SOPP 8119: Use of Email for Regulatory Communications

Version: 11
Effective Date: April 9, 2024

Table of Contents

I. Purpose

This Standard Operating Policy and Procedure (SOPP) serves as a guide for Center for Biologics Evaluation and Research (CBER) staff on the handling of regulatory electronic messages (emails). Regulatory emails may be either internal communications or messages received from or sent to sponsors/applicants or others external to FDA.

II. Scope

This SOPP applies to all regulatory communications.

III. Background

A. Increasing overall product review efficiency has been a significant component of the Prescription Drug User Fee Act (PDUFA) from its inception. Additional efforts to increase review efficiency, include the Medical Device User Fee and Modernization Act of 2002 (MDUFMA), PDUFA and MDUFA reauthorizations, development of electronic submission infrastructure such as CBER's Electronic Repository (CER) and the FDA Electronic Submissions Gateway (ESG). All of these necessitate streamlining the review process.

B. This streamlining does not diminish the Food and Drug Administration's (FDA) responsibility for maintaining a complete, accurate, and organized administrative file to ensure that all regulatory actions/decisions are appropriately documented. As a Federal Agency, FDA is required to administer and maintain its electronic records in compliance with 36 CFR 1236, "electronic Records Management." The Office of Chief Counsel (OCC), FDA has determined that emails are legal communications acceptable as regulatory submissions upon which regulatory decisions can be made and transmitted.

C. In December 2017, the FDA published a guidance document, "Best Practices for Communication Between IND Sponsors and FDA During Drug Development," that outlines email practices that must be followed by CBER staff. Although this guidance document is written to address communication between Investigational New Drug (IND) sponsors and FDA, the principles apply to all regulatory communication. Additional guidance published in April 2014, "Types of Communication During the Review of Medical Device Submissions", outlines appropriate use of email during the review of medical device submissions.

IV. Definitions

A. Administrative File - The file or files containing all documents pertaining to a particular administrative action, including internal working memoranda, and recommendations. (21 CFR 10.3)

B. Administrative Record – The documents in the administrative file of a particular administrative action on which the Commissioner relies to support the action (21 CFR 10.3). Administrative records include sponsor/applicant submissions, CBER/FDA generated documents, and CBER/FDA system records.

C. Commercial Information - Privileged or confidential information that is valuable data or information which is used in business and is of a type customarily held in strict confidence or regarded as privileged and not disclosed to any member of the public by the person to whom it belongs. (21 CFR 20.61 (b))

D. Email String – Includes an originating email and responses. The string could be several communications between two people or several people utilizing the "reply to all" function.

E. Record copy - The document that is kept on file as an original or official master record for the total retention period. According to FDA's Office of Chief Council, the outgoing correspondence record copy must be an exact duplication of what the sponsor/applicant receives. Record copies are sometimes referred to as the archival copy.

F. **Regulatory communication** – A communication that contains regulatory information, including correspondence generated by CBER. The inclusion of a submission's submission tracking number (STN) makes a communication regulatory in nature.

G. **Regulatory Email** – An electronic message that contains regulatory information. A regulatory email may be a stand-alone message or a message with an attached file. The inclusion of a submission's STN makes the email regulatory.

H. **Regulatory Information** – Information related to products regulated by FDA, including product, manufacturing, and facility or company information, adverse events, compliance actions, CBER-generated correspondence, etc. The submission's STN is considered regulatory information, particularly if the submission is pending FDA review and action.

I. **Secure Email** – An electronic message sent from a sponsor/applicant that has exchanged secure certificates with FDA. Secure certificates typically include the entire corporate or organization structure of a sponsor/applicant or a subset of users. Secure email makes use of encryption technology during transmission and decryption upon receipt using a public key within the certificate.

Instructions on how an organization may obtain a secure email certificate are included in Appendix A.

J. **Trade Secrets** - Consists of any commercially valuable plan, formula, process, or device that is used for the making, preparing, compounding, or processing of trade commodities and that can be said to be the end-product of either innovation or substantial effort and has a direct relationship between the trade secret and the productive process. (21 CFR 20.61 (a))

V. Policy

A. Secure Email Use

1. CBER personnel are responsible for protecting company confidential, trade secret and proprietary information. Therefore, CBER-generated regulatory communications are only sent to recipients via secure email. If recipients do not have secure email, regulatory communications will be sent by U.S. postal service or commercial carrier with a follow-up facsimile allowed as a rapid means of transmitting the information.

   a. Exceptions - the following are exceptions and communication for these purposes do not require email to be secure:

i. Requests for Individual Patient INDs under Expanded Access, including for emergency use and for oncology products.

ii. Compassionate Use IDEs.

iii. Requests for Emergency Use Authorizations (EUAs) and Pre-EUAs.

iv. Responses to requests for information that are general in nature, such as providing information in a guidance document, logistical information about how to attend a meeting at the White Oak campus or where to find information on the FDA website.

v. Emergency alternative procedures or exemptions under 21 CFR 640.120.

b. CBER staff will utilize available internal resources to validate whether anyone external to FDA has established secure email with the Agency (refer to *JA 820.05: Secure Email Verification and Email Best Practices for Regulatory Communications* for information).

c. Requests to establish secure email with FDA should be sent to SecureEmail@fda.hhs.gov.

B. Incoming Regulatory Emails

1. Submissions required to be in electronic format as described in FDA's guidance document "Providing Regulatory Submissions in Electronic Format – Submissions Under Section 745A(a) of the Federal Food, Drug, and Cosmetic Act" should be submitted electronically in eCTD format via the FDA Electronic Submissions Gateway (ESG). Submissions for blood and blood components (not required to be in eCTD format) should be submitted as directed on the FDA's eSubmitter website (https://www.fda.gov/ForIndustry/FDAeSubmitter/default.htm).

2. Formal submissions (e.g., new INDs, original BLAs, etc.,), information that is unsolicited, or that FDA did not agree to receive related to pending applications are not to be transmitted via email.,

a. Any such emails will not be accepted or included in the administrative file. Regulatory actions/decisions will **not** be made based on these types of emails.

i. The CBER recipient will respond (either by telecon or via secure email) to acknowledge receipt of the email and to let the sponsor/applicant know the appropriate means of submission, e.g., ESG, eSubmitter.

Note: In the event of an outage of FDA's Electronic Submissions Gateway, please see FDA's Outage Notification and Disruption Policy web page at: https://www.fda.gov/industry/policiesguidance/outage-notification-and-disruption-policy.

ii. Emails received from the sponsor/applicant and not accepted as the official document are not tracked in CBER's regulatory systems.

iii. Such emails will be deleted from Outlook mailboxes after contacting the sponsor/applicant to prevent inadvertent disclosure.

iv. CBER personnel should discourage sponsors/applicants from providing emails without prior approval.

b. Exception – CBER will accept formal IND submissions via email for Individual Patient Use under the Expanded Access provisions found at 21 CFR 312.310 [also referred to as single patient expanded access (SPIND)].

i. For oncology product related submissions that are received from "Project Facilitate," CBER staff must follow the procedures below for incoming regulatory emails to ensure proper uploading into CBER's CER in a timely manner.

3. SPINDs submitted by a sponsor/investigator may be emailed to CBERSPIND@fda.hhs.gov. All new submissions should be clearly identified in the subject line as a new request, e.g., Original Submission SPIND. Any subsequent IND amendments should include the assigned IND number in the subject line, e.g., Amendment to IND xxxxx.

NOTE: Initial requests for emergency use for an individual patient for biological products should NOT be submitted to CBERSPIND@fda.hhs.gov. During normal business hours (8:00 AM – 4:30 PM ET), emergency use requests should be directed to CBER's Office of Communication, Outreach and Development (OCOD), 240-402-8010 or 1-800-835-4709, e-mail: industry.biologics@fda.hhs.gov. After hours (after 4:30 PM ET weekdays, all day on holidays and weekends), contact the FDA Emergency Call Center, telephone: 866-300-4374 or 301-796-8240. Follow-up submissions for emergency use requests may be submitted via email.

4. For MDUFA submissions, including BLA submissions for IVD devices, most of which are subject to the eCopy requirements for medical devices as required by Section 745A(b) of the Federal Food, Drug, and Cosmetic Act (FD&C Act), added by section 1136 of the Food and Drug Administration

Safety and Innovation Act (FDASIA) (Pub. L. 112-144), incoming emails will be accepted and then managed according to *DCC Procedure Guide 26: Use of Email for Regulatory Communications* except that emails with many or large attachments should be submitted on electronic media through DCC. Prior agreement on the acceptance of incoming email is implicit based on the eCopy Program for Medical Device Submissions and other guidances pertaining to medical device communications.

C. Outgoing Regulatory Secure Emails

1. CBER staff will send outgoing emails containing regulatory information (see definition above) **only** through secure email for all product types, including MDUFA/device submissions.

2. Emails must be sent from official FDA email accounts only as they are secure.

3. The email’s subject line will clearly define the topic addressed in the communication and the related *submission tracking number (STN),* if assigned.

4. CBER staff is discouraged from creating email strings when communicating information to outside organizations regarding regulatory information. If an email string must be used and it contains an attachment with information used in regulatory decision making, the attachment must be included in the final documentation.

5. CBER generated regulatory letters that are signed and locked using the PIV badge may be issued to the sponsor/applicant by secure email (refer to *SOPP 8116: Use of Electronic Signatures for Regulatory Documents* and *JA 820.01: Guide for CBER’s Electronic Signature Process*). **Note:** the email with the letter attached that is sent to the applicant or sponsor should not be uploaded into the CER (through CBER Connect).

6. Outgoing secure email may be used in place of telephone communication to relay regulatory issues and requests for information.

7. Communications via secure email should include only information pertinent to the referenced application or a related precursor submission (e.g., pre-IND or Master File). Exceptions would include a trans-BLA or a bundled submission, i.e., multiple submissions “bundled” consistent with MDUFA provisions for bundling and the citing of predicates.

VI. Responsibilities

A. Document Control Center (DCC)

1. Process any email submissions/amendments as appropriate for the submission type.

2. Send load notifications when document loading is complete.

B. Regulatory Project Manager (RPM)

1. Provide CBER's DCC with a full electronic version of emails accepted as regulatory submissions. Note: this only applies to submissions not required to be in electronic format as described in Policy Section B (2), above.

2. Ensure all email communications are captured in the appropriate regulatory system and uploaded through CBER Connect.

3. Send regulatory communications via secure email only and ensure correct recipient is selected if auto-complete function of MS Outlook is used.

C. CBER recipients (of emails from sponsors/applicants) and authors of secure email

1. Include the RPM on all outgoing secure emails pertaining to a regulatory submission.

2. Ensure email is only sent to recipients that have secure email and that correct recipient is selected if auto-complete function of MS Outlook is used.

3. Provide information about how to obtain secure email to those that need instructions (see Appendix A).

4. Ensure incoming email submissions meet the acceptability requirements described in the Policy Section of this SOPP.

5. Respond to the sponsor/applicant in the appropriate timeframes as documented in the procedures section.

6. Forward all emails that did not include the RPM of a regulatory submission as an addressee **within one business day** to the RPM and remind the sponsor/applicant to include the appropriate RPM on all future emails.

7. Process internal emails that capture regulatory actions or decisions as part of the administrative file, i.e., log them into the appropriate regulatory system and upload through CBER Connect.

8. Document all emails appropriately as described in the procedures section.

9. Set Out-of-Office replies with an available point of contact for time periods away from email one day or more.

VII. Procedures

A. Incoming Regulatory Emails

1. Notify the sponsor/applicant by phone within **one business day** of receipt of an email if it is inadequate or cannot be read. CBER will reach a decision on whether the email should be resent, rejected, referred to DCC, or should be submitted in another format. **[RPM, CBER recipient]**

2. Remind the sponsor/applicant that all emails should be submitted to the appropriate RPM. **[CBER recipient]**

   a. Forward the email within **one business day** to the RPM for processing. **[CBER recipient]**

3. If CBER agreed to accept a submission as the official document, if it is a MDUFA product communication or if it is a Single Patient IND under expanded access, provide CBER's Document Control Center (DCC) with a full electronic version of the email per *DCC Procedure Guide 26: Use of Email for Regulatory Communications.* **[RPM or designee]**

B. Outgoing Regulatory Emails

1. Always include the RPM as a courtesy copy (cc:) on secure emails sent to sponsors/applicants related to a regulatory submission and inform the sponsor/applicant in the secure email to include the RPM on any responses or future emails, if the RPM was not included in the original email. **[CBER recipient, author]**

2. Determine the appropriate communication type for the email for data entry purposes. Emails will be entered as telecons only if the information would generally have been discussed in a telecon. Refer to *SOPP 8104: Documentation of Telephone Contacts with Regulated Industry* for additional information*.* **[CBER recipient, author or RPM or designee]**

VIII. Appendix

A. Appendix A: Secure Email Setup

IX. References

A. References below are CBER Internal:

1. DCC Procedure Guide #22: Procedure for Processing, Routing, and Storing Electronic Submissions

2. DCC Procedure Guide #26: Use of Email for Regulatory Communications

3. JA 820.01: Guide for CBER's Electronic Signature Process

4. JA 820.05: Secure Email Verification and Email Best Practices for Regulatory Communications

B. References below can be found on the Internet:

1. 21 CFR 601.14

2. Guidance for Industry and Review Staff: Best Practices for Communication Between IND Sponsors and FDA During Drug Development

3. SOPP 8104: Documentation of Telephone Contacts with Regulated Industry

4. Guidance for Industry and Food and Drug Administration Staff: Types of Communications During the Review of Medical Device Submissions

5. Guidance for Industry and Food and Drug Administration Staff: eCopy Program for Medical Device Submissions

6. SOPP 8116: Use of Electronic Signatures for Regulatory Documents

7. Guidance for Industry: Providing Regulatory Submissions in Electronic Format – Submissions Under Section 745A(a) of the Federal Food, Drug, and Cosmetic Act

X. History

Written/ Revised	Approved By	Approval Date	Version Number	Comment
Monser	Katie Rivers, MS, Chief, RABOB/DROP /ORO	April 9, 2024	11	Clarifies that initial requests for emergency individual patient expanded access should not be emailed to CBERSPIND@fda.hhs.gov.
Monser	Katie Rivers, Acting RABOB Chief	November 23,2022	10	Removes safety issues as an exception for sending regulatory submissions via email.

C. Williamson (OIMT)	Darlene Martin, MS, PMP, RABOB Chief	January 22, 2021	9	Appendix updated to current procedures.
Monser	N/A	December 11, 2020	8	Technical Revision for retirement of EDR and replacement with CER/CBER Connect and replacement of “database” with “system’
Monser	Christopher Joneckis, PhD	February 17, 2020	7	Revised to exempt all requests for individual patient expanded access INDs
Monser	Christopher Joneckis, PhD	August 26, 2019	6	Revised to change email policy for all single patient INDs and corrected typographical errors.
Martin	Christopher Joneckis, PhD	June 4, 2019	5	Revised to change email policy for oncology product Single Patient INDs
Monser	Christopher Joneckis, PhD	April 14, 2019	4	Revised to be consistent with SOPP 8116
Rehkopf	Christopher Joneckis, PhD	September 27, 2018	3	Revised to include use of secure email and update
BPWG/RMCC	Robert A. Yetter, PhD	February 11, 2009	2	Revised to include additional information on secure email
Thomas	Robert A. Yetter, PhD	September 12, 2008	1	First Issuance of this SOPP

SOPP 8119 Appendix A: Secure Email Setup

For FDA to send regulatory information via email, the email must be sent to a Secure E-mail partner, to allow FDA to digitally sign and encrypt the message. Requests to establish secure email with FDA should be sent to SecureEmail@fda.hhs.gov. Adequate time should be allotted for Secure Email set-up before expecting email responses from FDA.

To setup secure email with the FDA you must have a non-ISP email domain. Thus, @yahoo.com, @gmail.com, @hotmail.com, @earthlink.net, @verizon.net, etc., accounts cannot be secured.

If you have a non-ISP email domain:

There are two ways to securely send email to and from the FDA:

1. S/MIME Encryption
    a. S/MIME encryption is difficult to setup, use, and maintain as everything is done at the workstation level.
        - Typically, your certificate will need to be repurchased/renewed once-a-year. This will require the new certificate to be installed on your workstation and coordination with the FDA to attach it to your Secure Email profile. Thus, over a 5-year period, you will switch out your certificate 5 times.
        - If you change workstations or when you renew your digital certificate, your old certificates must be preserved otherwise you will lose the ability to read old encrypted emails.
        - If you have a Blackberry (or other mobile device), you will not be able to read the encrypted emails unless you install the Blackberry (or similar) S/MIME application and copy your certificate over. Any new certificates will need to be copied over.
        - For each FDA user or mailbox you wish to securely communicate with, a one-time setup process is required to create an FDA Outlook contact and corresponding FDA proxy certificate.
        - S/MIME is setup on a per user basis. Thus, if you wish 10 of your users to send secure email to the FDA, then they each have to be configured individually.
        - Your email server may apply disclaimers or legal notices on all outbound emails. An exception will need to be applied to the email server's transport rule to avoid doing this when sending to the FDA. The reason is disclaimers affect how S/MIME protected email is repackaged. These alternations cannot be processed correctly by the FDA S/MIME Email Firewall. Therefore, add the disclaimers via your email client (i.e. make it part of your default signature.) <u>If your organization requires these disclaimers to be appended by your email server, then you cannot use S/MIME and must use TLS.</u>

b. S/MIME does have the following advantages:
   - Technically adept users can set this up themselves and not involve their email administrators.
   - “End-to-end” encryption can be achieved. Thus, from your email client to an FDA internal S/MIME Email Firewall, the message is encrypted. This encryption is typically preserved regardless of the intermediate infrastructure.
   - Email sent to and received from the FDA will remain encrypted in your Inbox. Thus, even if your emails are stolen, they will remain encrypted.
   - A one year digital id (email certificate) for one person is around $60.
   - After the certificate is purchased and installed, typical setup with a knowledgeable IT staff is a couple hours.
   - After the first user in your organization is setup, the FDA S/MIME instructions can be shared and users can setup themselves; no intervention by the FDA Email Team is required.

2. Secure SMTP over TLS encryption
   a. Secure SMTP over TLS encryption (RFC3207) is far simpler to setup from the user perspective.
      - The configuration is done at the email server level and only involves your email administrator.
      - It will be your email administrator’s responsibility to ensure all the intermediate links between your infrastructure and the FDA (and vice-versa) are TLS encrypted.
      - Everyone at your organization will be able to send email securely to the FDA.
      - A one year DigiCert SSL certificate is $175. A three year certificate is $420.
      - If your organization’s email system is all internal, then total setup time is:
        - Certificate purchase and receipt is typically one to two days as the provider may need to perform verification.
        - Certificate installation and TLS setup with a knowledgeable email administrator is a couple of hours and a few emails.

If parts of your organization’s email system are outsourced, then setup time may be considerably longer as coordination with a third party and multiple links are involved.

S/MIME Instructions

Listed below is an overview of the steps of setting up S/MIME encryption with the FDA.

- The FDA proxy S/MIME server has been tested with the following clients:

  Windows 10 with Outlook 2016

  These instructions have been tested with Windows 10 and Outlook 2016. Previous versions of Windows and Outlook have worked. Therefore, you need to adapt these instructions to your particular combination of

Windows and Outlook. For assistance, please contact your local IT HelpDesk resources.

Mac OSX 10.12.3 (Sierra) with Outlook 2016

These instructions have been tested with Mac Sierra and Outlook 2016. It is unlikely previous versions of Outlook will work correctly. It is unknown if previous versions of Mac will work. For assistance, please contact your local IT HelpDesk resources.

- Obtain and install a digital ID from a Certificate Authority that has a good reputation (i.e. GlobalSign, DigiCert, etc.) (If already have a digital ID on another computer, you should use that certificate and its private key otherwise you will not be able to read older, encrypted emails.)

  https://www.globalsign.com/secure-email/

  SHA256 certificates are the current standard. If you have an older SHA1 certificate that has not yet expired, you may continue to use that.

If you are the first in your email domain (i.e. @yourcompany.com) to request S/MIME Secure Email, please proceed to step #3 otherwise, proceed to step #4. If you are unsure if you are the first in your company, you can proceed with step #3.

- Send a digitally signed only (no encryption) message to:

  To: SecureEmail@fda.hhs.gov
  Subject: S/MIME request

  Specify that you would like to be configured to use S/MIME with the FDA

Windows 10 + Outlook 2016 client

Press the **Options** tab, and then press the **Sign** button

Mac 10.12.3 (Sierra) + Outlook 2016 clients

Press the **Options** tab, then press **Security** and then select ***Digitally Sign Message***

The FDA Email Team will then configure internal email routing to allow your email domain to send/receive email from the FDA proxy S/MIME system. When you receive confirmation from the FDA Email Team that this has been done, please proceed with the next step.

- Send a digitally signed only (no encryption) message to:

  To: cert-query@fda.hhs.gov
  Subject: {the email address of the FDA recipient you wish to securely communicate with}

Windows 10 + Outlook 2016 client

Press the **Options** tab, and then press the **Sign** button

Mac 10.12.3 (Sierra) + Outlook 2016 clients

Press the **Options** tab, then press **Security** and then select ***Digitally Sign Message***

Within 5 minutes you will receive an email back with a proxy FDA certificate

- From that email:

Windows 10 + Outlook 2016 client

If you see a yellow triangle with an exclamation mark on the right side:

a. Click on the yellow triangle, a **Digital Signature Invalid** dialog box will open.
b. In the **Trusting the Certificate Authority**, click ***Trust***
c. In the **Security Warning** dialog box, read the warning and if you agree, click ***Yes***
d. Restart Outlook.

If you decided earlier in the **Trusting the Certificate Authority** **<u>not</u>** to Trust the FDA Certificate Authority, complete the following steps *for every FDA contact*:

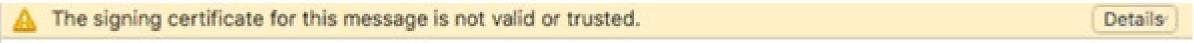
a. A new contact will open, press ***Save*** then in **View Source** click on ***Outlook (Contacts)***
b. A large contact box will open that has many options. In the ribbon, locate the ***Certificates*** button.
c. For the **fda.hhs.gov (proxy)(Default)** certificate, click ***Properties***, then the ***Trust*** tab.
d. In **Edit Trust**, select ***Explicitly Trust this Certificate*** then ***OK***

If you see a red ribbon on the right side:

a. Open the email and locate the from field and right-click on the FDA person's name and select **Add to Outlook Contacts**

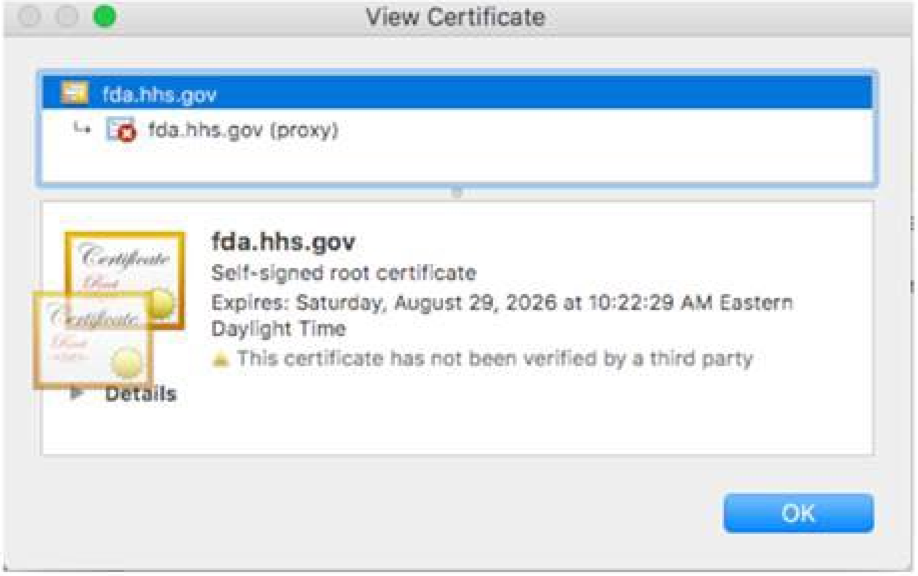
Mac 10.12.3 (Sierra) + Outlook 2016 clients
(https://technet.microsoft.com/en-us/library/jj984223(v=office.16).aspx)

If you see a yellow triangle with an exclamation mark on the left side with the message **"The signing certificate for this message is not valid or trusted"**



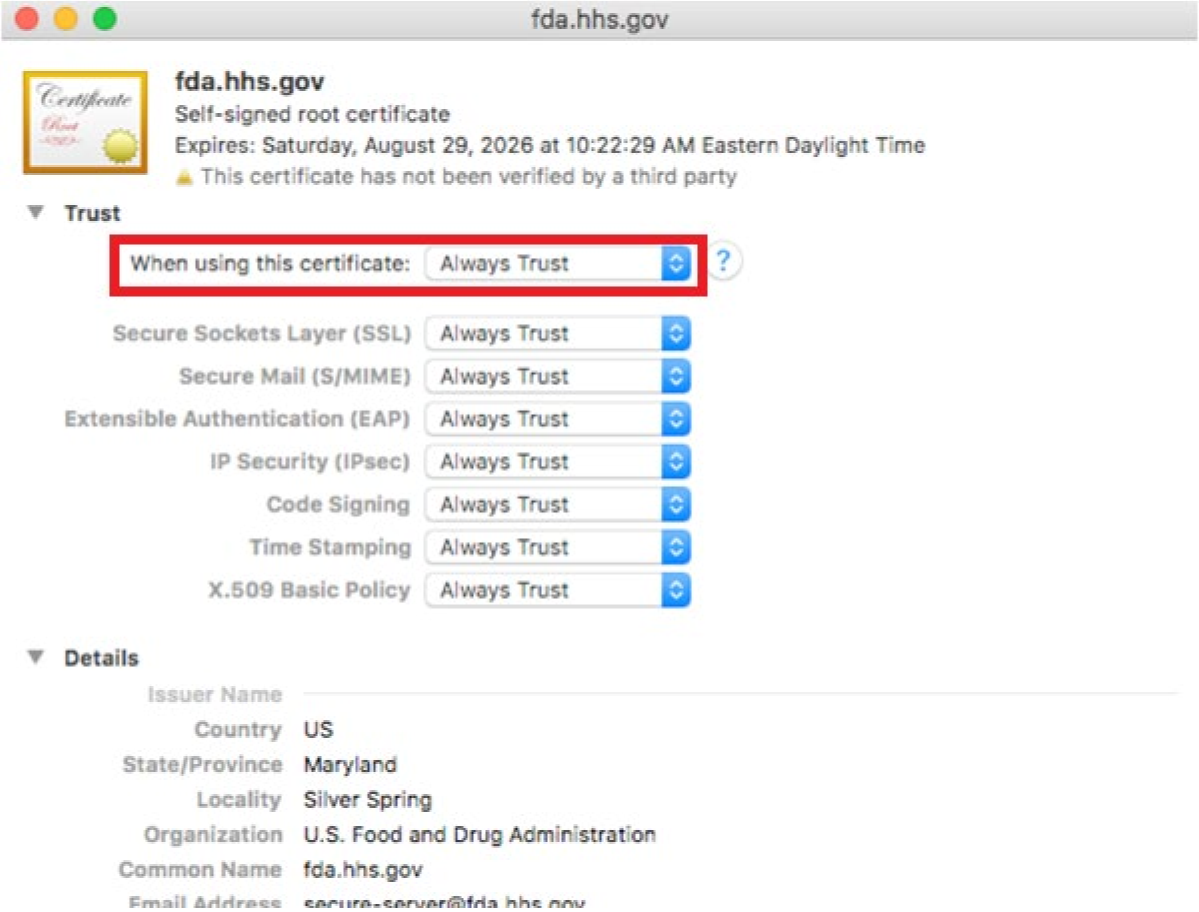
⚠ The signing certificate for this message is not valid or trusted.

a. Click on the **Details** button and select ***View Signing Certificate***
b. In the **View Certificate** dialog box, in the top pane, click on the ***fda.hhs.gov*** certificate, then in the bottom pane, drag the root CA certificate to your desktop



fda.hhs.gov
Self-signed root certificate
Expires: Saturday, August 29, 2026 at 10:22:29 AM Eastern Daylight Time
This certificate has not been verified by a third party

c. Open the Mac **Keychain Access** applet.
d. In the top left side, select **Keychains/login** and in the bottom left side, select ***Category/Certificates***
e. Drag and drop the **fda.hhs.gov.cer** root Certificate into the right pane
f. Locate the newly copied certificate and in the **Trust** section, select ***When using this certificate: Always Trust***



fda.hhs.gov
Self-signed root certificate
Expires: Saturday, August 29, 2026 at 10:22:29 AM Eastern Daylight Time
This certificate has not been verified by a third party

When using this certificate:	Always Trust
Secure Sockets Layer (SSL)	Always Trust
Secure Mail (S/MIME)	Always Trust
Extensible Authentication (EAP)	Always Trust
IP Security (IPsec)	Always Trust
Code Signing	Always Trust
Time Stamping	Always Trust
X.509 Basic Policy	Always Trust

Issuer Name	
Country	US
State/Province	Maryland
Locality	Silver Spring
Organization	U.S. Food and Drug Administration
Common Name	fda.hhs.gov
Email Address	secure-server@fda.hhs.gov

g. You may be prompted for user username and password to authorize the change. Enter this and press ***Update Settings***
h. Close and restart Outlook.
i. The email that was received earlier should no longer display the yellow triangle with the exclamation mark and instead should have a padlock and notation **This message was digitally signed by…**

If you see a yellow triangle with an exclamation mark on the left side with the message **The signing certificate for this message is not valid or trusted**

a. Click the **Details** button and select ***Add Encryption Certificate to Contacts***
b. Press ***OK***

- You are now configured to use S/MIME secured email with your FDA contact.

IMPORTANT: It is your responsibility to keep your S/MIME certificate up-to-date. If your certificate expires, it is possible that future emails you receive from the FDA will no longer be encrypted.

Food and Drug Administration (FDA) Instructions for Using Secure SMTP over TLS

- The Food and Drug Administration (FDA) only support “Enforced TLS” for securing SMTP over TLS connections between your organization and the FDA. Most modern MTAs use “Opportunistic TLS” or “TLS Preferred” when sending email but this is not considered secure email for two reasons: Opportunistic TLS opens the possibility of man-in-the-middle attacks — Refer to RFC3207, Section 6 (http://www.ietf.org/rfc/rfc3207.txt) If Message Transfer Agents (MTAs) are too busy or exceed their global TLS connection limit, MTAs can drop TLS and send or receive the message in clear text which is not secure.

Please Note the following:
By default, many hosted email providers (i.e. Office 365) will use opportunistic. You should be able to request that your email hosting provider to set up the necessary Enforced TLS connectors to the various FDA domains/sub-domains. If you are unable to obtain an “Enforced TLS” connection, then you will need to use S/MIME encryption instead.

Instructions:
Please read the following instructions carefully and follow them to ensure a secure end-to-end connection between your company and the FDA.

1. **For in-house email servers**: On your email server or mail appliance obtain and install a commercial grade certificate such as Verisign or Thawte. Digicert is a lower cost

alternative that is trusted by our MTA. Do not use a self-signed certificate or a private CA signed certificate.

In the future, the FDA will be enabling FIPS 140-2 on the Internet-facing MTA's. Therefore, you must ensure that your certificate keys are generated with sufficient length. If using RSA as the asymmetric algorithm, you must use at least a 2048-bit key size when generating the public/private keys. On your MTA, you must ensure that you have cipher suites that are compatible with FIPS 140-2. http://csrc.nist.gov/publications/PubsFIPS.html. The one exception to the NIST guidance is 3DES. Department of Homeland Security has mandated this cipher no longer be used: https://cyber.dhs.gov/bod/18-01/

When installing the certificate, it is important to install any intermediate/issuing CA's (the root cert is optional). Failure to install the intermediate/issuing CA's may result in a certificate verification/validation failure: "unable to get local issuer certificate".

Note: If you use a Barracuda MTA, you may need to combine your leaf and intermediate/issuing CA certificates into a single .pem file, install it, and then reboot the appliance.

Your certificate should have the names specified in your external DNS. Thus, if your external DNS name is smtp.pharma.com, that should be the Common Name and, if you use them, one of the Subject Alternative Names. Or, if you are using multiple email servers, you can use a wildcard certificate by specifying *.pharma.com for your Common Name.

The FDA will use the MTA(s) specified in your organization's MX records and will not create special routes to "TLS only" MTA(s). Part of the verification process is to do a reverse DNS lookup on your mail server/appliance specified by your organization's MX records. Thus, if smtp.pharma.com is at 100.100.15.16, then a reverse lookup of 100.100.15.16 should return smtp.pharma.com. You can only have one PTR record per IP address.

> You may want to verify your TLS configuration with http://www.checktls.com/perl/TestReceiver.pl.
>
> Put your email address in and for "Level of Output" select "CertDetail". Address any issues that are highlighted in yellow. One problem this website tool has is that it does not verify wildcard certificates. However, the FDA's MTA will accept wildcard certificates. Therefore, although this website's TLS verification methods differ slightly from the FDA's methods; it is useful in identifying the majority of TLS problems.
>
> It may be helpful to examine how TLS is setup (MX records, Public-Key key length, etc) on the FDA's boundary MTAs. To examine this, go to

http://www.checktls.com/perl/TestReceiver.pl, type in: SecureEmail@fda.hhs.gov and for "Level of Output", select "CertDetail".

The FDA MTA's use DigiCert certificates. This should be trusted by most MTA's. However, if you need to install the root certificate, you can download it here: https://www.digicert.com/CACerts/DigiCertGlobalRootCA.crt

2. **Certificates**: Configure your organization's MTA to use "TLS require" when sending to the FDA. The following are the FDA name spaces that may need to be configured on a custom TLS "send" or "SMTP" connector (if using Exchange)

   fda.hhs.gov
   fda.gov
   fda.gov

   At this time do not configure MTLS with the FDA. This is not currently supported.

   If you use Exchange as your internet-edge MTA, you may find the following helpful:
   - TLS with Exchange: If you configure a custom "TLSRequire" send connector, then you will need to run this PowerShell command:

     Set-SendConnector –identity "name of connector" -RequireTLS:$true

     https://docs.microsoft.com/en-us/powershell/module/exchange/mail-flow/set-sendconnector?view=exchange-ps

     Following the recommendations in IETF RFC 7525:
   - MTAs must not negotiate SSLv3 (due to POODLE risk).
   - TLS 1.0 and 1.1 do not support some of the strong ciphers, should be used only when TLS 1.2 or higher version is not available.
   - Implementations should not use symmetric cipher suites with key length less than 256 bits. In case of RSA, the minimum is 2048 bits.

3. **Outsourced Services**: Is any part of your email flow (sending or receiving) outsourced? Is your email hosted by a 3rd party? If so then you may need to contact your provider for assistance. They will also need to ensure that any links that connect through the Internet from the FDA to you are encrypted. For example:

   Sending to the FDA

   1. Do you use a "smarthost" on your in-house email server? If so, you should ensure that the connection between your email server and the smarthost is "TLS Require" (not "TLS Preferred") encrypted. Also, the hop between your "smarthost" and the FDA should also be "TLS Require" encrypted (not "TLS Preferred"). Any links that your "smarthost" provider exposes to the Internet when routing your email should also be encrypted.

2. If your email servers are hosted, does your email client have an encrypted connection to the hosted email server? Also, you will need to contact your email vendor to ensure that any email sent to the FDA domains (listed above) is sent only "TLS Require".

Receiving from the FDA

The FDA can only guarantee that the first link between the FDA and the servers specified in your public MX records are "TLS Require" encrypted, beyond that it is your responsibility to ensure the remaining links are encrypted. Thus:

1. **Where do your DNS MX records point?** If they point to outsourced servers, you will need to contact the vendor to ensure that when they route your email over the Internet that the path is over "TLS Require" links. The same would apply if your MX records point to outsourced anti-virus/anti-spam servers. When they deliver the email to you, it should be done over "TLS Require" links.
   If you use Google G Suite, please note the following:
2. https://support.google.com/a/answer/2520500?hl=en Keep in mind that whenever you switch email and/or anti-malware providers that the above precautions are adhered to. This will ensure that any Internet links are encrypted. If your provider requires any information on how the FDA is configured (Certificate Authority used, certificate key size, IP addresses, etc.), then go to http://www.checktls.com/perl/TestReceiver.pl, type in: SecureEmail@fda.hhs.gov and for "Level of Output" select "CertDetail".**Test Message to FDA**: Send me an email indicating the "TLS Require" has been setup outgoing to FDA. Check your message tracking logs. If the message fails to get delivered to the FDA, recheck your configuration.
3. **Test Message from FDA**: When I receive that email, and after your configuration is verified, I will correspondingly switch the FDA's outgoing connection to your organization to "TLS Require" and send you an email. If there are any issues, I will drop the connection back to "TLS Preferred" and contact you.
4. **S/MIME Usage**: If TLS is working and you are currently using proxy S/MIME with the FDA:
   1. Your S/MIME secure email configuration will be removed from the FDA servers.
   2. You will need to remove the FDA proxy certificate from your users' Outlook FDA contacts (if these exist) and instruct your users not to press "encrypt" when sending to the FDA as encryption will be handled automatically from the server-side.
5. **Certificate Renewal Reminder**: As a suggestion, you may want to create a calendar reminder one month before your TLS certificate is due to expire. This timeframe would be sufficient time to renew and install your new certificate.