヤー リファンレス)」の「Operating Responsibility (運用責任)」の下にある「Supplier Portal (サプライヤー ポータル)」に記載されています。