What Do I Need to Encrypt?

As NIH staff, we have access to various types of information, including Personally Identifiable Information, Protected Health Information, and other types of Sensitive Information. It's our responsibility to know how to protect this information by understanding when and how to encrypt.

The NIH requires staff to encrypt all Sensitive Information sent via email.

Sensitive Information (SI) is defined as any information for which the loss of confidentiality, integrity, or availability could be expected to have a serious, severe, or catastrophically adverse effect on individuals, organizational operations, or assets. This includes the following types of SI:

1. **Sensitive Personally Identifiable Information (PII) –** PII in any form which if lost, compromised, or inappropriately disclosed could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual – including elements that are sensitive alone as well as elements that become sensitive when combined with other information or because of the context in which they appear

   Examples | *Always Sensitive*: Social Security number, driver's license, biometric identifiers

   Examples | *Sensitive in Context or Combined with Other Identifiers*: Date of birth, criminal history, account numbers, citizenship status

2. **Protected Health Information (PHI) –** Information related to an individual's past, present, or future physical or mental health, the provision of healthcare to an individual, payment for the provision of healthcare, and other information that could reasonably be used to identify an individual in a healthcare setting

   Examples: Diagnoses, medical bills, laboratory results, medical records

3. **Other Sensitive Information –** All other information for which the loss of confidentiality, integrity, or availability could be expected to have a serious, severe, or catastrophically adverse effect on individuals, organizational operations, or assets

   Examples: Grant applications, trade secrets, unpublished manuscripts, NIH purchase card information, financial documents

Best Practices for Handling Sensitive Information

Encryption is one of many ways we can protect SI. Below are other ways we can protect it in a variety of different circumstances.

RECORDING *Digitally or on paper*

If recording Sensitive PII or PHI, ensure your Privacy Coordinator has provided approval

DISCUSSING *By phone or in person*

Do not discuss SI out loud in public

VIEWING

Use a screen protector when viewing SI in public

SENDING *By email, fax, or scan*

Only share SI with those who need to know, and always encrypt when sending via email

PRINTING

Print only the SI you need and do not leave hard copies unattended

STORING

Never send SI to personal email accounts, and save only to NIH-authorized online storage

DISCARDING

Discard hard copies of SI only in secure shred bins at NIH facilities

NIH Approved Encryption Methods at the NIH

Messages that include Sensitive Information in the body or in attachments must be encrypted using one of the approved methods below. For information on how to encrypt a message with each method, see the next page.

Method and Recommended Use	Permitted Data	Recipient Types	PIV Card Required	Maximum Size	Permissions Required	Shared Mailboxes*	Message Retention	More Information
Office 365 Message Encryption (OME) *Preferred encryption method for all non-medical messages under 150 MB, regardless of recipient*	PHI, PII, SI	Internal or external *Approved for clinician to clinician messages, not clinician to patient*	No	150 MB	No permissions required for Office 365 users	Can send and receive	Permanent	OME FAQs
Secure Email/File Transfer (SEFT) *Preferred encryption method for all non-medical messages over 150 MB, regardless of recipient*	PHI, PII, SI	Internal or external *Approved for clinician to clinician messages, not clinician to patient*	No	200 GB account storage limit	Sender and receiver must register and log in to SEFT	Can't send or receive	30 days	General Information on SEFT
Secure/Multipurpose Internet Mail Extensions (S/MIME) and PIV-D *Legacy encryption methods that use a PIV card to encrypt via laptop and phone respectively - OME is preferred*	PHI, PII, SI	Internal only *Approved for clinician to clinician messages, not clinician to patient*	Yes	100-120 MB	Sender and receiver both need valid PKI certificates	Can't send or receive	Permanent	S/MIME Encryption MobileIron: Derived PIV (PIV-D) FAQs
Secure Health Messaging (SHM) *Preferred method for messages between NIH care providers and from care providers to patients (messages attach to CRIS medical records by default)*	PHI, PII, SI	Internal or external *Approved for clinician to patient messages*	No	No file transfer permitted – messaging only	For intramural use only – sender and receiver must log in to the EHR/patient portal	Can't send or receive	Permanent	Clinical Center SHM Training
Medical Secure Email (MSE) *Preferred method for messages from NIH care providers to patients (allows attachment of files, messages are not automatically attached to medical records in CRIS)*	PHI, PII, SI	Internal or external *Approved for clinician to patient messages*	No	200 GB account storage limit	For intramural use only - sender and receiver must log in to MSE	Can't send or receive	3 years	Secure Mail User Guide

**** Note: NIH users can't send encrypted messages to listservs using any encryption method.***

How to Send Encrypted Messages

Click each method's name for more information, including guidance for external parties on how to view encrypted messages.

Office 365 Message Encryption (OME)

PC – Outlook 2016

1. Open a new email
2. Select the **Options** tab
3. Click **Permission**
4. Select the correct permission level

PC – Outlook 2019

1. Open a new email
2. Select the **Options** tab
3. Open the dropdown under the lock and select the correct permission level

Mac – Outlook

1. Open a new email
2. Select the **Options** tab
3. Click **Encrypt**
4. Open the dropdown by the lock and select the correct permission level

Outlook Web

1. Open a new email
2. Click **Encrypt**
3. Click **Change Permissions**
4. Select the correct permission level

Mobile Device

1. Open a new email
2. Type "**[secure]**" or "**[encrypt]**" in square brackets at the beginning of the subject line (not case sensitive)

Secure Email/File Transfer (SEFT)

All NIH Users

Before using for the first time, you must enable by contacting the NIH IT Service Desk.

1. Navigate to **SEFT Webmail** using a web browser
2. Sign in with your NIH credentials (type "NIH\" before your username)
3. Click **Secure Message**
4. Compose your message
5. Click **Choose Files** to add any attachments
6. Click **Send**

PIV Encryption for Mobile Devices (PIV-D)

All NIH Users

Before using for the first time, you must enable on your device by following these instructions for iOS or these instructions for Android.

1. Open a new email
2. Click the lock icon to the right of the email subject line
3. Select **Encrypt**

Secure/Multipurpose Internet Mail Extensions (S/MIME)

PC – Outlook 2007

1. Open a new email
2. Select the **Options** ribbon
3. Click **Encrypt Message Contents and Attachments**
   If you don't see that button:
   a. *Click More Options*
   b. *Click Security Settings*
   c. *Click Encrypt Message Contents and Attachments*
   d. *Close the Options box*
4. Click **Send** and enter PIN

PC – Outlook 2010 – 2016

1. Open a new email
2. Select the **Options** ribbon
3. Select **Encrypt** in Permissions
4. Click **Send** and enter PIN

Mac

1. Open a new email
2. Add the recipient's NIH email address to the To section
3. Click the **Security** icon
4. Click **Encrypt Message**
5. Click **Send** and enter PIN

Secure Health Messaging (SHM)

All NIH Care Providers

Access the Secure Health Messaging training materials for an overview of messaging in CRIS and detailed instructions on how to send provider to provider or provider to patient messages.

Medical Secure Email (MSE)

All NIH Care Providers

1. Click **Manage Packages** and click the email icon to the right of the desired package name
2. Enter recipients, a subject, a secure message, and a notification message
3. Click **Add Files** to select files to upload and update other optional preferences as needed
4. Click **Send** to deliver the package