目的:リリーまたは リリーの代理から提供された「情報」を取り扱う際の留意事項

日本イーライリリー株式会社（リリー）の業務上の目的において、「情報」には、当社が事業目的で使用する秘密情報と個人情報の両方が含まれます。個人情報には、単独またはその他の情報と組み合わせて個人を特定できるような情報が含まれます。秘密情報とは、開示者が秘密と見なす、または公開されていないと見なすあらゆる情報を指します。

貴社の組織内で確認し、リリーまたはリリーの代理から提供される情報を現在取り扱っている担当者、および今後担当する従業員に伝達してください。

重要なポイント

- 貴社と従業員はリリーにとって大切なビジネスパートナーであり、貴社と従業員がとる行動は、情報への不正アクセスを食い止める第一線の重要な一部となります。
- 情報を保護することは、リリー と患者さんにとって非常に重要です。

以下のキー メッセージは、NIST(National Institute of Standards and Technology：米国国立標準技術研究所)の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 プラクティスに基づいたものであり、「情報」を取り扱う際のリスクを引き続き下げるために、現在の方法に組み入れていただく必要があります。

全般:

- どうしても必要な場合を除き、「情報」を含む文書の電子コピーまたはハードコピーの作成は避けてください。

電子データの保管:

- 「情報」が含まれている電子ファイルは、安全に保管する必要があります。
    - リリー またはリリーの代理から提供される「情報」を保管するために、今までリリーに知らせていない、またはリリーとの合意に至っていない外部のストレージまたはクラウドサービスを使用する場合は、リリー担当者に相談する。
    - 「情報」が含まれている電子ファイルへのアクセス権は、知る必要がある人に限定し、内容も必要な範囲に限り、必要期間のみ(最低限の権限)に限定して付与する。
    - 機密レベルに見合ったアクセス権が付与されていることを確認する。これには、貴社が管理する保管場所だけではなく、貴社からの下請負業者が管理する保管場所も含まれる。
    - 社員が退職した場合、または「情報」にアクセスする業務上の必要性がなくなった場合は、速やかにアクセスを無効にする。
- リリー からの許可なく、以下の場所に「情報」を保管することを禁止します。
    - リムーバブル記憶装置（外付けハードドライブ、USBなど）
    - 社員の個人所有デバイス（ノートパソコン、iPadなど）

電子データ転送:

- 「情報」が含まれている電子ファイルは、機密レベルに合わせて安全に転送する必要があります。リリー担当者と相談して、利用する転送方法を決めてください。
- 送信前に受信者の電子メール アドレスを確認した後、業務上知る必要性のある人以外は含まれていないことを確認します。
- 次の方法で情報を転送することを禁止します。
    - 外付けハードドライブ、USB などのリムーバブル記憶装置 (リリーからの許可がない場合)
    - 個人の電子メール

印刷:

- 自宅/個人所有のプリンタまたは公共の場で「情報」を印刷することは推奨されません。自宅または社外で印刷する必要がある場合は、ラップトップまたはその他の許可されたデバイス (iPad など) をケーブルまたはワイヤレスネットワークでプリンタに接続してください。

電話会議:

- Skype for Business、Cisco WebEx、または Citrix GoToMeeting を使用して実施してください。いずれも使用できない場合は、リリー担当者に相談してください。
- 通知および リリーからの事前承認なく、オンライン会議を記録しないようにしてください。
- 「情報」について話し合う際は、周囲を意識し注意を払ってください。

物理的セキュリティ:

- 安全な職場の維持:
    - コンピュータから離れるときは、コンピュータを常にロックする。
    - 帰宅するときには、施錠できるキャビネットにラップトップと iPad を保管するか、ケーブルでロックするか、自宅に持ち帰る。
    - 帰宅時には、机、キャビネット、ロッカー/オフィスを施錠する。
    - ハードコピーをプリンタに置いたままにしない。
    - 可能な場合は、郵送、配送、またはファックスは使用せずに、常に合意した電子転送方法を使用する。
    - 「情報」を安全に破棄する (シュレッダーにかけるなど)。

テキスト メッセージング(ショートメッセージサービス(SMS)の電子メールなど):

- リリーまたは リリーの代理から提供された「情報」はテキストメッセージに含めないでください。

情報セキュリティ インシデント報告:

- 情報セキュリティ インシデントが発生した場合は、リリー 担当者に連絡してください。
  インシデントには次のものがありますが、これらに限定されるものではありません。
    - 「情報」が含まれている電子メールを誤った送信先に送信した。
    - 「情報」が保存されているラップトップ、ハードドライブ、またはリムーバブル記憶装置を紛失した、または盗まれた。
    - 「情報」にアクセスできる下請負業者から、貴社にインシデント通報があった。
    - ランサムウェア
      以下の画面に類似した画面が表示された場合は、リスクを軽減するために以下の手順に従ってください。
        - ネットワークケーブルを抜くか、ワイヤレスアダプタを無効にする。
        - コンピュータを休止状態にする。

フィッシング詐欺に注意!

- フィッシング詐欺は、信頼できる実在する企業を装って情報を入手するために悪意のある部外者が使用する手口です。電子メールに記載されている不明な添付ファイルまたはリンクをクリックすると、コンピュータやネットワーク全体が侵害される恐れがあります。
- フィッシング詐欺は予想外の出来事に関するメッセージで企てられ、ほとんどの場合、以下のような特徴があります。
  - 対応を要求する警告 (例: クレジット カードの支払いが遅れている)。
  - 時間的要素 (例: 何かの締め切りまであと 2 日)。
  - 結果 (例: この問題を解決しないと何か悪いことが起きる)。
  - 文法が稚拙であったり、スペルが間違ったりしている。
  - リンクや添付ファイルなど、何か「クリック」するものが必ず付いている。

- 手を止めて考え、勘を働かせてください。疑わしい電子メールは、注意深く観察してください。受信を予期していたものでなければ、リンクをクリックしたり、添付ファイルを開いたりしないでください。
- リリー の電子メール アドレスを使用する人は、リリー公式のフィッシング詐欺教育プログラムの対象になります。何度もクリックしてしまう人の名前は第三者機関に通知され、フォローアップコーチングを受けていただきます。リリー公式のフィッシング詐欺教育プログラムに関して質問がある場合は、リリー担当者に相談してください。リリー電子メールから疑わしいメッセージに記載されているリンクをクリックしたり、添付ファイルを開いてしまったりした場合は、リリーの報告システムである Operation Screen Door を利用して報告してください。

質問または懸念がある場合:

- 上記の内容に関して質問または懸念がある場合は、リリー担当者にご相談ください。
- この情報は、リリーホームページ の「購買の手続きについて」でもご覧いただけます。