

Encryption and the Protection of Amesbury Email

Email is an insecure method for sharing information and you should always use an approved secure method to transmit your protected information. If you need to transmit protected information, both the sender and recipient must agree to the method that you are using. This email encryption is to protect information that has been inadvertently sent through email.

Below are links regarding records and why they should not be emailed:

- Medical Records
 - o From the Anna Jacques Hospital Website regarding medical records requests and the protection of patient records:
 - ***All records will be mailed to the address specified on the Release of Information Authorization Form. To protect patient privacy, they will not be faxed except in the case of emergency care to the provider; we do NOT email patient information under any circumstances.***
- Tax Documents
 - o Secure Ways to Send Tax Documents to Your Accountant
 - <http://taxes.about.com/od/findataxpreparer/tp/secure-ways-to-send-tax-documents.htm>
- Student Records - FERPA
 - o From The University of Washington, please see the section ***“Email is safe? RIGHT?”***
 - <https://depts.washington.edu/registra/blog/2013/02/05/ferpa/>

Our server that delivers email from Amesbury to the outside world has a Data Loss Prevention component that has been active since November 2014. The server has been scanning and blocking emails that may contain the following information:

- Confidential
- Health Information
- Credit Card/Debit Card Information
- Driver’s License Number
- Bank Account Information
- Passport Information
- A combination of the following information
 - o Name
 - o Address
 - o Account Number
 - o Student Name
 - o Student ID Number

When the server finds a combination of information from the list above, it will perform the following steps to protect the information from possible compromise:

1. Encrypt the information (encryption information is below)
 - a. http://esa.sophos.com/docs/esa/sea_docs/en/ESA/concepts/SPXOverview.html
2. Automatically add a password that will allow the recipient to open the email
3. Send the password to the "Sender" of the email which they will need to share "SECURELY" with the recipient
 - a. EMAILING the password is NOT a secure way to share the password
4. Here are document links that can give you some insight as to why the emails are being scanned and encrypted.
 - a. [http://www.zixcorp.com/documents/case-studies/Case for Email Encry Required by Law.pdf](http://www.zixcorp.com/documents/case-studies/Case%20for%20Email%20Encry%20Required%20by%20Law.pdf)
 - b. <http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf>
 - c. <http://www.tomsguide.com/us/personally-identifiable-information-definition,news-18036.html>

Documents that are public record can be uploaded to your portion of the Amesburyma.gov website if they are inadvertently encrypted by our server and cannot be emailed. You can email a link to our website and recipients can download documents and bypass any encryption that does not need to be applied.