**有关安全处理信息的业务规则**

**目的：有关处理来自 Lilly 公司或代表 Lilly 公司提供的信息（以下简称为“信息”）的关键消息。**

**为什么这很重要？**

- 您的组织及员工是 Lilly 的重要贡献者，您和您的员工所采取的行动是抵御信息泄露的第一道防线，也是最好的防线。
- 保护信息对于 Lilly 以及我们服务的患者至关重要。

通过行业最佳实践（包括 NIST 网络安全框架）总结出的以下关键信息应纳入到当前的实践中，以继续降低处理信息时的风险。

**一般原则：**

- 除非绝对必要，否则请避免重复制作包含信息的文档的电子或纸质副本。

**电子数据存储：**

- 包含信息的电子文件必须安全存储。未经 Lilly 公司批准，不得使用可移动存储设备，例如外部硬盘驱动器和 USB。
    - 授予文件访问权限时应采用最低特权原则（即，信息的访问权应仅授予需要知道这些信息的人员，授予的权限不超过所需的权限，并且有效期仅限定在所需的时间范围内）。应根据信息敏感度来审查访问权限。这包括您管理的存储位置以及分包商管理的存储位置。
    - 当相关人员离开公司或不再负责需要访问信息的业务时，应及时取消其访问权限。
- 未经 Lilly 公司批准，不得将信息存储在以下位置：
    - 员工的个人设备，例如笔记本电脑、iPad 等
    - 外部存储服务或网站。

**电子数据传输：**

- 包含信息的电子文件必须安全传输。请咨询 Lilly 公司联系人，以建立信息传输的首选方法。未经 Lilly 公司批准，不得使用可移动存储设备，例如外部硬盘驱动器、CD/DVD 和 USB。
- 信息不得通过以下方式传输：
    - 不安全的电子邮件（除非敏感度级别不要求）。
    - 外部存储设备，例如外部硬盘驱动器或 USB（未经 Lilly 批准）。
    - 个人电子邮件。

**电话会议/在线会议：**

- 使用 Lilly 批准的会议服务安排和举行有关公司业务的会议。如果您对电话会议/在线会议有疑问，请咨询 Lilly 公司联系人。
- 讨论信息时，请注意周围的环境并保持谨慎。

**物理安全性：**

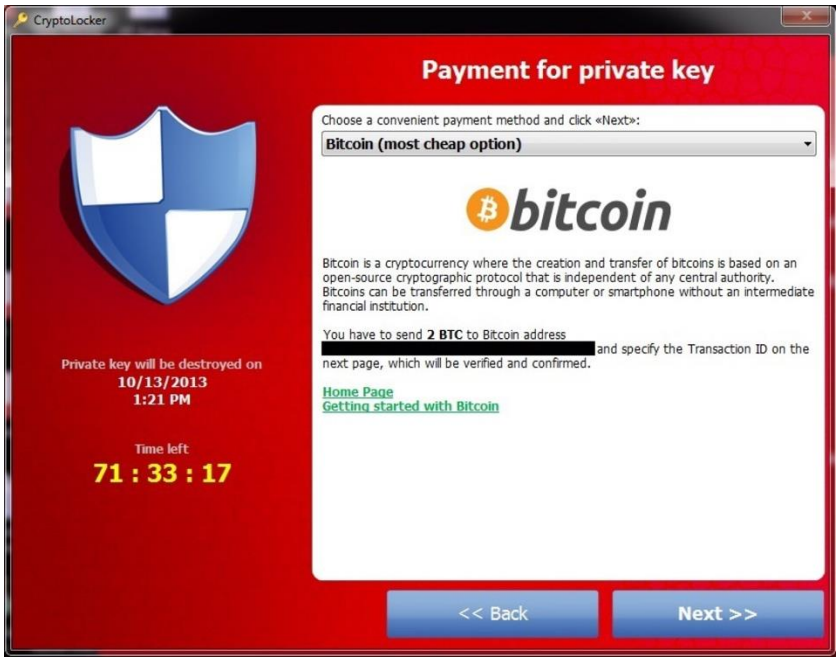
- 维护安全的工作空间：
    - 每当您离开设备时，都应锁定对设备的访问。
    - 当您在外出、出差或度假时，应将设备放在可上锁的柜子中或用缆线锁好，或者随身携带设备。
    - 当您在外出、出差或度假时，请锁好办公桌、柜子和办公室。
    - 不要将打印材料留在打印机上。
    - 通过保密方式丢弃信息（例如，粉碎）。

**即时消息和文本：**

- 利用 Lilly 批准的工具来发送有关公司业务的即时消息和文本消息。如果您对即时消息或文本消息有疑问，请咨询 Lilly 公司联系人。

**信息安全事件报告：**

- 及时向 Lilly 联系人报告事件。事件包括但不限于：
  - 包含信息的电子邮件意外发送给了非预期的收件人。
  - 包含信息的笔记本电脑、硬盘驱动器或可移动存储设备丢失或被盗。
  - 具有信息访问权限的分包商向您的公司发出事件警报。
  - 收到勒索软件（一种恶意软件，旨在阻止对设备的访问，直到付款为止）。请参见下面的示例。立即执行以下步骤可能有助于降低风险：
    - 拔下网络电缆或禁用无线适配器。
    - 让电脑休眠。




**警惕社交工程陷阱***（例如，网络钓鱼、电话钓鱼、短信钓鱼）*！

- 社交工程陷阱是利用欺骗手段操纵个人泄露可能用于欺诈目的的机密或个人信息。诈骗者伪装成信誉良好的来源，意图窃取身份或获取信息，例如密码、银行详细信息和信用卡号等。
  - **网络钓鱼**（电子邮件）
    - 网络钓鱼尝试是一种非预期的消息，其特征包括：
      - 使人惊慌的行动呼吁（例如，您的信用卡付款逾期）。
      - 时间元素（例如，两天内到期）。
      - 结果（例如，解决此问题，否则可能会导致不良后果）。
      - 语法不正确或单词拼写错误。
      - 并且总是有一些要“单击”的内容，例如链接或附件。
    - 如果您单击电子邮件中的未知附件或链接，则您的计算机和整个网络可能会受到威胁。
  - **电话钓鱼**（电话或语音留言）
    - 电话钓鱼尝试是一种非预期的电话，具有以下特征：
      - 寻求信息确认或请求信息。
      - 可能会与网络钓鱼攻击结合使用。

- **短信钓鱼**（短信）
  - 短信钓鱼尝试是一种非预期的短信，具有以下特征：
    - 寻求信息确认或请求信息。
    - 可能会与网络钓鱼攻击结合使用。
    - 通常有一些要“单击”的内容，例如链接或附件。

- **如果您有 Lilly 公司的电子邮件地址**，您将参加 Lilly 正式的网络钓鱼教育计划。
  - 屡次单击钓鱼链接或附件的员工将会被报告给第三方并获得后续指导。如果您对 Lilly 正式的网络钓鱼教育计划有疑问，请咨询 Lilly 联系人。
  - 如果您使用 Lilly o365 电子邮件帐户，请通过 Outlook“Home”（主页）功能区中的“Report Phishing”（报告网络钓鱼）按钮报告可疑电子邮件。


  - 如果您通过 VPN 或 virtual.lilly.com 连接到了 Lilly 内部网络，请通过 cyber@lilly.com

- **暂停和检查。使用直觉：**
  - 如果电子邮件看起来可疑，请花点时间仔细查看邮件。
  - 如果您不想接收它们，则不要点击链接或打开附件。
  - 如果您没有 Lilly 公司的电子邮件地址，并且您单击了您认为可疑的邮件中的链接或打开了附件，请通过您雇主的程序进行举报。

**如果您有任何疑问或疑虑：**

- 有关上述任何项目的问题或疑虑，请咨询 Lilly 公司联系人。
- 此信息也可以在 Supplier Portal（供应商门户网站）的“Supplier Resources”（供应商资源）中的“Operating Responsibility”（运营责任）下找到。