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. Work with your Lilly Contact if you have questions relating to the storage of Information.
    - Access to electronic files that include Information should only be granted to those with a need to know, not more than is needed and only for the time required (least privilege). 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.
    - Deactivation should occur timely 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:
    - Any removable storage device such as external hard drive, USB, etc.
    - Employees' personal devices such as laptops, iPad etc.
    - External storage services or sites such as Google Docs, DropBox, SkyDrive, etc.

Electronic Data Transfer:

- Electronic files that include Information must be transferred securely. Work with your Lilly Contact to establish the preferred method to transfer Information.
- 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.
    - GigaFile, WeTransfer, SlideShare.

Teleconferences:

- Should be conducted using Skype for Business. Work with your Lilly Contract if Skype for Business is not an option.
- Should NOT be conducted using any Google services.
- Be aware of your surroundings and be cautious when discussing information.

Physical Security:

- Maintain a secure workspace:
    - Lock out access to your computer ANY time you step away from it.
    - Laptops and iPads are either 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 Skype for Business.
- Texting or instant messaging used for communicating logistics only, not sharing Information.
- The following should NOT be used: Google IM, ChatHour, AOL IM, Yahoo/MSN Messenger.

Information Security Incident Reporting:

- If there is an Information security incident, please contact your Lilly relationship manager or sponsor AND Report a Concern via the Ethics and Compliance hotline if internal Lilly access or EthicsPoint if external. Incidents can 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.
  - Ransomware
    If you see a screen similar to the one shown below, performing the following steps may help to reduce risk:
    - Unplug the network cable or disable the wireless adapter.
    - Hibernate.

Beware of Phishing!

- Phishing is an approach used by malicious outsiders to acquire Information by masquerading as a trustworthy entity. Once you click on an unknown attachment or link in an email, your computer and entire network could be compromised.

- A phishing attempt is an unexpected message and almost always has:

  - 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.

- **P**ause and **I**nspect. 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 click a link or open an attachment in a message you believe to be suspicious, please report following your employer's process.

- Those individuals who have a Lilly email address will be part of Lilly's formal educational phishing program. The names of repeat clickers will be communicated to the third party with an expectation of follow-up coaching. Work with your Lilly Contact if you have questions relating to Lilly's formal phishing education program. If you click a link or open an attachment in a message you believe to be suspicious from your Lilly email, please report via Operation Screen Door.

If you have questions or concerns:

- Contact your Lilly sponsor or Relationship manager with questions or concerns related to any of the items discussed above.
- This information can also be found on the Supplier Portal under Protect Lilly.