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   **Examples**: Grant applications, trade secrets, unpublished manuscripts, NIH purchase card information, financial documents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

**SENDING** By email, fax, or scan
Only share SI with those who need to know, and always encrypt when sending via email

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

**DISCUSSING** By phone or in person
Do not discuss SI out loud in public

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

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

**VIEWING**
Use a screen protector when viewing SI in public
# 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.

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

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

Need help? Contact the [IT Service Desk](#) for OME, SEFT, or S/MIME and the [Health Information Management Department](#) at 301-496-3331 for SHM or MSE.
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)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Open a new email</td>
<td>1. Open a new email</td>
<td>1. Open a new email</td>
<td>1. Open a new email</td>
<td>1. Open a new email</td>
</tr>
<tr>
<td>2. Select the <strong>Options</strong> tab</td>
<td>2. Select the <strong>Options</strong> tab</td>
<td>2. Select the <strong>Options</strong> tab</td>
<td>2. Click <strong>Encrypt</strong></td>
<td>2. Type “[secure]” or “[encrypt]” in square brackets at the beginning of the subject line (not case sensitive)</td>
</tr>
<tr>
<td>3. Click <strong>Permission</strong></td>
<td>3. Click <strong>Encrypt</strong></td>
<td>3. Click <strong>Permission</strong></td>
<td>3. Click <strong>Change Permissions</strong></td>
<td>3. Select the <strong>correct</strong> permission level</td>
</tr>
<tr>
<td>4. Select the <strong>correct</strong> permission level</td>
<td>4. Open the dropdown by the lock and select the <strong>correct</strong> permission level</td>
<td>4. Open the dropdown under the lock and select the <strong>correct</strong> permission level</td>
<td>4. Select the <strong>correct</strong> permission level</td>
<td></td>
</tr>
</tbody>
</table>

### 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**

### 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