Beaumont HEALTH

Title	Location	Functional Area
Electronic Communication Standard	**ALL Beaumont Health**	**End User Computing**
Policy Owner	Document Type	Effective Date
Director Corp Information Services	**Policy**	**02/09/2016**

I. CORPORATE AUTHORITY

Beaumont Health ("BH") as the corporate parent to William Beaumont Hospital, Botsford General Hospital, and Oakwood Healthcare Inc., ("Subsidiary Hospitals") establishes the standards for all policies related to the clinical, administrative and financial operations of the Subsidiary Hospitals. The Subsidiary Hospitals, which hold all health facility and agency licenses according to Michigan law, are the covered entities and the providers of health care services under the corporate direction of BH. The Subsidiary Hospitals' workforces are collectively designated as BH workforce throughout BH policies.

II. PURPOSE AND OBJECTIVE:

The purpose of the Beaumont Health (Beaumont) Electronic Communication Standard is to establish the security and control requirements for proper use of eCommunication Tools and management of information within eCommunications.

All eCommunication resources are provided for business purposes. Within this standard, eCommunications include, but are not limited to, electronic mail, instant messaging, online chat, voice recording, video conference recording and mobile communications.

Beaumont information is a critical company asset and must be protected. This Standard outlines the requirements to provide assurance that the confidentiality, integrity and availability of Beaumont Information contained in Beaumont eCommunications is maintained and that employees and users utilize eCommunication tools in accordance with Beaumont standards and applicable laws and regulations.

Please Note: The Beaumont Information Security Policy and Acceptable Use Policy are referenced in this document; it is important to be familiar with these policies. Other policies may also be referenced within this standard.

III. POLICY STATEMENT:

This Standard is applicable to Beaumont workforce members and all eCommunications related to the business of Beaumont which are created, acquired, or managed during the normal course of business by, or on behalf of, Beaumont. This Standard also applies to eCommunications produced from information systems (application or infrastructure) that may be located within the Beaumont computing environment or hosted for Beaumont by a third party. eCommunications generated through purchased services and suppliers on behalf of Beaumont must also conform to this Standard.

IV. DEFINITIONS:

A. **Archives:** Archived information is stored for the purpose of retrieving specific information through the use of selection criteria in the normal course of business.

Beaumont HEALTH

Title	Location	Functional Area
Electronic Communication Standard	**ALL Beaumont Health**	**End User Computing**
Policy Owner	Document Type	Effective Date
Director Corp Information Services	**Policy**	**02/09/2016**

B. **Availability:** The assurance that information and information systems are accessible to the business when they are required.
C. **Backup:** A back-up is used solely for the restoration of a repository to its state at a given date/time in the event of a disaster or to support business continuity.
D. **BCC:** Blind Carbon Copy is a feature of email that does not display the email addresses to the recipient.
E. **Beaumont Information:** Beaumont Information includes all information in any form, including personal information, which is related to the business of Beaumont and is created, acquired, or managed during the normal course of business by, or on behalf of, Beaumont.
F. **Confidentiality:** The protection of Beaumont information from unauthorized disclosure.
G. **Electronic Communication (eCommunication):** Any message conveying Beaumont Information via electronic means that includes, but is not limited to, electronic mail, instant messaging, online chat, voice recording, video conferencing, mobile communication and internal social media.
H. **Electronic Communication Tools:** Any method used to convey Beaumont Information that is transmitted via electronic means that includes, but is not limited to, electronic mail, instant messaging, online chat, voice recording, video conferencing, mobile communication and internal social media.
I. **Electronic Mail (email):** A method of transmitting text messages and files digitally over communication links.
J. **Externally-Facing Application/Website:** Applications and websites that are accessed by external users (general public) including both internally and externally hosted applications.
K. **Information Owner:** The individual whose business is supported by the information. The Information Owner is accountable for the application of appropriate information classifications, determining appropriate access restrictions, and ensuring appropriate controls are used throughout the information's lifecycle.
L. **Instant Messaging (IM):** A form of real-time communication between two or more people based on typed text that is digitally transmitted over a communication link.
M. **Integrity:** The assurance that information is accurate and has not been improperly modified either intentionally or unintentionally.
N. **Internal Web Site:** The Beaumont-owned or controlled web sites that reside behind the Beaumont firewall or hosted by Beaumont authorized service providers. They are private web sites and are fortified from the outside world. Only authorized users can access an internal web site.
O. **Mobile Communication:** Communication using electronic mobile devices that include, but are not limited to, phone, SMS (text) messaging and email.
P. **Presentation Recording:** A system or method for recording and exporting slide show presentations or video presentations.
Q. **Systems:** For the purpose of this publication, systems are any application or infrastructure component with email capability.

Beaumont HEALTH

Title	Location	Functional Area
Electronic Communication Standard	**ALL Beaumont Health**	**End User Computing**
Policy Owner	Document Type	Effective Date
Director Corp Information Services	**Policy**	**02/09/2016**

R. **Users:** Users of Beaumont eCommunication are employees, contractors, and other members of the workforce supporting Beaumont who are authorized to access and use Beaumont eCommunications.
S. **Video Conferencing:** Remote conferencing to one or more specific site with the ability to send and receive both live visual and audio.
T. **Voice Recording:** An electrical or mechanical inscription and re-creation of sound waves, such as the spoken voice, audio conference, etc.

V. ROLES AND RESPONSIBILITIES:

A. **Users of Electronic Communications**
1. Comply with all requirements in this Standard to protect Beaumont eCommunications created, used, or acquired during the normal course of business.
2. Abide by all applicable laws and regulations pertaining to Beaumont eCommunications.

B. **Departments**
1. Work with departmental staff to ensure they are aware of, and adhere to, the requirements in this Standard.
2. Educate staff to only include confidential information in electronic communications when necessary and to properly secure those electronic communications.

C. **IT Management**
1. Assist departments in selecting and implementing eCommunications tools that meet business needs and also comply with this Standard and the requirements in the Beaumont Information Security Policy.
2. Establish operational procedures to manage eCommunication tools and protect Beaumont Information contained within the eCommunications to ensure their confidentiality, integrity and availability.

VI. REQUIREMENTS:

A. **Electronic Mail**
1. Acceptable Use
   a. Professional and appropriate language must be used in all electronic mail messages. Users are prohibited from sending abusive, harassing, threatening, menacing, discriminatory, pornographic, disrespectful, or otherwise offensive electronic mail messages.
2. Account Management
   a. All Beaumont email accounts and distribution lists must have a Beaumont manager sponsor. By default, a department manager is the sponsor of the departmental staff's email accounts.
   b. Users must not share their passwords used to access Beaumont email accounts.
   c. Group mailbox accounts:
      i. Group mailbox accounts must be approved by a Beaumont Manager sponsor or an authorized delegate.

Beaumont HEALTH

Title	Location	Functional Area
Electronic Communication Standard	**ALL Beaumont Health**	**End User Computing**
Policy Owner	Document Type	Effective Date
Director Corp Information Services	**Policy**	**02/09/2016**

ii. Under normal circumstances, individuals with access to send on behalf of the group mailbox should be given delegate access so recipients can identify the individual who sent the message (i.e., it will show "John Doe on behalf of Information Security"). For group mailbox accounts which intentionally mask the original sender of the message, the Beaumont Manager sponsor of the mailbox is accountable for any and all communications that originate from that mailbox.
iii. The sponsor or authorized delegate of the sponsor must conduct access reviews of the group mailbox account at a minimum of every 6 months and have access removed for anyone who is no longer authorized to use the account.

d. The user name, email address, company affiliation and related information included within an email message must reflect the actual sender or group mailbox the message originated from.
e. All email sent from a Beaumont email account must use a valid company email address in the message 'From' field. A valid email address consists of a Beaumont workforce member name or group mailbox name and a Beaumont hosted domain name (e.g., information.security@beaumont.org). The use of disguised, misrepresented or spoofed email addresses is strictly prohibited.
f. HR approval is required to provide an individual access to another individual's email account who is still a member of the Beaumont workforce (e.g. an individual takes a temporary leave of absence). Confidential investigations requiring access to an individual's mailbox requires approval from all of the following:
   i. HR
   ii. Legal Affairs
   iii. An Executive Vice President who is overseeing an internal investigation
g. With the exception of group mailbox accounts, no individual must access, read or send email from another Beaumont email account, except under approved conditions and only when delegate access is provided.

3. Creation and Transmission
   a. Systems hosted or located outside the Beaumont email infrastructure must not use a Beaumont-hosted domain email address as the sender (i.e., the message 'From' field must not use a Beaumont-hosted domain name such as @beaumont.edu). If email is sent on behalf of Beaumont, it must indicate that the message being sent is from Beaumont and must have valid MX and SPF records according to Beaumont messaging guidelines.
   b. All email messages created, stored or transmitted on Beaumont email systems are the property of Beaumont, whether originating from internal or external email systems, and may be deleted or disclosed to others by Beaumont at any time without prior notice in accordance with Beaumont policy or as required by law or regulation.
   c. When forwarding email, altering the content to change the intention of the originator is strictly prohibited. If content is altered to remove some information, it must be clearly indicated in the new message.

Beaumont HEALTH

Title	Location	Functional Area
Electronic Communication Standard	**ALL Beaumont Health**	**End User Computing**
Policy Owner	Document Type	Effective Date
Director Corp Information Services	**Policy**	**02/09/2016**

d. Email sent from the Beaumont network or from a Beaumont computing device must use the Beaumont email infrastructure.
e. Users must not use personal email accounts for Beaumont business or for transmitting or receiving Beaumont Information.
f. A Beaumont workforce member must never ask patients to send PHI or credit/debit card data to Beaumont using unsecured email.
g. Email messages sent to, or received from outside parties should not contain protected health information (PHI), credit/debit card data or other confidential Beaumont information. If a business need exists to do so, those emails must be transmitted via Beaumont-approved secure email mechanisms.
h. The following legal disclaimer must accompany all secure email containing PHI transmitted outside of Beaumont:
i. "This Internet message along with any documents, files or attachments may contain information that is legally privileged, confidential and/or proprietary and protected from disclosure unless authorized by the sender. The message is intended for use only by the person to whom it is addressed. If you are not the intended addressee, please immediately notify the sender and delete the message. The sender takes no responsibility for: any alterations to the electronic message, documents, files or attachments which may occur due to software or printer variations at the addressee's location, or unauthorized access across the Internet."
j. When accessing Outlook Web Access (OWA) from non-Beaumont devices, users must not save Beaumont Information to that non-Beaumont device.
k. Automatically forwarding Beaumont email to a non-Beaumont mailbox (e.g., your personal email account or the account of a contract individual from another company) is prohibited.
l. Any email being distributed to more than 50 individuals must put the list of addresses in the BCC field and must clearly indicate in the email the description to whom the email is being distributed.
m. Beaumont Information Technology Directors, or a specifically authorized delegate of Information Technology, must authorize and approve any IT internal email to be distributed to more than 100 individual recipients. Such emails must conform to established IT communication standards.
n. Beaumont Corporate Communications, or a specifically authorized delegate of Corporate Communications, must authorize and approve any internal email to be distributed to more than 250 individual recipients.
o. Technical support personnel must not access an individual's electronic mailbox without approval from the account owner, Human Resources, Legal Affairs and an Executive Vice President who is overseeing an internal investigation. An exception exists if the Information Security Officer or Corporate Communications authorizes the removal of specific email messages based upon a threat or business need.

4. Retention and Storage

Beaumont HEALTH

Title	Location	Functional Area
Electronic Communication Standard	**ALL Beaumont Health**	**End User Computing**
Policy Owner	Document Type	Effective Date
Director Corp Information Services	**Policy**	**02/09/2016**

a. Beaumont email systems are tools to facilitate communication, and are not for the long-term retention and storage of Beaumont Records. Users must manage email containing Beaumont Information that is an official record, according to the relevant record retention guidelines and record retention policy. Official records must be maintained in an appropriate and approved repository (e.g., shared drive) and not in an email mailbox. All other email must be deleted when it no longer supports ongoing business operations.
b. Workforce members accessing Outlook email from the desktop:
   i. Email messages will be retained for a maximum of 1 year.
   ii. After 90 days email will be moved to the archive.
   iii. Email older than 1 year must be purged.
   iv. Any email in the deleted items folder of a mailbox will automatically be purged after 30 days.
   v. Voicemail messages delivered to a mailbox will automatically be purged after 30 days.
c. For workforce members who can only use web browser-based mailboxes (Outlook Web Access), email will be purged after 90 days.
d. Email system Backups are for disaster recovery purposes only and are not retained for email discovery purposes. Backups from Beaumont mail servers must be managed accordingly.
e. Beaumont must dispose of the email on backup media according to the Beaumont Information Disposal Security Standard.
f. Upon termination of employment or contract with Beaumont, if individuals held a vice president or higher position with Beaumont, their email must be retained for review for 12 months. If individuals held a position below the vice president level, their email must be retained for review for 3 months. After the 3 month or 12 month review and retention period, the mailbox must be purged and removed from Beaumont systems. At all times, litigation holds supersede any company retention policies.
g. Upon notice from Legal Affairs, Treasury Administration or Human Resources, users' email accounts can be held for longer periods of time. Legal Affairs, Treasury Administration and HR must release email account holds upon the satisfaction of the purposes for which these departments issued the hold.

5. Termination of an individual's working relationship with Beaumont:
   a. An out of office message must be set on the individual's account indicating the individual is no longer with Beaumont and directing responses to the individual's manager/sponsor unless they have indicated otherwise in advance.
   b. The individual must be removed from the corporate address book within seven days.
   c. Managers are authorized to review the email of former workforce members for which they were responsible to determine if information must be retained for records

Beaumont HEALTH

Title	Location	Functional Area
Electronic Communication Standard	**ALL Beaumont Health**	**End User Computing**
Policy Owner	Document Type	Effective Date
Director Corp Information Services	**Policy**	**02/09/2016**

retention purposes. The review must be completed within the prescribed interval indicated in section, VI.A.4.f.

d. At no time is an email message allowed to be sent under a terminated account owner's name by another individual unless delegate authority is in place, i.e. emails must show "from (sender) on behalf of (original account owner)".

6. Securing Email (Using Encryption)
   a. Email messages sent to, or received from, outside parties should not contain Protected Health Information (PHI), credit/debit card data or other confidential Beaumont information. If a business need exists to do so, those emails must be transmitted via Beaumont-approved secure email mechanisms.
   b. Management discretion must be used when sending Beaumont proprietary information externally to ensure the exposure of that information would not cause negative consequences to Beaumont business activities or strategic initiatives.
   c. When email messages containing Protected Health Information (PHI), credit/debit card data or other confidential Beaumont information are sent within Beaumont (i.e. from a Beaumont email account to another Beaumont email account);no special sending actions are required as these are already secure.
   d. Printers, copiers and other multi-function devices with the capability to send email must have capabilities to send messages secure if they are configured with the ability to send email outside Beaumont.
7. Malware and Security Alerts
   a. Beaumont must scan all email that enters or leaves the Beaumont networks for malware (viruses, spam, worms, etc.), including email sent from applications or other systems.
   b. Beaumont must take proactive steps to prevent viruses from entering Beaumont systems. At a minimum, individuals must not open unexpected file attachments, or attachments from unknown or untrusted sources until the sender validates the attachment through telephone or via a separate email.
   c. Users must promptly report all suspected viruses or other malware to Information Security, at information.security@beaumont.org.
   d. Beaumont Information Technology and Corporate Communications are the only organizational units authorized to email information about security alerts and determine the appropriate action in response to such notices. Users must not propagate or forward any virus or malware notification emails that do not originate from Beaumont Information Technology or Corporate Communications.
8. Application and Infrastructure Email

Beaumont HEALTH

Title	Location	Functional Area
Electronic Communication Standard	**ALL Beaumont Health**	**End User Computing**
Policy Owner	Document Type	Effective Date
Director Corp Information Services	**Policy**	**02/09/2016**

a. All systems that send or receive email must use Beaumont-approved domains and must be approved by the Beaumont Unified Communications Team. The Beaumont email infrastructure must not process email from unauthorized systems.
b. Systems that reside within the Beaumont networks must use the Beaumont email infrastructure to send and receive email. All exceptions must be approved by Information Security and the Unified Communications Team.
c. Email is not an acceptable mechanism for the purposes of business application file or data transfer where high availability or confidentiality is required. If email is used for file transfer, compensating controls must ensure that the data is accurate and protected in transport.
d. System email IDs and their associated passwords used to send and/or receive email must follow the requirements in the Beaumont Identity and Access Management Standard.
e. If emailing from a multifunctional device, the user must authenticate and the 'From' field must auto-fill the user name.
f. Multifunctional devices with email capabilities must use the Beaumont email infrastructure to send email.
g. Systems must have the ability, or an associated process, to manage replies to email messages sent out from these systems. For example, returned messages must have a valid mailbox that receives these messages.
h. Complete accountability is required for system-generated email (i.e., all email must be traceable to the originating system).
i. System Owners or designated delegates must monitor for email and mailbox issues and address them in a timely manner.
j. System Owners must approve all predefined email contents prior to use. Where email content is created in real time, the owner must ensure that the content of these messages complies with Beaumont policies.
k. For any bulk email sent outside the Beaumont environment, Corporate Communications review and approval is required; Corporate Communications will review with Legal Affairs as necessary.
    i. Where required by legislation, all bulk email sent outside the Beaumont network must contain a statement or instruction that gives recipients the option to unsubscribe from the distribution list.
    ii. When an unsubscribe request is received the request must be completed as soon as practical or in line with local legislation, whichever is sooner.

Beaumont HEALTH

Title	Location	Functional Area
Electronic Communication Standard	**ALL Beaumont Health**	**End User Computing**
Policy Owner	Document Type	Effective Date
Director Corp Information Services	**Policy**	**02/09/2016**

l. Unsubscribe instructions are not required for mandatory/compulsory internal email where receipt and review of the content by recipients is necessary and required. Such email includes, but is not limited to: email sent by the Corporate Communications Department, all employee and all personnel bulletins and announcements, executive communications, etc.

B. **Instant Messaging (IM) and Paging**

1. Acceptable Use
   a. The only Beaumont-approved instant messaging system in use is Microsoft Skype for Business (previously known as Lync) and is approved for Beaumont internal use only. Individuals are prohibited from downloading and using unauthorized IM software (e.g., AOL Instant Messenger, Yahoo!, or MSN) within the Beaumont computing environment.
   b. Professional and appropriate language must be used in all instant messages and pages. Users are prohibited from sending abusive, harassing, threatening, menacing, discriminatory, pornographic, disrespectful, or otherwise offensive messages.
   c. Users must not publish another individual's message(s) unless authorized by the originating sender.
   d. Users must not use paging for sending messages containing PHI or sensitive information.
   e. Users are prohibited from using IM or paging for transmitting or storing credit card data.
2. Account Management
   a. All Users IM accounts must be authorized and accountability is required. Beaumont issued IDs must be used to identify individual accounts and users must not use another individual's account for exchange of messages.
3. System Configuration
   a. Beaumont must not configure the IM system to transmit messages between Beaumont's network and any external information systems. Any exceptions must be reviewed by Beaumont Information Security and the Beaumont network team, and then reviewed by the Information Access, Privacy and Security Committee.
4. Retention and Storage
   a. Instant Messages are not official records and must not be treated as such.
   b. Instant messages are intended to be transient. As such, the storage and retention of instant messages is prohibited.

C. **Voice Recording and Voice Mail**

Beaumont HEALTH

Title	Location	Functional Area
Electronic Communication Standard	**ALL Beaumont Health**	**End User Computing**
Policy Owner	Document Type	Effective Date
Director Corp Information Services	**Policy**	**02/09/2016**

1. Voice Recordings created to communicate official Beaumont business must be managed in compliance with the relevant record retention policy and record retention guidelines.
2. Any voice recordings containing credit card payment information must be encrypted and cannot be stored longer than 18 months from the transaction.
3. Any processes where voice recordings are made must adhere to all applicable laws and regulations.

D. **Video Conference Recording**

1. Video conferencing must not be recorded without the permission of Senior Management (i.e., Vice President and above).
2. Recorded video conferences must be managed consistent with the classification of information discussed or presented during the video conference and in compliance with applicable law.
3. Recorded video conferences created to communicate official Beaumont Business must be managed in compliance with the relevant record retention policy and record retention guidelines. All other recorded video conferences must be deleted when they no longer support ongoing business operations.

E. **Mobile Communication**

1. The use of Beaumont-issued mobile devices and personal mobile devices accessing Beaumont information must be in compliance with the Beaumont Mobile Device Security Standard.
2. Mobile communications are transient; Beaumont must not log them or treat them as records. Communication carriers may log and retain these messages for quality control and disaster recovery purposes in accordance with their policies.

F. **Beaumont Internal Website**

1. Internal web site owners must verify that the contents of their sites adhere to all Beaumont policies.
2. Beaumont internal web sites are not official information repositories. All content displayed on a Beaumont internal Web site is considered unofficial and is not subject to any relevant record retention guidelines.
3. Individual Web site owners must approve site content before it is published.
4. Information that is PHI or sensitive which is posted on any internal Web site must restrict access to authorized individuals only.
5. When hyperlinks to a non-Beaumont-controlled web site(s) are used, it must be clear to users that they are leaving a Beaumont internal Web site. The links to the non-Beaumont-controlled site(s) must be reviewed at least annually to ensure they are accurate and still appropriate.

Beaumont HEALTH

Title	Location	Functional Area
Electronic Communication Standard	**ALL Beaumont Health**	**End User Computing**
Policy Owner	Document Type	Effective Date
Director Corp Information Services	**Policy**	**02/09/2016**

G. **Externally-Facing Website**

1. Externally-facing website owners must verify the content of their site adheres to good business practice and complies with Beaumont policies and applicable laws and regulations. Marketing must approve the information published on Externally-Facing Web sites that are managed by or on behalf of Beaumont, and seek guidance as needed from Legal Affairs regarding compliance with applicable laws and regulations. The information owner must periodically review the published contents, including external links, for appropriateness and must determine and document the review cycle based on their business requirements.
2. Information owners must manage content containing Beaumont Information that is an official record according to the relevant record retention policy and record retention guidelines. All other content must be deleted when it no longer supports ongoing business operations.
3. Externally-facing websites must display any relevant Beaumont-approved security, privacy and terms of use statements. The site owner must obtain approvals from Legal Affairs and Corporate Compliance for the appropriate jurisdiction to ensure that all necessary security and privacy disclaimers are displayed, clearly stated, and updated as required.
4. Websites that collect personally identifiable information such as name, address, and e-mail IDs must comply with all applicable laws and regulations.
5. Personally identifiable information, or PHI collected via an externally-facing website, must be protected in transmission and storage using Beaumont-approved encryption methods.
6. Externally-facing websites that display, offer or sell Beaumont products or services must encrypt consumer account information (e.g. PHI, bank account, credit card number, debit card number, etc.) in transmission and storage using Beaumont-approved encryption methods.

VII. REFERENCES:

A. Information Security Policy
B. Identity and Access Management Standard
C. Mobile Device Security Standard
D. Information Disposal Security Standard

VIII. DOCUMENT CHANGE CONTROL:

A. **Revision History**

Beaumont HEALTH

Title	Location	Functional Area
Electronic Communication Standard	**ALL Beaumont Health**	**End User Computing**
Policy Owner	Document Type	Effective Date
Director Corp Information Services	**Policy**	**02/09/2016**

Version #	Date	Revision Author(s)	Summary of Major Changes Made
3.0	03-FEB-2016	Jim Fisher	Corrected reference in section VI.A.5.c.
2.0	02-FEB-2016	Jim Fisher	Differentiated retention requirements between full client and web access users.
1.0	28-SEP-2015	Jim Fisher, Doug Copley	Creation of Beaumont Health Standard