BUSINESS RULES FOR SECURE HANDLING OF INFORMATION

Purpose: Key messages for handling information from or provided on behalf of Lilly, hereafter referred to as Information.

Why is this important?

- Your organization and its workforce are valued contributors to Lilly, and actions you and your workforce take are part of the first and best line of defense against the compromise of Information.
- Protecting Information is essential to Lilly and the patients we serve.

The following key messages, which are informed by industry best practices, including the NIST Cybersecurity Framework, should be incorporated into current practices to continue to reduce risk when handling Information.

In General:

- Avoid making duplicative electronic or hard copies of documents containing Information unless absolutely necessary.

Electronic Data Storage:

- Electronic files that include Information must be stored securely. Removable storage devices such as external hard drives and USBs cannot be used without Lilly approval.
    - Principle of Least Privilege should be applied to grant access to files (i.e., access to Information should only be granted to those with a need to know, not more than is needed, and only for the time required). Access should be reviewed commensurate with the level of sensitivity. This includes storage locations you manage as well as those managed by your sub-contractors.
    - Timely access deactivation should occur after an exit from the company or when individuals no longer have a business need to access Information.
- Information must NOT be stored in the following locations without approval from Lilly:
    - Employees' personal devices such as laptops, iPad etc.
    - External storage services or sites.

Electronic Data Transfer:

- Electronic files that include Information must be transferred securely. Consult your Lilly contact to establish the preferred method for Information transfer. Removable storage devices such as external hard drives, CDs/DVDs, and USBs cannot be used without Lilly approval.
- Information must NOT be transferred via:
    - Unsecured e-mail (unless sensitivity level does not warrant).
    - External storage devices such as external hard drive or USB (without approval from Lilly).
    - Personal e-mail.

Teleconferences/Online Meetings:

- Use Lilly approved meeting services for scheduling and conducting meetings about company business. Consult your Lilly contact if you have questions relating to teleconferences/online meetings.
- Be aware of your surroundings and be cautious when discussing Information.

Physical Security:

- Maintain a secure workspace:
    - Lock access to your devices ANY time you step away from them.
    - Devices should be placed in a lockable cabinet, cable locked or taken with you when you leave for the day, are away for business travel, or on vacation.

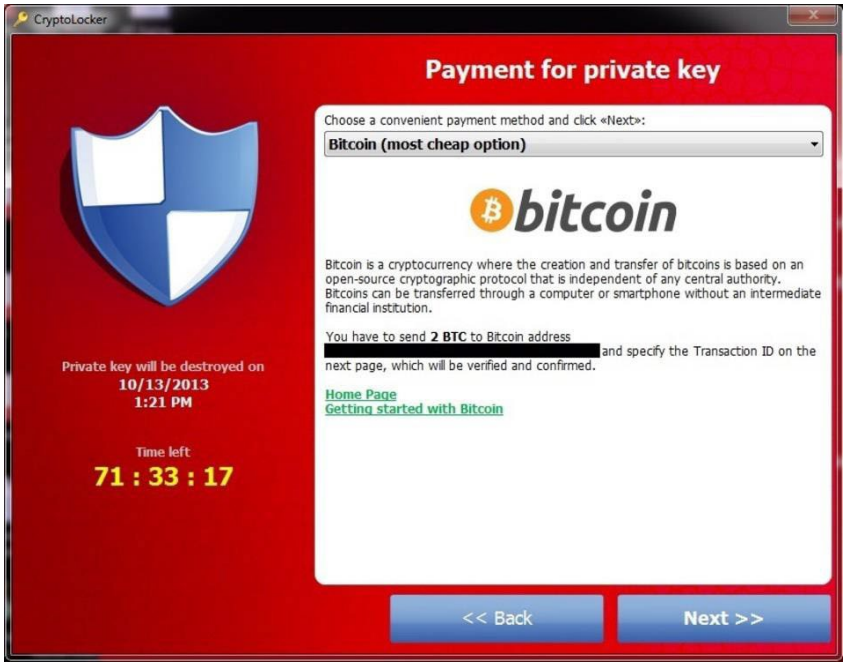
- Lock your desk, cabinets and locker/office when you leave for the day, are away for business travel, or on vacation.
- Do not leave hard copies on printers.
- Confidentially discard Information (e.g., shred).

Instant Message and Text:

- Utilize a Lilly-approved tool for instant messages and text messages for company business. Consult your Lilly contact if you have questions related to instant messaging or text messaging.

Information Security Incident Reporting:

- Report incidents to your Lilly contact in a timely manner. Incidents include but are not limited to:
  - Email containing Information was accidentally sent to an unintended recipient.
  - Lost or stolen laptop, hard drive or removable storage device that contains Information.
  - A sub-contractor with access to Information alerts your company to an incident.
  - Receive Ransomware, a type of malicious software designed to block access to device until a sum is paid. See example below. Immediately performing the following steps may help to reduce risk:
    - Unplug the network cable or disable the wireless adapter.
    - Hibernate.



Beware of Social Engineering *(e.g., Phishing, Vishing, SMiShing)***!:**

- Social engineering is the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes. Scammers masquerade as a reputable source in an effort to steal identities or retrieve Information, such as passwords, bank details, and credit card numbers, etc.
  - **Phishing** (email)
    - A phishing attempt is an unexpected message and characteristics include:
      - An alarming call to action (for example, your credit card payment is late).
      - A time element (for example, something is due within two days).
      - A consequence (for example, solve this problem, or something bad will happen to you).
      - Poor grammar or misspelled words.
      - AND always has something to “click” on, such as a link or attachment

        - If you click on an unknown attachment or link in an email, your computer and entire network could be compromised.

    - **Vishing** (phone calls or voice messages)
        - A vishing (voice phishing) attempt is an unexpected phone call that:
            - Seeks confirmation of Information or requests Information.
            - May be used in combination with a phishing attack.
    - **SMiShing** (SMS text messages)
        - A SMiShing attempt is an unexpected text that:
            - Seeks confirmation of Information or requests Information.
            - May be used in combination with a phishing attack.
            - Typically has something to "click" on, such as a link or attachment.

- **If you have a Lilly email address**, you will participate in Lilly's formal educational-phishing program.
    - Individuals who are repeat clickers will be reported to the third party with an expectation of follow-up coaching. Consult your Lilly contact if you have questions about Lilly's formal educational phishing program.
    - If you are utilizing a Lilly o365 email account report suspicious emails via the "Report Phishing" button in the Outlook "Home" ribbon.

    - If you are connected to the Internal Lilly network via VPN or virtual.lilly.com, report suspicious message via cyber@lilly.com.

- **Pause and Inspect. Use your intuition:**
    - If an email seems suspicious, take a moment to look closely at the message.
    - Do not click links or open attachments if you were not expecting them.
    - If you do not have a Lilly email address and you click a link or open an attachment in a message you believe to be suspicious, please report it via your employer's process.

If you have questions or concerns:

- Consult your Lilly contact with questions or concerns related to any of the items discussed above.
- This information is also available on the Supplier Portal under Operating Responsibility in the Supplier Resources.