HIPAA Faxing Checklist

EC Data Systems, Inc.
Last Revised: March 20, 2018

Contents

Confidentiality Notice

This documentation is the confidential and proprietary property of EC Data Systems, Inc. These materials are provided only for the purpose of an existing or potential customer evaluating and potentially implementing fax functionality using the FAXAGE Internet fax service. Any other use or disclosure is strictly prohibited unless the express written consent of EC Data Systems, Inc. is obtained in advance of such use or disclosure.

Introduction

FAXAGE offers mechanisms designed to allow our service to be used in a HIPAA compliant fashion. This checklist is provided by FAXAGE to you in order to guide you through the decision making process. The goal is to ensure that your setup with us meets your security needs.

It is important to understand that there is no one-size-fits-all solution that is 'HIPAA compliant' all by itself, but rather there are different ways to address sending and receiving Protected Health Information (PHI) so that it is not exposed to eavesdropping.

In principle, the most important consideration is to ensure that your faxes, which may contain PHI, are not sent in an unencrypted fashion between FAXAGE and your computer, smart phone or whatever means you use to access incoming faxes and send outgoing faxes. Additionally, it is important to ensure that we have committed to you to comply with HIPAA as either your Business Associate or Subcontractor, as may be appropriate for your situation.

This checklist mainly addresses email fax sending and receiving specifically, though the BAA (Step 1) is applicable in all situations. The FAXAGE website outgoing fax sending and incoming fax downloading and API interfaces are always SSL/TLS protected without any need for you to make any special settings to enable that protection.

Our checklist follows. We hope that it will be helpful to you and encourage you to reach out to us at support@faxage.com if you have additional questions that we can help you to address.

Checklist

Step 1 - FAXAGE BAA

The first step is to get a Business Associate Agreement (BAA) in place with us. To request a BAA, simply email support@faxage.com. We will send you our BAA in which you will:

a. Fill out your information in the first paragraph and sign the last page
b. Return the completed BAA to us either via scan and email to support@faxage.com or fax to 303.991.6021.
c. We will return a countersigned copy for your records within 1 business day or less.

Having obtained the countersigned copy above, this step is complete.

Step 2 – Address Receiving Faxes

The second step is to determine how best you would like the system to send you faxes that are received for you. By default, the system is set up to email them to the email address you supplied when you signed up for faxes. This may be good enough if you have a TLS/SSL enabled email service, but it is something to consider. Select one of the following options:

1. **TLS Secured Email Transport -** FAXAGE will automatically prefer to use TLS email if your email server offers it. What this means is that the email will be sent to your email server from FAXAGE's email server in an encrypted session (like a secure download from an https secure website). However, it is important if this option is selected to:
    a. Ensure that your email account does support TLS (ask your email provider).
    b. Understand that while the email transmission from FAXAGE to your email server will be secured in accordance with HIPAA guidelines, the fax itself is just a regular PDF file and could be read from your email if someone other than you had access to your email account. This could be mitigated either by deleting your received faxes from your email periodically or by ensuring that others do not access your email account without your permission.

2. **Secure Email via Sending you a Link** – If you do not have a TLS capable email service and/or if you prefer that faxes not be stored in your email box, you can configure FAXAGE to send you a link to download your fax securely (which requires logging in to the FAXAGE website to make the download happen) instead of attaching the actual fax. This is done by:
    a. Log in to your FAXAGE account at https://www.faxage.com/login.php
    b. Click on 'Admin'
    c. Under 'Incoming Fax Settings', select 'Secure Email'
    d. Select the 'On/SSL' option
    e. Click the 'Apply Changes' button

3. **Secure Email via Password Protection –** It is possible to receive your faxes and have them stored in your email box, but encrypted with a password that is required to open the PDF each time. This encryption is done using AES 128 bit encryption and can be changed to 256 bit, if desired by emailing us at support@faxage.com and requesting that it be upgraded to 256 bit. To set this up:
    a. Log in to your FAXAGE account at https://www.faxage.com/login.php
    b. Click on 'Admin'
    c. Under 'Incoming Fax Settings', select 'Secure Email'
    d. Select the 'Password' option and type in a password of your choosing
    e. Click the 'Apply Changes' button

4. **Secure Email via PGP** – If you use PGP, the 'Secure Email' page referenced in #2 and #3 above allows you to upload your public PGP key and select the 'PGP' option. This is only recommended for clients who already know how to use PGP, as FAXAGE does not offer support in terms of your PGP software and configuration.

Step 3 – Address Sending Faxes

The third step is to figure out how you would like to send faxes in a secure fashion. The easiest option is to just send faxes from our website and not to use your email to send faxes, as all sessions are secured automatically via SSL/TLS when logged in to the FAXAGE website. If you do wish to send faxes from your email, please select one of the following options:

1. **TLS Secured Email Transport -** FAXAGE will automatically use TLS email if your email server requests it. What this means is that the email will be sent from your email server to FAXAGE's email server in an encrypted session (like a secure upload to an https secure website). However, it is important if this option is selected to:
    a. Ensure that your email account does support TLS (ask your email provider).
    b. Understand that while the email transmission from your email server to FAXAGE will be secured in accordance with HIPAA guidelines, the fax itself could be read from your email outbox or 'sent' folder if someone other than you had access to your email account. This could be mitigated either by deleting your sent items periodically or by ensuring that others do not access your email account without your permission.

2. **PGP Encrypt your Attachments** – If you use PGP, you can encrypt your attachments using our public key associated with the email address pgp@faxage.com. We will automatically decrypt any files having the extensions '.asc', '.pgp' or '.gpg' that arrive for faxing here. Like PGP fax receiving, FAXAGE does not offer support for your PGP software or setup, it is assumed that you already know how to use PGP if selecting this option. Some considerations to keep in mind:
    a. The public key for pgp@faxage.com is available for download by:
        i. Log in to your account at https://www.faxage.com/login.php
        ii. Click on 'Admin'
        iii. Under 'Company Settings', select 'PGP Keys'
        iv. Click the link that says 'download our public key'
    b. Your faxes are still to be emailed to (number)@faxage.com or fax@faxage.com with the number in the subject line, not to pgp@faxage.com. Thus, it is necessary to either encrypt the attachments offline using the pgp@faxage.com public key using your PGP software and then attach them to a regular email or to configure your PGP email plugin in such a way as to be able to use the pgp@faxage.com public key for encryption, even though you are not emailing to pgp@faxage.com.