

## Frequently Asked Questions (FAQ)

---

**Q1: What is the purpose of CIO Directive 16-01? ..... 1**

**Q2: What is the definition of CMS sensitive information? ..... 2**

**Q3: What are the CMS-approved solutions for encrypting attachments? ..... 4**

**Q4: What are the CMS-approved methods of sharing passwords? ..... 7**

**Q5: How do I report a potential incident?..... 8**

<b>DO...</b>	<b>DON'T...</b>
1. Consider all personally identifiable information (PII) including protected health information (PHI) and federal tax information (FTI) as sensitive information that must be protected.	1. Use email as a substitute for establishing an approved business process for sharing sensitive information.
2. Encrypt sensitive information when any email address is outside of the CMS controlled environment	2. Send any sensitive information without confirming that it is both encrypted and addressed to the appropriate parties.
3. Send the password using an out of band method (e.g., phone, text, SharePoint).	3. Send the password using an email, in a Lync/Skype message, or in a voicemail.
4. Use a CMS approved, FIPS 140-2 encryption method such as SecureZip.	4. Use WinZip without configuring it for FIPS 140-2 compliant encryption.
5. Report any incident or potential incident to the IT Service Desk (1-800-562-1963).	5. Try to resolve a security or privacy incident without reporting it to the IT Service Desk.

**Q1: What is the purpose of CIO Directive 16-01?**

This directive provides guidance for protecting sensitive information in email. Specifically, the directive:

- Requires sensitive information to be protected using a CMS-approved solution whenever any recipients of the email are outside the CMS trusted domain (Approved TLS Connection)
  - The sensitive information must be encrypted in an email attachment with a CMS-compliant password. Current CMS policy requires passwords to be a minimum of eight characters in length and contain at least one character from each of the four character categories (A-Z, a-z, 0-9, and special characters), or
  - The entire email may be encrypted using Outlook encryption, when appropriately configured as described below.
- Defines the HHS email shared service environment as the HHS Exchange Domain which includes Operating Division (OpDivs) and Staff Divisions (StaffDivs) that utilize (OPDiv.HHS.gov) within their email accounts. CMS also has a number of approved trusted domains with which enforced Transport Layer Security (TLS) is implemented and information is protected as it is transmitted via email. See the list below:
  - **HHS OpDivs/StaffDivs** - HHS email shared service system: OS, CMS, ACF, ACL,

## CIO Directive 16-01

### CMS Encryption of Sensitive Information in Email - FAQ

AHRQ, and SAMHSA

- **Federal agencies:** .whitehouse.gov, .senate.gov, .ssa.gov
- **Other CMS trusted domains:** cotiviti.com and qssinc.com, lilly.com, elanco.com, agspan.com, network.lilly.com, network.elanco.com, networks.agspan.com, lists.lilly.com

*The authoritative list of domains included in the CMS controlled environment is maintained by the Office of Technology Solutions (OTS) Enterprise Infrastructure Operations Group (EIOG). Please contact Ricco Jenkins of the Division of Customer Liaison and Support Services (DCLSS) for an authoritative list of domains.*

- Requires users to send passwords using a separate mechanism. This prohibits users from sending a password via a separate email or using Microsoft Lync (which converts conversations into emails). Authorized methods of password transmittal are text message, phone conversations, predetermined shared secrets, or a shared file system (e.g. SharePoint). A predetermined shared secret is the most practical for sharing information with large groups. An example of a predetermined shared secret would be a password established in a group meeting.
- Reinforces the requirement to use encryption that is approved by CMS.
- Supersedes previous guidance, including CIO Directive 14-04, *CMS Encryption of Sensitive Information in Email*, dated November 13, 2014; Section 4.E.7 of the *CMS Policy for Privacy Act Implementation & Breach Notification*; and This Directive also supersedes the July 17, 2015 Best Practices document entitled, “5 things you can do to protect CMS information” in which use of the Lync application must be removed as a viable option for transmitting passwords.

#### ***Does this Directive apply to email accessed from a non-Government Furnished Device?***

Yes. Ownership of the device that is accessing email is not relevant. The CMS data must be encrypted with a CMS-compliant password using SecureZip when information is being sent via any email domain.

#### **Q2: What is the definition of CMS sensitive information?**

The Privacy Act, Health Information Portability and Accountability Act (HIPAA), and Federal Information Security Modernization Act (FISMA) of 2014 identify specific types of information that CMS must protect including PII and protected health information. Internal Revenue Service (IRS) Publication 1075 mandates the protection of Federal Tax Information (FTI). CMS Sensitive Information may also include pre-award contract information and information system component information (e.g. IP Address, MAC Address etc...). CMS includes a complete definition of CMS Sensitive information in the Risk Management Handbook <sup>1</sup>

#### ***Are PII and PHI considered sensitive information?***

Yes. NIST defines PII<sup>2</sup> as “any information about an individual maintained by an agency,

---

<sup>1</sup> *Risk Management Handbook* Vol 1. Ch 10. CMS Risk Management Terms, Definitions, and Acronyms, dated July 2012, found here: <http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html>.

<sup>2</sup> NIST Special Publication (SP) 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, <http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf>

## CIO Directive 16-01

### CMS Encryption of Sensitive Information in Email - FAQ

including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information." Examples of PII include:

- Name, Date of birth, Place of birth
- Contact information (phone numbers, mailing address, email address)
- Mother's Maiden Name
- Social Security Number (or other number originated by a government that specifically identifies an individual)
- Certificate/license numbers (e.g., Driver's License Number)
- Vehicle Identifiers (e.g., license plates, Vehicle Identification Number)
- Passport number, Alien (A-) number
- Financial account numbers

PHI is any information in a medical record that can be used to identify an individual, and that was created, used, or disclosed in the course of providing a health care service, such as a diagnosis or treatment. Examples of PHI include:

- Medical record numbers, Account numbers, Health plan beneficiary number
- Biometric Identifiers (e.g., fingerprint and voiceprint)
- Name of relative
- Biometric identifiers, including fingers and voice prints
- Photographic Identifiers (e.g., photograph image, x-rays, and video)
- Blood test results, billing information, emails with prescription information

#### ***Does Federal Tax Information constitute sensitive information? Are there special guidelines for handling and emailing FTI?***

Yes. The Internal Revenue Code and IRS regulations define specific requirements for transmitting FTI through email.<sup>3</sup> IRS guidance identifies many forms of FTI, including:

- Any information, besides the return itself, that IRS obtained from any source or developed through any means that relates to the potential liability of any person under the Code for any tax, penalty, interest, fine, forfeiture, or other imposition or offense.
- Information extracted from a return, including names of dependents, or the location of business.
- The taxpayer's name, address and identification number.

---

<sup>3</sup> Internal Revenue Services (IRS) Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies, dated October 2014, found here: <http://www.irs.gov/pub/irs-pdf/p1075.pdf>.

- Information collected by the IRS about any person's tax affairs, even if identifiers like name, address and identification number are deleted.
- Whether a return was filed, is or will be examined or subject to other investigation or processing, including collection activities.
- Information contained on transcripts of accounts.

**Q3: What are the CMS-approved solutions for encrypting attachments?**

CMS recommends the SecureZip software for encrypting attachments. Outlook encryption using certificates contained on federally issued PIV cards is also an acceptable mechanism. For additional instructions for encrypting an email attachment and other approved CMS encryption software, please contact the CMS IT Service Desk by calling 410-786-2580 or 1-800-562-1963, or via email to [CMS\\_IT\\_Service\\_Desk@cms.hhs.gov](mailto:CMS_IT_Service_Desk@cms.hhs.gov).<sup>4</sup>

***Does encrypting the email attachment provide additional security? How?***

Yes. Encrypted attachments can only be read by someone with the password. Encryption protects the confidentiality of the email by scrambling the message, thus requiring a password to decrypt the message. Encrypting email attachments also protects them from being compromised on unencrypted servers.

***Does it matter what type of encryption I use?***

Yes. While all encryption solutions provide some level of protection, federal standards dictate which solutions are robust enough to protect the sensitive information.<sup>5</sup>

***Should I use SecureZip to encrypt attachments?***

Yes. SecureZip is a CMS-approved encryption software that allows the user to compress and encrypt an attachment. Employees and contractors should use this software if it is available on their desktops.

All CMS government furnished equipment includes SecureZip as part of the base image software package. Information technology (IT) procurement preconfigures SecureZip to enable Federal Information Processing Standard (FIPS) 140-2 compliant encryption on CMS computers. If any CMS machine does not include SecureZip, please contact the CMS IT Service Desk (410-786-2580, 800-562-1963, or at [CMS\\_IT\\_Service\\_Desk@cms.hhs.gov](mailto:CMS_IT_Service_Desk@cms.hhs.gov)).

If this software is not available, the employee or contractor must encrypt the CMS sensitive information in an attachment using an alternate CMS-approved, FIPS 140-2 compliant solution.

Figures 1 and 2 illustrate how to encrypt an attachment using SecureZip:

1. Compose new Email message
2. Click **SecureZIP** Tab and then select **SecureZIP Encrypt**

---

<sup>4</sup> Intranet users may visit [http://intranet.hhs.gov/it/cybersecurity/enterprise\\_security/Encryption/](http://intranet.hhs.gov/it/cybersecurity/enterprise_security/Encryption/) for encryption solutions and SecureZIP guides.

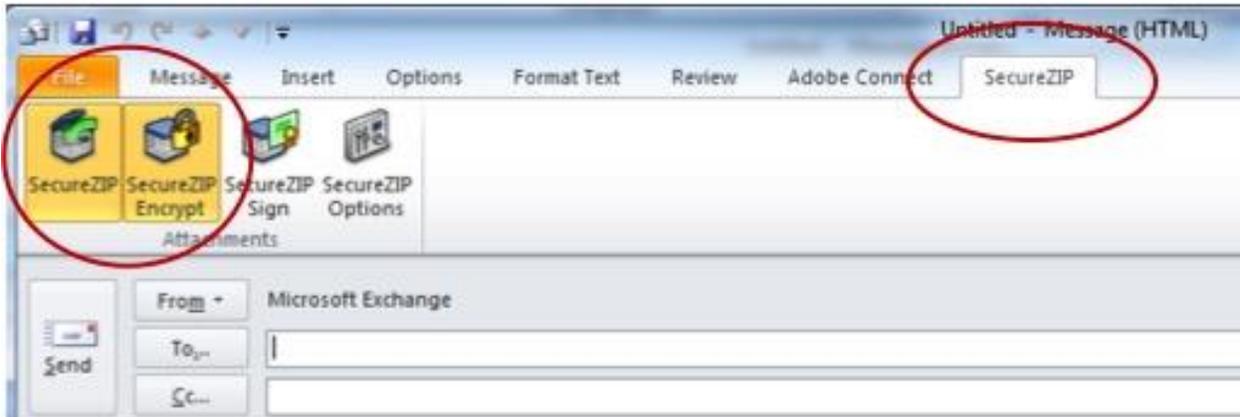
<sup>5</sup> As directed in *Acceptable Risk Safeguards* (ARS) control SC-13, the encryption used must be a CMS-approved solution that complies with the Federal Information Processing Standard (FIPS) 140-2 standard.

## CIO Directive 16-01

### CMS Encryption of Sensitive Information in Email - FAQ

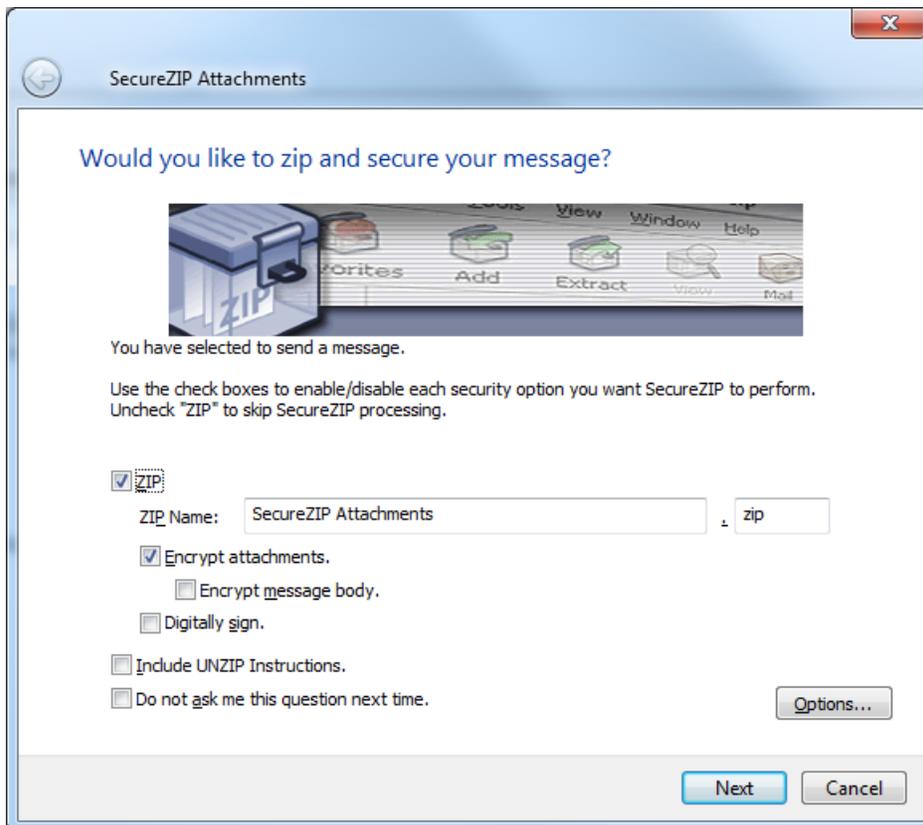
3. Fill out appropriate fields
4. Insert Sensitive Attachment
5. Click **Send**

**Figure 1.** Using SecureZip to Encrypt an Attachment



6. Ensure “**Encrypt attachments**” is selected
7. Click **Next**

**Figure 2.** SecureZip Attachment Settings



## CIO Directive 16-01

### CMS Encryption of Sensitive Information in Email - FAQ

8. Enter Passphrase (At least 8 Characters)
9. Click **OK**
10. Contact recipients and provide the passphrase

#### ***Can I use WinZip to encrypt attachments?***

Yes, if WinZip is version 18.5 or later and is configured to use FIPS 140-2 compliant AES encryption. For details, see the WinZip website: <http://kb.winzip.com/kb/entry/65/>.

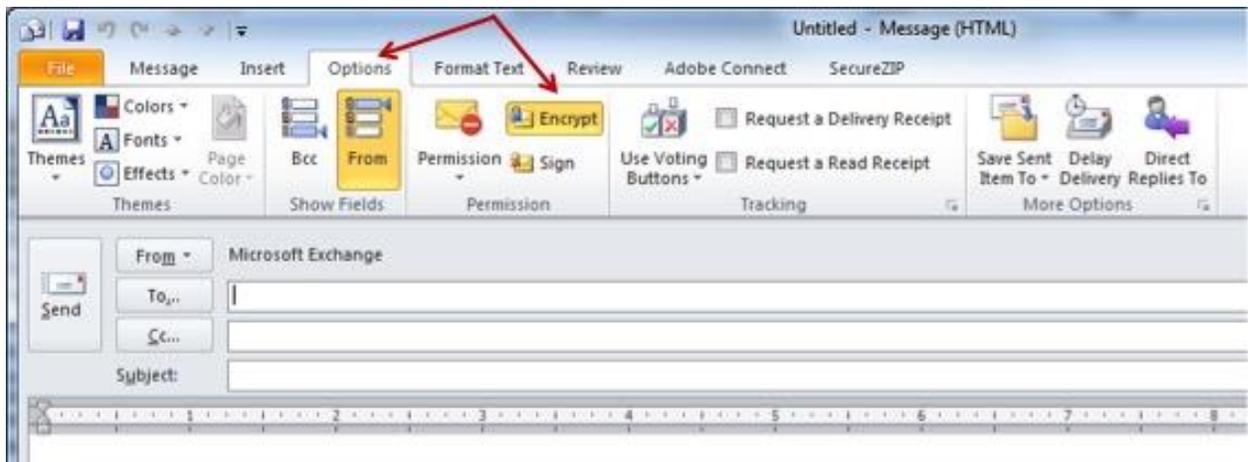
#### ***Can I use Outlook encryption to encrypt the entire email?***

Yes. Outlook encryption provides end-to-end encryption that encrypts both the email body and the attachment. Within the CMS controlled environment, Outlook may store the appropriate encryption certificates and be activated by the following steps:

1. Compose new email message
2. Click the **Options** tab
3. Click the **Encrypt** button
4. Fill out appropriate fields and insert sensitive attachment
5. Click **Send**
6. Enter your PIV card **PIN**

Figure 3 illustrates the use of Outlook encryption.

**Figure 3.** Enabling Outlook Encryption



**IMPORTANT NOTE:** Outlook encryption only works if both users have access to both encryption certificates. If you receive an “Encryption Problems” dialogue box, do NOT send the email. For more information on sharing PIV encryption certificates, contact the IT Service Desk, or visit the HHS site:

[http://intranet.hhs.gov/it/cybersecurity/enterprise\\_security/Encryption/email-encryption-pivcard.pdf](http://intranet.hhs.gov/it/cybersecurity/enterprise_security/Encryption/email-encryption-pivcard.pdf)

- Click the **Cancel** button to close the warning. Do NOT send the email.

***The CMS email exchange server uses enforced Transport Layer Security (TLS); is that secure?***

Yes. As long as the email is sent from an HHS/CMS account and is addressed to parties within the CMS controlled environment, no further encryption is required. If one or more parties receiving the email are outside of the HHS email shared service environment (*OpDiv.HHS.gov*) domain or the trusted domains, an encrypted attachment must be used.

***Is FIPS 140-2 compliant encryption required? What is the baseline FIPS 140-2 encryption algorithm for encrypting sensitive information?***

Yes. The federal standard for cryptographic algorithms under FIPS 140-2 contains a complete list of approved algorithms and is located at:

<http://csrc.nist.gov/groups/STM/cavp/validation.html>

A cryptographic module validated to FIPS 140-2 shall implement at least one approved security function used in an approved mode of operation. However, implementing an approved security function is only the start. The product must also be approved for use by CMS.

***Can I use my digital signature to encrypt email?***

No. Digitally signing a message creates a fingerprint for the message to make sure that the content has not been altered or changed during transmission. It does not encrypt the message. Encryption renders the entire message unreadable without the appropriate password to decrypt the data. Encrypting the message protects the confidentiality, while digitally signing the message protects the integrity of the message.

**Q4: What are the CMS-approved methods of sharing passwords?**

Passwords for encrypted attachments must be sent using an alternative means (“out-of-band”) from the CMS email system. This includes pre-sharing the password in a separate location on the network, using a text message, or through a phone call. Passwords must not be sent via email message and should not be sent via voicemail.

***May I establish a temporary group password to be used by my colleagues for encrypting files?***

Yes. Passwords are not considered accounts and may be shared for a group’s internal use. These passwords should not be sent to the group via email. They may be stored in a secure area that is accessible to the team (i.e., shared drive or SharePoint with appropriate access controls).

***Can I send my password to decrypt the attachment with sensitive information via a separate email?***

No. All passwords for encrypted files must be submitted out-of-band. Please send your password (via text, phone call, shared secret, shared file etc..) but not via email.

***Can I send my password via Lync?***

No. Microsoft Lync software messages are considered in-band. Messages sent via Lync convert to emails in Outlook Messaging once the conversation ends.

***Can I use another instant messaging service to share the password?***

## CIO Directive 16-01

### CMS Encryption of Sensitive Information in Email - FAQ

Yes. Although Lync/Skype is connected to the CMS email system, you may use another instant messaging service (e.g., Blackberry messaging) to share passwords. However, it is best not to link this password to the document by referencing the title of the document, etc.

#### **Q5: How do I report a potential incident?**

All suspected or verified incidents must be reported immediately to the CMS IT Service Desk (410-786-2580 or 800-562-1963, or email [CMS IT Service Desk@cms.hhs.gov](mailto:CMS_IT_Service_Desk@cms.hhs.gov)). Additionally, please contact the Information System Security Officer (ISSO) of the affected system ASAP.

#### ***Which of the following is considered a potential incident?***

- I emailed sensitive information without encrypting it to someone in the CMS controlled environment ***who was not the intended recipient.***
- I emailed unencrypted sensitive information to one or more recipients with email addresses ***outside the CMS controlled environment.***
- I ***received*** an unencrypted email containing sensitive information from someone ***outside of the CMS controlled environment.***

All of the above. Each of these events may constitute a security and/or privacy incident. Determine if the user that received the email is the intended user. If the recipient is not the intended user, the incident must be reported immediately to the CMS IT Service Desk.