What is considered PHI?
The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:

- Names;
- All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census: the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000;
- All elements of dates (except year) for dates directly related to an individual, including birthday, admission date, discharge date, date of death; and ages over 89 and elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into single category of age 90 or older;
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social security numbers;
- Medical record numbers;
- Health plan beneficiaries number;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URL’s);
- Internet Protocol (IP address numbers);
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images; and
- Any other unique identifier number, characteristic, or code, except as permitted by the section entitled "Re-Identification" of this policy; AND
- Spectrum Health does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

What is considered PII?
All of the above listed under PHI but when it is noted for someone other than a patient, i.e., employees, vendors, etc.

Sending Secure E-mail
Protected Health Information (PHI) and similarly sensitive material cannot be communicated over regular e-mail for security purposes. You can use the settings in Outlook 2007 or Outlook 2010 to send a secure message that will protect contents via encryption. ****Note – All emails with sensitive data must be secured each time you send an email (new emails, replying to an email or forwarding an email) even if you secured the initial email.
**How does Secure E-mail Work?**
Message sent to someone else within the Spectrum Health organization is already secure and will be sent and received normally. Some recipients outside of Spectrum Health might be running special security software that will make it possible for them to receive secure e-mails normally as well. However *some* external recipients will receive a message that says they have a secure e-mail waiting for them. They will then access a Secure Web Mail portal web page where they can create a password to access the message.

**How Do I Send a Secure Message?**

Option 1

1. Type [secure] on the subject line of the email (square brackets required). Please ensure there is a space after [secure] before the subject starts.

2. Send your message as normal

Option 2

1. Type the subject on the subject line then a space before placing [marked for secure delivery] (square brackets required).
Option 3 (Windows 7)

1. Type your message as normal
2. Click the small arrow to the bottom of tags

3. Change the sensitivity to confidential

![Image of Properties window with sensitivity set to Confidential]

4. Click Close

Option 3 (Windows XP)

1. Type your message as normal
2. Click the Message Options button in the bottom-right hand corner of the Options section; the Message Options window will appear.

3. In the Message Settings section of the Message Options window, set the Sensitivity pull-down to Confidential.

4. Click Close.

5. Send your message as normal.
How Will My Secure Message be Received?
Members of the Spectrum Health organization and some external parties who are running secure e-mail software will receive your message normally. But some recipients will instead receive a message from you that looks like this example:

You have received a Spectrum Health secure email from frank.vanlangfort@spectrum-health.org. Please click on the link below to retrieve your message.

View Message

- First time users will be prompted to create/confirm a new password and then answer security questions which can be used to reset a forgotten password
- Passwords must be 8 characters in length with one numeric and one uppercase character
- Previously registered users will be prompted for their password

Forgot Your Password?

For Additional assistance please contact the Spectrum Health Help Desk at 616.391.1361 or helpdesk_tis@spectrum-health.org

This allows individuals or entities that are not running secure e-mail software can still receive protected information

By following these instructions, your recipient will be able to access the secure site and retrieve the message you sent them. Once they have followed these instructions, they will be able to use the password they set up to access any secure e-mail you send them in the future from the Secure Web Mail Portal.

📖 Take Note: Many people are wary of clicking links they receive via e-mail and creating accounts & passwords. For this reason, it’s a good idea to inform your recipient in advance that they may be receiving a message from you similar to the one above so they know it is trustworthy.
Sending Secure Email

Spectrum Health has implemented a Data Loss Prevention (DLP) system, which meets HIPAA/HITECH standards and the internal policies for protecting sensitive data (365 - De-identification of Protected Health Information Policy).

The DLP system constantly monitors for PHI, Personally Identifying Information (PII) and Spectrum Health sensitive data sent outside of the network unsecured (355 - Electronic Messaging Appropriate Use). ****Note - All emails with sensitive data must be secured each time you send an email (new emails, replying to an email or forwarding an email) even if you secured the initial email. [Secure] should appear on the subject line if you are replying to an email stream where you previously placed it there. This was previously stripped as emails left the network but will no longer be stripped. This should help determine whether an email is still secured when replying to a previously secured email stream.

The DLP system monitors email, including emails sent to mobile devices that are hosted by third-party organizations, texts sent from Insite, emails sent by copy machines, web posts that contain sensitive data, emails sent using Internet email accounts and automated emails sent by different systems within the network.

Examples of PHI:

- Name and medical record number
- Name and diagnostic information with enough information to allow a third party to determine the patient
- FIN and location
- Name without any other identifiers

Examples of PII:

- Social Security number
- Federal Employer Identification Number for privately held organizations
- Credit card numbers

Examples of Spectrum Health Sensitive Data:

- Research or medical protocols that are not available to the public
- Financial data
- Anything that is not to be viewed by the public

There are two methods for sending email securely from the desktop:

- Mark the email confidential using the confidentiality flag under Microsoft Outlook's options menu; select more options or click the small arrow in the bottom right of the options ribbon and change the sensitivity to Confidential
- Type [secure], square brackets required, on the subject line of the email in Microsoft Outlook

If emailing from multifunctional devices (Xerox Machine, etc):

- Type [secure], square brackets required, on the subject line of email on the device.

Either method enables Spectrum Health to encrypt the email before it is sent outside of the network. It also protects the recipient if they are not using encryption to protect email once it is received and redirected.

For more information on how to secure emails and what the recipients can expect when receiving a secured email if they do not have encryption, visit the following InSite page.

It is imperative that employees are vigilant in protecting sensitive data that is sent outside of the network electronically. If you have questions, contact Cheryl Waters, senior security analyst, at 616.486.4080. Thank you for helping Spectrum Health to remain compliant.
De-identification of Protected Health Information Policy

This Policy is Applicable to:
SYSTEM WIDE
Continuing Care, Corporate, Gerber, Outpatient/Physician Practices, Priority Health, Reed City, SH GR Hospitals, SHMG, United/Kelsey, Zeeland, Big Rapids

Reference #: 65
Version#: 3
Effective Date: 06/13/2014
Functional Area: Information Services, Privacy and Information Security

1. Purpose
   To ensure compliance with federal regulations regarding de-identification of Protected Health Information.

2. Definitions
   The definitions to the following terms used within this document may be found in the Information Services Glossary of Terms Used in Policies and Procedures (v.2):
   - Business Associate
   - De-identified Information
   - Individual
   - Individually Identifiable Health Information
   - Protected Health Information (PHI)

3. Compliance
   Any person in violation of this policy is subject to corrective action, up to and including termination.

4. Policy
   It is the policy of Spectrum Health to de-identify Protected Health Information when appropriate and practical, thus rendering such information not subject to HIPAA Regulations.

A. Uses and Disclosures to Create De-Identified Information
   Spectrum Health may use Protected Health Information to create information that is not Individually Identifiable Health Information, or disclose Protected Health Information only to a Business Associate for such purpose, whether or not the De-identified Information is to be used by Spectrum Health.

B. Uses and Disclosures of De-Identified Information
   Health information that meets the requirements for de-identification hereunder is not considered to be Individually Identifiable Health Information, i.e., it is De-identified Information. The HIPAA Regulations do not apply to De-Identified Information, provided that:
- A code or other means of record identification designed to enable coded or otherwise De-
identified Information to be re-identified cannot be disclosed,

and

- If De-identified Information is re-identified, Spectrum Health may use or disclose such re-
identified information only as permitted or required herein.

C. Requirements for De-Identification of Protected Health Information

Spectrum Health may determine that health information is De-Identified Information only if:

- A person with appropriate knowledge of, and experience with, generally acceptable and
statistical and scientific principles and methods for rendering information not individually
identifiable, determines that the risk is very small that the information could be used alone or
in combination with other reasonably available information, by an anticipated recipient to
identify an individual who is the subject of that information; and documents the methods and
results of the analysis that justify such determination;

or

- All of the following identifiers of the Individual or of relatives, employers, or household
members of the Individual, are removed:
  - Names;
  - All geographic subdivisions smaller than a state, including street address, city, county,
precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip
code if, according to the current publicly available data from the Bureau of the Census:
the geographic unit formed by combining all zip codes with the same three initial digits
contains more than 20,000 people; and the initial three digits of a zip code for all such
geographic units containing 20,000 or fewer people is changed to 000;
  - All elements of dates (except year) for dates directly related to an individual, including
birthday, admission date, discharge date, date of death; and ages over 89 and elements
of dates (including year) indicative of such age, except that such ages and elements may
be aggregated into single category of age 90 or older;
  - Telephone numbers;
  - Fax numbers;
  - Electronic mail addresses;
  - Social security numbers;
  - Medical record numbers;
  - Health plan beneficiaries number;
  - Account numbers;
  - Certificate/license numbers;
  - Vehicle identifiers and serial numbers, including license plate numbers;
  - Device identifiers and serial numbers;
  - Web Universal Resource Locators (URL’s);
  - Internet Protocol (IP address numbers);
SPECTRUM HEALTH

- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images;

and

- Any other unique identifier number, characteristic, or code, except as permitted by the section entitled "Re-Identification" of this policy;

and

- Spectrum Health does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

- Use of patient initials is not a sufficient means of de-identification.

D. Re-Identification

Spectrum Health may assign a code or other means of record to allow De-Identified Information to be re-identified by Spectrum Health, provided that:

- DERIVATION
  The code or other means of record identification is not derived from or related to information about the Individual and is not otherwise capable of being translated so as to identify the Individual;

and

- SECURITY
  Spectrum Health does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

5. Revisions

Original Effective Date: 04/13/2003
Revised Dates: 05/01/2011, 09/23/2013

Spectrum Health reserves the right to alter, amend, modify or eliminate this policy at any time without prior written notice.

6. References

- HIPAA Privacy Regulations 45 CFR §§ 164.502(d) and 164.514(a)-(c)
- Uses and Disclosures of Protected Health Information

7. Authors, Reviewers and Approval

Document Owner:
Lacher, Gary  System Director, Privacy

Writer(s) (formerly Author):
Not Assigned
Reviewer(s):
  Leah Voigt (Senior Counsel)

Approver:
  Patrick J. O'Hare, SVP and Chief Information Officer

8. Keywords:
  hipaa, de-identification, de-identification, phi, authorization, disclose, phi, protected health information, privacy, minimum necessary, uses of phi, authorized disclosures, business associate, de-identified data, re-identified data, individual identifiable health information, sh-hip-priv-017
Electronic Messaging Appropriate Use Policy

This Policy is Applicable to:
SYSTEM WIDE
Continuing Care, Corporate, Gerber, Outpatient/Physician Practices, Priority Health, Reed City, SH GR Hospitals, SHMG, United/Kelsey, Zeeland

Reference #: 55
Version#: 2
Effective Date: 06/16/2014
Functional Areas: Information Services, IS Operations, Privacy and Information Security

1. Purpose
To define policy for the appropriate use of Spectrum Health corporate electronic messaging and communication systems, this policy contains the following sections:
A. Right to Monitor
B. Legal Review of Electronic Messaging and Communications
C. Auditing of Electronic Messaging and Communications
D. General Administrator Responsibilities
E. General Notes on Electronic Messaging and Communication
F. Appropriate Use
G. Inappropriate Use
H. Internal E-mail
I. Message Forwarding
J. Internet (External) E-mail
K. Use of Encryption
L. Out of Office Reply Guidelines
M. E-mail Archiving
N. Internet E-mail Synchronization
O. Exceptions

2. Definitions
The definitions to the following terms used within this document may be found in the Information Services Glossary of Terms Used in Policies and Procedures:
- Business Associate
- Electronic Messaging and Communications
3. Responsibilities

It is the responsibility of all users to report any misuse of electronic messaging and communications by other individuals to their manager, supervisor, Human Resources or the Information Services Helpdesk.

4. Compliance

Any violation of this policy may result in disciplinary action up to and including termination.

5. Policy

Spectrum Health's internal and external electronic messaging and communication systems are intended to be used for business purposes only.

Incidental personal use is permissible as long as it does not consume more than a trivial amount of system resources, does not interfere with worker productivity, and does not preempt any business activity.

All persons granted electronic messaging and communications access by Spectrum Health must abide by the terms of the Spectrum Health Confidentiality Statement, along with the outlined data protection standards and acceptable use guidelines.

A. Right to Monitor

Spectrum Health owns the hardware and/or software that provide electronic messaging and communications, and all messages generated on or handled by Spectrum Health's electronic communications systems are considered to be the property of Spectrum Health (excluding employee owned mobile devices).

While Spectrum Health does not intend to regularly review user's electronic messaging and communications records, users have no right or expectation of privacy in their use of electronic messaging and communications; Spectrum Health permits users to utilize these tools in the performance of their assigned duties.

The content and record of activity regarding Spectrum Health electronic messages are to be treated like shared paper files, with the expectation that any of the information regarding their use is available for review by authorized Spectrum Health representatives.

B. Legal Review of Electronic Messaging and Communications

Spectrum Health reserves the right to disclose all forms of electronic messages, communications, and/or messaging logs to law enforcement, government officials or to other third parties without notification to or permission from the Spectrum Health electronic messaging user sending or receiving messages.

As a condition of initial and continued employment, all staff consents to Spectrum Health's review and disclosure of electronic messages and communications.

C. Auditing of Electronic Messaging and Communications

An audit of electronic messaging content of an individual utilizing Spectrum Health systems is generally acceptable only under the following circumstances; however, exceptions will be made, as deemed necessary, by any of the approved parties referenced below.

- Litigation Hold and Information Discovery Request, ordered by subpoena or other legal action
- Human Resource Issues – Requests must come through approved HR requestor
• Patient Privacy Investigations
• Corporate Compliance Issues and Legal Investigations

The following Spectrum Health roles are approved requestors:

I. Human Resources Generalist, per request of the up-line supervisor (Director or above) of the individual to be audited.

II. System General Counsel.

Information Security shall receive the requests, provide notifications to the appropriate leadership, conduct the reviews and deliver the results to the requestor.

D. General Administrator Responsibilities

To support the healthcare system and/or individual users, there will be situations when Information Services electronic messaging and communications administrators are required to intercept electronic messages, sign-on with someone else’s identity or perform some other type of problem determination that may not comply with the outlined guidelines. This will only take place with the approval of an Information Services Vice President.

In these cases, Information Services personnel are to act responsibly with due care, and be sensitive to any confidential Spectrum Health information.

E. General Notes on Electronic Messaging and Communication

I. Users should exercise caution and good judgment when sending confidential Spectrum Health information through electronic messaging and communication systems.

This includes the encryption of confidential or sensitive information. (See Section K.)

Note: “Confidential information” may be interpreted differently, dependent upon job function; it can range from patient information to personnel records, from financial reports to business strategies, etc.

II. E-mail should be used as a means to exchange non-urgent messages and scheduling information between employees of Spectrum Health, as well as to provide messaging communications to organizations and customers outside of Spectrum Health.

III. In general, e-mail should not be used to replace all other types of communications currently available to Spectrum Health employees, such as personal conversations and meetings, voice mail, faxes and other interpersonal communications that are required in a large organization.

E-mail is not proper for all types of communication, and care should be taken when composing and sending mail to other employees and outside the organization.

IV. Electronic paging and/or texting devices should be used for urgent messages of notification.

Data classified as Protected Health Information, Confidential or Internal should not be transmitted to a paging or texting device without the use of an encryption process approved by the Information Security Department.

F. Appropriate Use

I. Acceptable use of electronic messaging and communications is based on common sense and etiquette, and should be consistent with Spectrum Health’s Core Values and Information Protection policies.
Whenever sending electronic messages, the user’s name must be included in each message, if possible. (Pagers are an example where this may not be possible.)

II. An individual user is responsible for all electronic messages originating from their unique user ID.

III. The user name, electronic messaging address, organizational affiliation and related information included with electronic messages or postings must reflect the actual originator of the messages or postings.

With the exception of hot lines that are intended to be anonymous, workers must not send anonymous electronic communications.

At a minimum, all workers must provide their name and phone number in all electronic communications.

Electronic mail signatures indicating job title, company affiliation, address, and other particulars are strongly recommended and/or must be used when required by corporate or departmental policy for all electronic messages.

IV. Management approval and authorization is required to send messages to large distribution lists such as “SH-Everyone”.

Only a small percentage of e-mail messages should ever be sent to large distribution groups such as the “SH-Everyone” distribution list.

Use of this group to send e-mail is strongly discouraged, and should not be used if at all possible. (Generally speaking, “Everyone” in the organization does not need to know when you go on vacation, or when someone is having a birthday.)

There are alternate ways to communicate information to most of the employees at Spectrum Health that are more effective, and better suited to meet your needs. Contact your supervisor or administrative assistant for alternative ways of reaching your audience, before using the “SH-Everyone” or other large distribution list.

V. Messaging and communications applications must be approved for use by Information Services, and support all corporate, privacy and security, legal and regulatory logging and message archiving requirements.

G. Inappropriate Use

It is the responsibility of all users to report any misuse of electronic messaging and communications by other individuals to their manager, supervisor, Human Resources or the Information Services Helpdesk.

Inappropriate uses include, but are not limited to, the following:

I. Using electronic messaging or communications for commercial purposes (for example, to promote interests of a business other than Spectrum Health) or for partisan political purposes (for example, to promote the candidacy of a candidate for public office).

II. Using electronic messaging or communications for any purpose which violates federal, state, local or regulatory laws.

III. Misrepresenting a user’s identity or affiliation in electronic messaging or communications.

IV. Forwarding sensitive or confidential electronic messages or communication without the sender’s permission, and/or lack of use of encryption, if sent outside the organization (see Section K).
V. Sending harassing, obscene, offensive material and/or other threatening e-mail, or electronic messages to another individual or group.

VI. Posting harassing, obscene, offensive, threatening or confidential information on web site blogs or social networking sites.

VII. Attempting to read, delete, copy, intercept or alter the electronic communications of another user.

VIII. Using someone else's identity and password to gain access to any technology service, including electronic messaging and communications (except as mentioned in Section C).

IX. Misrepresenting, obscuring, suppressing or replacing another user's identity on an electronic communications system.

X. Causing congestion on the network by the propagation of "chain letters" or sending inappropriate messages to distribution lists.

XI. Persistent storing or sending of non-job-related files such as pictures, movies, music, personal finance, jokes, etc.

XII. Spectrum Health staff employing e-mail addresses (such as gmail, yahoo etc.) other than official Spectrum Health approved e-mail addresses, for corporate business matters.

XIII. Spectrum Health staff employing instant messaging (chat) addresses (such as gmail, yahoo etc.) other than official Spectrum Health instant messaging addresses, for corporate business matters.

H. Internal E-mail

I. E-mail is not considered a totally secure application, and the confidentiality of the material sent cannot be guaranteed. For example, e-mail messages can be saved indefinitely by the receiving individual; copies can easily be made and forwarded to others either electronically or on paper.

II. Due care should be used when sending any confidential, sensitive or internal information.

Users are required to exercise good judgment, along with a conscientious understanding of proper e-mail usage and functionality, to prevent the intentional or unintentional receipt of confidential information by unauthorized third parties.

III. Patient identifiable information should never include a patient’s full name, but two patient identifiers must be used with every internal transmission of patient identifiable information.

Acceptable patient information includes initials, medical record number, social security number or any other reference number.

The recommended and best approach in communicating patient sensitive information is to use a more secure method, such as the phone or setting up network directories with restricted access.

IV. Electronic mail containing patient information will not be considered part of the patient’s medical record.

V. Due care should be used when sending e-mail containing peer review information.

VI. Confidential Spectrum Health Information, as well as documents considered to be legal record, are not to be permanently retained in employee e-mail or other forms of electronic messaging and communications.
Multiple services are provided by Spectrum Health for the long-term storage of documents and records. These services include the M: drive, the My Documents folder, SharePoint and Homeweb/InSite.

All records requiring long term storage should be moved from e-mail or other electronic message formats into one of these approved storage locations.

I. **Message Forwarding**

I. Users must exercise caution when forwarding messages.

II. Spectrum Health information, such as "confidential" or "internal," must not be forwarded to any party outside Spectrum Health without the prior approval of a local department manager.

III. Blanket forwarding of messages to parties outside Spectrum Health is prohibited, unless the prior permission of the Information Security Manager has been obtained.

IV. Messages sent by outside parties must not be forwarded to other third-parties, unless the sender clearly intended this, and such forwarding is necessary to accomplish a customary business objective.

In all other cases, forwarding of messages sent by outsiders to other third parties can be done only if the sender expressly agrees to this forwarding.

See Section K for encryption requirements.

J. **Internet (External) E-mail**

E-mail is a widely-used facility on the Internet. When communicating outside of Spectrum Health, users are responsible for adhering to all the internal e-mail guidelines along with the following standards of conduct:

I. The Internet environment is NOT secured or private; users should assume others could read and possibly alter their messages.

II. Confidential or sensitive patient information must not be sent over the Internet under any circumstances, without the use of an approved encryption process. (See Section K.)

III. Forgo downloading attached files from people you do not know; they may contain viruses or other harmful software.

IV. Subscribe to automatic mailing list programs (listservs) selectively, and only those that are business related.

V. Unsubscribe to automatic mailing list programs (listservs) when no longer needed.

VI. When sending potentially controversial communications, representing individual views, and not those of the entire Spectrum Health system, include a disclaimer statement, such as "These opinions are mine and do not necessarily reflect the viewpoint of Spectrum Health."

K. **Use of Encryption**

Many corporate electronic messaging and communications systems are not encrypted by default.

If Protected Health Information or sensitive data classified as "confidential" or "internal" must be sent by electronic communication systems to third parties (such as external recipients on the Internet), an encryption process approved by the Information Security Department must be employed.

Encryption must protect the sensitive information from end-to-end (from sender to recipient).
Mobile computers, personal digital assistants and similar devices (including personal devices) that store or transmit Spectrum Health sensitive information must consistently employ encryption to protect sensitive data when it is stored or transmitted. Stored data on mobile devices includes accompanying data storage media, such as SD memory cards.

Transmission of sensitive data including authentication credentials using wireless technologies (such as Bluetooth wireless) must also be encrypted.

Users of devices who are recipients of sensitive information sent by electronic messaging or communication must delete this information from their systems if they do not have encryption software that can properly protect it.

Separately, workers must not use encryption for any Production electronic communications system, unless a backup key or a key escrow system has been established with the cooperation of the Information Security Department.

L. Out of Office Reply Guidelines

Outlook “Out of Office" messages may be sent to Internet e-mail recipients as well as internal corporate Spectrum Health e-mail recipients. Please keep information in Out of Office reply messages as generic as possible. Do not provide confidential or private information in Outlook Out of Office messages.

I. OUT OF OFFICE GUIDELINES

All Spectrum Health staff, Workforce and Business Associates using Outlook or other electronic messaging systems that are capable of sending automatic Out of Office reply messages must adhere to the following Out of Office reply guidelines.

a. Always keep Out of Office reply information as generic as possible.

b. Never specify that you are going on a vacation or leaving for a holiday.

c. Never include your own, other staff, or patient personal contact details such as home phone, home address, financial or health information.

An example Out of Office reply message follows:

I will be out of the office until [date]. I will have [limited] [no] access to email and voicemail. For urgent issues please contact [name] at [phone number].

Thank You.

M. Retention of E-mail

I. Generally, e-mail messages should be considered temporary communication that may be discarded routinely; however, depending upon the content of the e-mail message or attachments, it may be considered a more formal record and should be retained pursuant to Spectrum Health Administrative policy “Records Management, Retention and Destruction.”

Multiple services are provided by Spectrum Health for the long-term storage of documents and records, such as the M:\ drive, the My Documents folder, SharePoint and Homeweb/InSite.

All records requiring long-term storage should be moved from e-mail into one of these approved storage locations.
II. All e-mail content stored in users “Deleted Items” and “Sent Items” Outlook folders will be purged after 90 days from receipt of the message.

III. All other e-mail content within the user’s mailbox will be purged after seven years from the date of the message.

IV. Messages older than 180 days may be moved to an archive system, requiring the user to be connected to the Spectrum Health Network in order to retrieve.

V. Certain e-mail users may have system archiving enabled, dependent upon their role within the organization.

The archiving system will receive a copy of every message sent or received by the user.

This data will be stored for seven years, and may be audited as necessary pursuant to the terms outlined in this policy.

Users may access the archive to retrieve and view messages previously deleted from their mailbox, however these messages cannot be altered or deleted by the user.

a. Exceptions for retention periods beyond seven years may be made on a case-by-case basis, and must be approved by the Spectrum Health System Vice President, CIO.

b. Any such exceptions will be catalogued in the CIO's office, and will include the basis for the exception.

VI. The size of an outgoing message or attachment shall be limited to 25 megabytes.

Users attempting to send messages or attachments larger than 25 megabytes will receive a warning message, and the message will not be allowed to be sent out.

If there is a valid requirement to send out a large attachment, an alternate means of transmitting data elements greater than 25 megabytes should be chosen, such as HTTPS or Secure FTP.

VII. The maximum allowed inbound attachment size shall be limited to 25 megabytes.

Attempts to receive attachments from external sources, such as the Internet, greater than 25 megabytes will be blocked.

The Spectrum Health intended recipient will receive a notification e-mail explaining the attachment exceeded the size limit.

An alternate means of receiving data elements greater than 25 megabytes should be chosen, such as HTTPS or Secure FTP.

VIII. Each mailbox shall have an initial storage limit of 500 megabytes.

Anyone that reaches this limit will be prohibited from sending messages until more disk space is allocated or messages are deleted from the mailbox.

A warning message will be issued to the user when 400 megabytes is reached.

At this point, the e-mail user needs to free up disk space by deleting old messages.

All users are requested to perform regular deletion of unneeded messages, to maintain system performance.

If additional mailbox space over 500 megabytes is required, a request form for additional mailbox space must be submitted to the Information Services Helpdesk.
Requests for additional storage space will be granted if there is a valid business reason for the request, and the user has "cleaned" the mailbox sufficiently, deleting old messages that are no longer needed, and deleting any personal files from their mailbox.

A cursory review by the e-mail administrator may be made prior to approval being granted.
IX. E-mail backups are maintained for 30 days.

E-mail messages can be restored, if they are within the current backup library, upon request, with a valid business reason.

N. E-mail Archiving

These policy statements apply to users who are integrated into the Spectrum Health e-mail system. Any entity (e.g.: new mergers/acquisitions) who has a separate e-mail system will be unable to participate in e-mail archiving until full integration takes place.

Human Resources, the Office of the General Counsel and other staff in leadership must refer to these policy statements before requesting e-mail archiving for roles that are not automatically granted the functionality.

I. E-MAIL ARCHIVING ACCEPTABLE USE

a. E-mail data files (PSTs) are regularly used for HR investigations, supervisor access of terminated/former staff e-mail and electronic discovery efforts.
   * To prevent loss of sensitive data, PST files are not allowed in the Spectrum Health environment for the purposes of personal archival or e-mail portability.
   * Due to the nature of the files, the storage and use of PST files in unauthorized areas negatively impacts the performance of enterprise systems.
   * PST files will be generated only by IS Information Security and IS Intel Server Engineering teams.
   * PSTs that are identified in unauthorized areas will be removed without notice.

b. E-mail archiving will be centrally and automatically performed using a standard third-party archival solution, selected and implemented by Spectrum Health IS.

Native archiving capabilities within the core messaging system may also be implemented by Spectrum Health IS, independent of a third party archival solution.

c. Retention of e-mail in the archive is subject to the IS Electronic Records Retention and Destruction policy.

d. E-mail archiving is based upon enrollment to the standard e-mail archiving solution, and there should be no expectation of notification enrollment in the e-mail archiving solution.

e. Enrollment is based upon the following criteria:
   * Individuals possessing the title of Director or above will be automatically enrolled.
   * Due to their executive support role, select administrative staff may be enrolled.
   * Other individuals may be enrolled because they regularly handle sensitive e-mail content (i.e. patient information, corporate confidential information, personnel information, etc.).
   * At the discretion of Human Resources, Chief Risk Officer and/or the Chief Legal Officer, any individual may be enrolled in the archiving solution. These divisions will screen and validate appropriate use cases.

f. Access to e-mail for a departed staff member is granted according to the Accessing Terminated Employee Stored Data policy.
II. E-MAIL ARCHIVING RETENTION PERIOD
   a. All e-mail shall be retained for a minimum of seven (7) years.
   b. Exceptions for retention periods beyond seven years may be made on a case-by-case basis, and must be approved by the Spectrum Health System Vice President, CIO.
      Any such exceptions will be catalogued in the CIO's office, and will include the basis for the exception.
   c. Some archiving solutions may not support more than one policy.

III. E-MAIL ARCHIVING STORAGE, AUDIT, AND RETRIEVAL
   a. The archiving system shall provide automatic and immediate archiving of all sent and received messages.
   b. This data may be audited as necessary.
   c. Users may access the archive to retrieve and view messages previously deleted from their mailbox, however these messages cannot be altered or deleted by the user.

O. Internet E-mail Synchronization
   Devices configured to synchronize e-mail or other corporate messaging systems containing sensitive or confidential data must employ encryption for the connection to corporate messaging servers or systems.
   Also see Section K for additional encryption requirements.

I. RPC OVER HTTPS
   Only corporate-owned or managed devices are permitted to use the “RPC over HTTPS” Outlook synchronization method.

II. MOBILE DEVICE SYNCHRONIZATION
   Corporate and personal handheld mobile devices such as PDAs, Smartphones and Blackberrys may synchronize corporate e-mail, providing encryption is used as outlined in Section K – Use of Encryption.

P. Exceptions
   Unless otherwise noted, all exceptions to this policy must be approved by the Spectrum Health System Information Security department.
   Any such exceptions will be catalogued by the Information Security department.

6. Revisions
   Original Effective Date: 02/01/2000
   Revised Date: 02/23/2010, 09/24/2012

Spectrum Health reserves the right to alter, amend, modify or eliminate this policy at any time without prior written notice.

7. References
   • HIPAA Regulations 45 CFR § 164.312(b)
8. Authors, Reviewers and Approval

Document Owner:
Melscn, Paul

Writer(s) (formerly Author):
Jeremy Jordan (Architect, Sr)
Darrin Wassom, Architect, IS Security, Risk & Comp, 07/18/2012

Reviewer(s):
Brett Hoffman (Mgr, Information Security)
Darrin Wassom, Architect, IS Security, Risk & Comp, 07/18/2012
Larry Whiteside, Director, IS Security, Risk & Comp, 09/24/2012

Approver:
Richard C. Breon, President and Chief Executive Officer

9. Keywords:
electronic messaging, email, e-mail, instant message, im, communicate, message, encryption, out of office guidelines, administration of electronic messaging, legal review of messages, appropriate use of electronic messaging, inappropriate use of electronic messaging, ooo assistant, outlook, messenger, webex connect, webex, business associate, workforce, monitor transmissions, system, network, distribution list, forwarding messages, obscene, threaten, harrass, offensive, offend, confidential information, hipaa, privacy, security, tis-cta-d0051