Beaumont HEALTH

Title	Location	Functional Area
Acceptable Use Policy	**ALL Beaumont Health**	**Administration**
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 this Acceptable Use Policy (Policy) is to outline the requirements for proper management of computing and information assets for Beaumont Health (Beaumont). This Policy is intended to align with the Information Security Policy and the Confidentiality & Computer Systems Usage Agreement.

This Policy is applicable across Beaumont and applies to all individuals who use or manage Beaumont computing or information assets, including, but not limited to, physical assets, such as equipment and supplies, information, and information technology.

III. POLICY STATEMENT:

Beaumont information is one of Beaumont's most important assets and must be properly protected. Beaumont information includes all information in any form, 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. Beaumont information may exist in many forms including, but not limited to, paper, microfilm, electronic storage media, photograph, video and voice.

Beaumont computing assets are vital to the operation of Beaumont and must be properly protected. Beaumont computing assets include any and all technology assets used in support of Beaumont operations including, but not limited to, servers, PCs, removable media, cellular and desktop telephones, smart phones, fax machines and printers. Users have a critically important role to ensure that Beaumont computing and information assets are protected.

IV. DEFINITIONS:

A. **Availability:** Assurance that information and information systems required by the business are accessible when necessary.

B. **Beaumont Computing Asset:** Beaumont computing assets include any and all technology assets used in support of Beaumont operations including, but not limited to, servers, applications, networks, telecommunications devices, PCs, smart phones, tablets, removable media, cellular and desktop telephones, fax machines and printers.

Beaumont HEALTH

Title	Location	Functional Area
Acceptable Use Policy	**ALL Beaumont Health**	**Administration**
Policy Owner	Document Type	Effective Date
Director Corp Information Services	**Policy**	**02/09/2016**

C. **Beaumont Information:** Beaumont information includes all information in any form, 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.
D. **Card Validation Code or Value (CVC):** The CVC is either a data element on the card's magnetic stripe used to cryptographically protect the information on the stripe or the three or four digit number printed on the back or front of the card used to validate physical possession of the card during transactions.
E. **Confidentiality:** The protection of Beaumont information from unauthorized disclosure based on the premise of least privilege, or "need-to-know." Beaumont employees, contractors and Beaumont third parties, with a need for access to Beaumont information, must only be given that amount of access needed to complete their required job function or assignment.
F. **Credit Card Service Code:** Three-or four-digit number on the magnetic-stripe that specifies acceptance requirements and limitations for a magnetic-stripe read transaction.
G. **Encryption:** The process of taking a plain text message, applying cryptographic techniques to it (a mathematical algorithm with a key), and producing a message which can only be understood by a person or system with the appropriate decryption key.
H. **Information System (System):** The computer systems and information resources used by an organization to support its business operations.
I. **Integrity:** The protection of information from unauthorized use and modification that could cause harm to Beaumont, its patients or business partners. Integrity provides assurance to the accuracy, reliability, and completeness of Beaumont information.
J. **Least Privilege (need-to-know):** A control principle that requires that an individual or entity (user, computer processes, etc.) be given only sufficient access or authority to complete the required job function or task.
K. **Official Record:** Records are documentation of business decisions, transactions, policies, operations or other official business. The Official Record is the designated copy that must be retained for the time period required in the Beaumont Records Retention Schedule.
L. **Protected Health Information (PHI):** PHI is any information, in any form, that is created or received by a health care provider that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual. In addition, a patient's social security number will also be managed as PHI and will only be obtained, used, or disclosed as necessary to achieve treatment, payment or health care operations.
M. **Users:** Users of Beaumont information and computing assets are employees, contractors, and other representatives supporting Beaumont who are authorized to access and use Beaumont Information.

V. STANDARDS, PRACTICES AND PROCEDURES:

A. **Applicable Laws and Regulations**

Beaumont HEALTH

Title	Location	Functional Area
Acceptable Use Policy	**ALL Beaumont Health**	**Administration**
Policy Owner	Document Type	Effective Date
Director Corp Information Services	**Policy**	**02/09/2016**

1. This Policy, including all risk standards described herein, is intended to be consistent with all applicable legal and regulatory requirements regarding their subject matter, including:
   a. The Health Insurance Portability & Accountability Act (HIPAA) of 1996
   b. The Health Information Technology for Economic and Clinical Health (HITECH) Act, passed as part of American Recovery and Reinvestment Act of 2009 (ARRA)
   c. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act, dated January 25, 2013
   d. State of Michigan IDENTITY THEFT PROTECTION Act 452 of 2004 MCL 445.63(o)
   e. Payment Card Industry Data Security Standard (PCI DSS)
   f. Federal Trade Commission's Identity Theft Prevention Red Flags Rule (16 CFR § 681.2)

B. **Management of Beaumont Information Assets**

Beaumont Information used to support Beaumont business must be properly protected to ensure its confidentiality, integrity and availability. Beaumont Information stored on any medium including paper, film and electronic media must be managed and protected according to Beaumont policies.

1. **Ownership and Monitoring**
   a. All Beaumont information is the property of Beaumont. It must not be disclosed outside Beaumont without approval from the leadership responsible for the Beaumont information.
   b. All electronic communications transmitted via Beaumont's systems (including, but not limited to, telephone, e-mail, voice mail and instant messages) are Beaumont property.
2. **Information Handling**
   a. Beaumont information must be handled and protected consistent with its sensitivity. Where encryption is required, Beaumont-approved methods must be used. The Beaumont information owner at all times remains accountable for the Beaumont information and its protection.
   b. Users must make all reasonable efforts to store Beaumont information on a secured server, where access is controlled and based on least privilege (e.g. SharePoint or network drives).
3. **Publicly Accessing or Discussing Beaumont Information**
   a. Users must not access non-Public Beaumont information in public places where there is risk it could be viewed by unauthorized individuals.
   b. Users must not discuss non-Public Beaumont information in public places where unauthorized individuals could overhear conversations.
4. **Protection of Cardholder Data**

Beaumont HEALTH

Title	Location	Functional Area
Acceptable Use Policy	**ALL Beaumont Health**	**Administration**
Policy Owner	Document Type	Effective Date
Director Corp Information Services	**Policy**	**02/09/2016**

a. Cardholder data (i.e. credit/debit card numbers, expiration dates and/or CVV codes and PINs) must not be copied, moved or stored onto local/shared hard drives, removable electronic media devices, or unsecured physical file folders or cabinets. CVV codes must never be stored in any manner. Refer to the Treasury Policies for additional requirements regarding credit card processing.

5. **Protection of Printed Information**
   a. To the extent practical, Beaumont information must not be left unattended on desks, file cabinets, in meeting rooms or other place where unauthorized individuals may have access to it.
   b. In locked offices, Beaumont information must not be left out where those passing by could view the information from outside the office.
   c. Faxes containing confidential information must be attended by the receiving individual so the information is not exposed to others.
6. **Removing Access Privileges**
   a. Upon separation from employment or transfer to another position, all access privileges must be reviewed and adjusted to maintain only the authorization required for the position. Management must promptly complete the appropriate transfer or separation checklist when individuals leave the system or transfer to another department.
7. **Reporting Incidents**
   a. If any printed or electronic Beaumont information may have been disclosed to unauthorized individuals (such as a report left in a public place, a stolen laptop or smart phone, a fax containing PHI sent to the wrong destination, etc.), management and Information Security must be notified immediately.

C. **Management of Beaumont Computing Assets**

1. **Privacy and Monitoring**
   a. Users should have no expectation of privacy concerning their use of Beaumont's computing and information assets, including email, Beaumont-provided technology or office equipment, telephones, voicemail, the Beaumont intranet, Beaumont-provided access to the public Internet, or other Beaumont information systems, except where applicable law provides differently.
   b. Beaumont has the right to review, audit, and monitor all use of Beaumont computing and information assets, in accordance with Beaumont internal policies and applicable law, and any identified user non-compliance may result in possible action by Beaumont as outlined in section Policy Monitoring and Maintenance below.
   c. Beaumont may use data collected through review and monitoring of Beaumont computing and information assets in accordance with applicable law for a variety of personnel, administrative, employee, work and general management purposes.
   d. These purposes include:
      i. To maintain the security and proper operation of Beaumont networks and systems.

Beaumont HEALTH

Title	Location	Functional Area
Acceptable Use Policy	**ALL Beaumont Health**	**Administration**
Policy Owner	Document Type	Effective Date
Director Corp Information Services	**Policy**	**02/09/2016**

ii. To protect the confidentiality and integrity of Beaumont data.
iii. To maintain a safe and secure workplace Beaumont may transfer this data to Beaumont databases located worldwide. Where such transfer occurs, appropriate technical and organizational security measures must be in place to adequately protect the data in accordance with the applicable laws.

e. A certain amount of personal use of e-mail and the Internet is permitted. Users should mark any such e-mail correspondence as 'Private' or 'Personal', and file the correspondence in their mailbox in files labeled accordingly. However, as far as permitted by applicable law, Beaumont reserves the right to monitor any correspondence transacted via Beaumont computer and information assets in relation to the purposes outlined above. In some jurisdictions, Beaumont may only access a user's private e-mails for legitimate purposes, in the user's presence or having duly requested user presence.

f. In situations where PHI may be collected, used, shared, or transferred, users must comply with the Compliance with Federal and State Privacy Laws and Regulations and applicable local laws.

2. **Acquisition and Approval**
   a. All information systems must have approval from the Executive Vice President and Chief Transformation and Information Officer or their delegate(s) before introducing them into the Beaumont environment.
   b. Computing hardware and software must be procured according to the Beaumont purchasing processes. Computing hardware and software must meet Beaumont standards, or have an approved exception prior to acquisition and implementation.
   c. Where provided by Beaumont and where legally permissible, tools that encrypt the entire contents of electronic storage media (e.g. hard drives) on laptop computers and removable electronic media must be implemented.
   d. Where approved exceptions to Beaumont software standards exist, Beaumont reserves the right to request proof of compliance to the vendor's licensing requirements.
   e. Software and other forms of intellectual property must not be copied for personal use or used in violation of license agreements.
3. **Business Use**
   a. As outlined in the Confidentiality & Computer Systems Usage Agreement, Beaumont computing and information assets are provided for legitimate business purposes.
   b. Occasionally, limited personal use of Beaumont computing or information assets is permitted if it is reasonable, ethical, does not interfere with work responsibilities, and does not conflict with local management directives. Incidental personal use is not permitted in any patient care or publicly accessible area under any circumstances.
   c. Abuse of long distance and international telephone calls is prohibited. Beaumont reserves the right to hold the user accountable for any charges incurred by Beaumont for such calls.

Beaumont HEALTH

Title	Location	Functional Area
Acceptable Use Policy	**ALL Beaumont Health**	**Administration**
Policy Owner	Document Type	Effective Date
Director Corp Information Services	**Policy**	**02/09/2016**

d. Users must never use Beaumont computing or information assets to create, access, transmit or store any material that may cause embarrassment to Beaumont or would be considered inappropriate or in bad taste, offensive or disrespectful of others (e.g. obscene, lewd, pornographic or violent material, depicted nudity, sexually oriented jokes or cartoons, and/or other offensive material related to age, race, color, sex, religion, national origin, disability or sexual orientation). Users encountering or receiving this kind of material should immediately report the incident to Beaumont management.
e. Beaumont computing and information assets must never be used for personal political activity or for personal profit or gain. Information stored on corporate networks is only to be used for corporate purposes. The use of non-Public Beaumont information for a competitor or other purposes is prohibited. Access to non-Public Beaumont information after individuals have stopped working for or on behalf of Beaumont is strictly forbidden.
f. Access to a Beaumont resource does not imply permission to use the resource. Users must only manage or access those resources that are required for the performance of their assigned jobs. Users must not abuse their system privileges by accessing or managing Beaumont accounts (including their own, or those of friends, relatives and co-workers) outside of those required to perform their job responsibilities.
g. Casual browsing through Beaumont network files and directories is prohibited. Searching is permitted if users are trying to locate work-related information. Browsing through the Beaumont intranet, where sites have been created for informational, educational or recreational purposes, is exempt from this clause.
h. Users whose negligence results in damage to or loss of Beaumont property, other than normal wear and tear, may be responsible to reimburse Beaumont for such damage or loss.

4. **Configuration Control (Software and Hardware)**
   a. Beaumont computer systems must not be altered, modified, patched or upgraded (e.g., OS or application patches or upgrades, processor upgrades, changing memory, or adding extra circuit boards) without authorization. Changes, if required, must be performed by authorized IT personnel or processes.
   b. Laptops, desktops or workstations must not be configured as servers to support production business activities.
   c. Users must not copy Beaumont information from their PCs (desktops and laptops) to removable media (e.g. DVD, USB flash drives), unless an approved business case exception has been approved by Information Security. If data backup is required, the information must be stored in a Beaumont-approved data repository (e.g. SharePoint, network drive or other approved method).
   d. Users are not permitted to load, install or store, non-Beaumont owned or sanctioned software or applications on Beaumont computer systems without express permission and/or authorization from the appropriate IT authority. Such software includes but is

Beaumont HEALTH

Title **Acceptable Use Policy**	Location **ALL Beaumont Health**	Functional Area **Administration**
Policy Owner **Director Corp Information Services**	Document Type **Policy**	Effective Date **02/09/2016**

not limited to, unauthorized games, web browser "plug-ins", remote control software, instant messaging software (such as Facebook messenger Yahoo Messenger, SnapChat, etc.), consumer file sharing software such as Dropbox and Filepost, shareware, open source software, public-domain software, and freeware.

e. Users must not change, modify or delete any configuration files or settings that will prevent, stop or interfere with the delivery of official corporate patches, updates and/or system enhancements. The unauthorized copying or distribution of system configuration files is prohibited.
f. Users must not maliciously degrade or disrupt the performance or services of any computer system or network (both Beaumont-owned and non-Beaumont-owned).
g. Beaumont reserves the right to remove any unauthorized or illegal software on Beaumont-provided computing equipment without notice to the user. In appropriate cases, Beaumont may require users to reimburse Beaumont for the costs for rebuilds or other expenses associated with the use or installation of unauthorized or illegal software on Beaumont computing equipment. If unauthorized or illegal software use on Beaumont computing equipment is discovered, the incident must immediately be reported to Information Security.
h. Security software tools can be used for system penetration testing, password discovery, software copy-protection removal, port scanning, exploiting computer system vulnerabilities or illegally decrypting encrypted files. Unless specifically authorized by Information Security, users are prohibited from having these tools installed on their systems or running these tools on any Beaumont computing asset or network.
i. Users must connect to Beaumont networks to install software and upgrade packages (e.g., virus protection .dat files, Service Packs, patches, etc.) as soon as they are made available or as directed by Beaumont. Disabling these features is prohibited.
j. Beaumont-approved anti-malware software must be installed, functional and updated on PCs, laptops, workstations and similar devices. If a virus is found and the anti-virus software cannot clean the virus, or if an infection is suspected, the user must immediately disconnect the involved device from all networks, call the local technical support group or the Beaumont help desk, and make no further attempt to eradicate the virus.

5. **Passphrases, Passwords and PINs**
   a. Users must comply with all Beaumont passphrase requirements defined in the Identity and Access Management Standard.
   b. Users must select and maintain the confidentiality of individually assigned passphrases.
   c. Users must not use the identity of others and are responsible for any and all activity carried out using their credentials.
   d. Sharing of access codes, account numbers, passphrases or other authorizations which have been assigned is not permitted.

Beaumont HEALTH

Title	Location	Functional Area
Acceptable Use Policy	**ALL Beaumont Health**	**Administration**
Policy Owner	Document Type	Effective Date
Director Corp Information Services	**Policy**	**02/09/2016**

e. In the event of a business emergency or sudden illness, access may be temporarily provided with documented management and Beaumont Human Resources (HR) approval.

6. **Mobile Devices and Personal Computers**
   a. Users must only store Beaumont information on a laptop or mobile device for the minimum amount of time necessary to fulfill the specific business need.
   b. Beaumont-owned desktop computer equipment and software may be removed from Beaumont premises only temporarily and only with written authorization of the department manager. Users provided with laptop computers or other mobile devices may remove them from Beaumont premises for work-related purposes. Individuals are not permitted to move their desktop computer or peripheral devices, or re-assign laptop computers, iPads or other computing devices without approval from the Information Technology Department. All movement or reassignment of equipment must be coordinated through the information technology department. Managers are responsible for the equipment inventory of their staff.
   c. Users must employ all reasonable means to physically secure their computing devices from theft, abuse, damage or unauthorized use. These devices may include all computer equipment and cellular phones. When traveling, storing devices in checked luggage should be avoided if possible. Depending on the circumstances, the user may be charged the replacement cost for any Beaumont computing asset stolen from the user's possession.
   d. If necessary, users may temporarily secure laptops or other mobile computing devices in a vehicle provided they are locked in the vehicle and are not visible from outside the vehicle. If devices will be locked in a trunk, they should be placed in the trunk before leaving for the destination and not after arrival.
   e. Storage of laptops or other mobile computing devices in a vehicle overnight is prohibited.
   f. Use of recording devices in the workplace, including cameras and video recorders in enabled mobile devices, is strictly prohibited. Authorization may be granted when a specific business need will be served by use of the device and it is used in a lawful manner.
   g. Those required to use mobile devices in the course of business must comply with the following requirements while driving a vehicle:
      i. Use of mobile devices must always comply with all applicable laws.
      ii. Beaumont strongly recommends that users refrain from operating their mobile device while driving.

7. **Non-Beaumont Computing Assets**
   a. Users with non-Beaumont equipment that work on Beaumont premises must not physically connect their equipment to a Beaumont corporate network at any time. This equipment must only connect to Beaumont wireless networks approved for non-Beaumont equipment (e.g. Beaumont Guest Network).

Beaumont HEALTH

Title	Location	Functional Area
Acceptable Use Policy	**ALL Beaumont Health**	**Administration**
Policy Owner	Document Type	Effective Date
Director Corp Information Services	**Policy**	**02/09/2016**

b. Beaumont reserves the right to audit non-Beaumont assets used in support of Beaumont business, for compliance with Beaumont policies.

8. **Returning Equipment**
   a. When computer systems or computer media are transferred/reassigned to another user, all information must be deleted from the systems or media. Information with retention requirements must be copied or moved to an alternate location/system where the records must be accessible and retrievable to support the business and meet legal obligations. The system must be restaged or returned to the default Beaumont specification and media must be erased prior to transfer.
   b. Upon termination of employment or contract with Beaumont, individuals must immediately return all Beaumont computing and information assets in their possession or under their control. Unless otherwise specified, items must be returned to the individual's direct supervisor.
   c. All Beaumont information must be removed from information systems and equipment at the end of lease or prior to redistribution.
   d. When no longer required to support Beaumont, all Beaumont information must be removed from Beaumont and non-Beaumont assets.
   e. Contractors performing services for Beaumont must permanently remove Beaumont information from the laptop at the end of their engagement. The information removal must be confirmed. Beaumont reserves the right to audit the computing equipment to ensure the requirements are met.
9. **Reporting Incidents**
   a. If a Beaumont computing device or Beaumont information is lost or stolen, the user must immediately notify their management and contact Information Security at information.security@beaumont.org.

D. **Network Access and Usage**
   1. **Beaumont Network**
      a. Users must be authorized to access any Beaumont network (wired or wireless) and must only be granted access to those resources required to perform their job functions.
      b. Remote access to Beaumont's computing or information assets must be limited to activities related to, or in support of, a user's job-related functions. Beaumont-provided and approved remote access methods must be used.

E. **Electronic Mail**
   1. **Acceptable Use**
      a. Users must maintain a professional demeanor in all internal and external Beaumont communications. Due to the nature of the computing environment, users must be mindful of the possibility that others may regard their communications as authorized or official communications of Beaumont.
         i. The user name, email address, company affiliation and related information included with email messages must reflect the actual originator of the messages.

Beaumont HEALTH

Title	Location	Functional Area
Acceptable Use Policy	**ALL Beaumont Health**	**Administration**
Policy Owner	Document Type	Effective Date
Director Corp Information Services	**Policy**	**02/09/2016**

ii. Email containing Beaumont information which is sent from a Beaumont network or from a Beaumont computing device must use the Beaumont email infrastructure.
iii. 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 at any time without prior notice.
iv. Illegal, unethical, unauthorized or disruptive use of Beaumont information systems or equipment is prohibited. This includes, for example, accessing, transmitting, or storing inappropriate material (such as pornography, depicted nudity, lewd or violent materials, chain letters, sexually oriented jokes or cartoons, or other offensive or demeaning material related to age, race, color, sex, religion, national origin, disability or sexual orientation). Violators are subject to disciplinary action up to and including termination of employment or termination of contract.
v. Beaumont has the right to review, audit, or monitor email created, stored or transmitted on Beaumont email systems in accordance with local law.
vi. Unencrypted Beaumont confidential information must never be forwarded to a non-Beaumont email account.
vii. Email must not be automatically forwarded to a non-Beaumont mailbox (e.g., your personal email account or the account of a contract individual from another company).
viii. Personal non-Beaumont email accounts must not be used for Beaumont business.
ix. Credit/debit card data must never be transmitted or stored via email. This includes attachments that have credit card data.

2. **Email Storage**
   a. Beaumont email systems are tools to facilitate communication, and are not for the long-term preservation and storage of Beaumont Business Records. Email containing Beaumont information which is part of an Official Record, must be retained according to the Beaumont Records Retention Schedule. All other emails must be deleted when they no longer support ongoing business operations.
3. **Encryption**
   a. Beaumont information outside a Beaumont-controlled environment must be protected as follows:
      i. Confidential information must be encrypted in storage and transmission.
      ii. Proprietary information must be encrypted in storage and transmission unless Beaumont Management has explicitly determined exposure to the public would not cause negative consequences to Beaumont business activities or strategic initiatives.
      iii. Public information does not require encryption.

Beaumont HEALTH

Title	Location	Functional Area
Acceptable Use Policy	**ALL Beaumont Health**	**Administration**
Policy Owner	Document Type	Effective Date
Director Corp Information Services	**Policy**	**02/09/2016**

b. Beaumont information within a Beaumont-controlled environment must be protected as follows:
   i. PHI and Beaumont confidential information must be encrypted in transmission and storage outside of a Beaumont-enterprise-class datacenter
   ii. Encryption of non-personal confidential information is at the information owner's discretion.
   iii. Complete credit/debit card numbers must be encrypted in storage and transmission including in Beaumont-enterprise-class datacenters
   iv. Credit/debit card service code and expiration dates for credit/debit cards must be encrypted if stored or transmitted with the complete credit/debit card number including in Beaumont-enterprise-class datacenters.
   v. Card validation code or value (CVC) must never be stored. The CVC is either a data element on the card's magnetic stripe used to cryptographically protect the information on the stripe or the three or four digit number printed on the back or front of the card used to validate physical possession of the card during transactions.
   vi. Proprietary information does not require encryption.
   vii. Public information does not require encryption.

F. **Instant Messaging**
   1. **Usage**
      a. Skype for Business (also known as Lync) is permitted for Beaumont internal use only. Individuals are prohibited from downloading and using unapproved IM software (e.g. AOL Instant Messenger, Yahoo!, SnapChat, etc.) within the Beaumont computing environment.
      b. Professional and appropriate language must be used in all instant messages. Users are prohibited from sending abusive, harassing, threatening, menacing, discriminatory, pornographic, disrespectful, or otherwise offensive instant messages.
      c. Use of IM for transmitting or storing credit card data or PHI is prohibited.

G. **Beaumont-Provided Internet Access**
   1. **Use as a Business Tool**
      a. Internet access is provided for business purposes. Internet access is a privilege which can be taken away at any time without notice.
      b. Users are accountable for their actions when accessing the public Internet using the Beaumont network or using Beaumont computing assets.
      c. Nominal personal use of Internet access is permitted if it does not interfere with work or productivity, and does not conflict with directions from leadership. When in doubt, ask your immediate supervisor if the purpose is acceptable.
      d. Users must not download or install unauthorized Internet applications such as games and entertainment software, peer-to-peer network sharing applications, screen savers, instant messaging services or browser "plug-ins."

Beaumont HEALTH

Title	Location	Functional Area
Acceptable Use Policy	**ALL Beaumont Health**	**Administration**
Policy Owner	Document Type	Effective Date
Director Corp Information Services	**Policy**	**02/09/2016**

e. Access to the Beaumont Intranet by non-Beaumont employees requires approval of Beaumont management, and is permitted only when deemed to be in the best interest of Beaumont.

2. **Posting Beaumont Information**
   a. Employees are not permitted to make public postings (i.e., blogs or social networking websites) of confidential and/or proprietary information related to any aspect of Beaumont's business.

VI. ACCOUNTABILITY:

A. This Policy and any material revisions to it are subject to review and approval by the Information Access, Privacy and Security Committee (IAPSC). The Beaumont Information Security Officer (ISO) is responsible for the review and governance of this Policy. The Information Security Governance Team within the Information Security Program is responsible for maintaining and recommending revisions to this Policy. All departments are responsible for implementation of this Policy.
B. Supplementary Information Security Standards and Baselines may be issued so that Beaumont information and computing assets are protected in compliance with this Policy and applicable local laws, regulations and, as appropriate, best practices.
C. Departments are responsible for implementing this Policy and requiring that all Beaumont employees, contractors, suppliers and Beaumont third party service providers who have access to, use or create Beaumont information comply with this Policy.
D. All users of Beaumont information and computing assets are responsible for protecting the confidentiality, integrity and availability of Beaumont assets consistent with the requirements in this Policy and for the following:
   1. Promptly reporting ethics issues to the Trust Line: 800-805-2283
   2. Promptly reporting any actual or suspected inappropriate use of Beaumont information or computing assets to management and Information Security.

VII. INFORMATION AND COMMUNICATION:

A. Management will communicate to the ISO regarding major changes in corporate strategy, the regulatory environment or financial conditions that may necessitate changes in this Policy and recommend changes.
B. This Policy and any updates to it are accessible on the Beaumont Health intranet website.
C. This Policy will be communicated to all Beaumont employees, contractors, suppliers, Beaumont third party service providers affected. The Acceptable Use Policy must be acknowledged by users within 30 days of hire or contract inception. All Beaumont employees and those supporting the Beaumont computing environment must acknowledge and confirm compliance with this Policy annually.
D. Training and awareness for the Policy will be provided by Information Security and Beaumont HR via Policy Release Communications, news on the Beaumont Health intranet homepage, Information Security poster and CBT, etc.

Beaumont HEALTH

Title	Location	Functional Area
Acceptable Use Policy	**ALL Beaumont Health**	**Administration**
Policy Owner	Document Type	Effective Date
Director Corp Information Services	**Policy**	**02/09/2016**

VIII. POLICY MONITORING AND MAINTENANCE:

A. IT and other business review functions will validate compliance with this Policy. Any deficiencies and areas of non-compliance must be reported to management of the department.

B. Beaumont Information Security retains authority to enforce this Policy. Failure to comply with this Policy may result in the termination of access to Beaumont computing or information assets, and possible further disciplinary action, up to and including termination of employment or termination of contract. Beaumont will also comply with all applicable laws in relation to violations of this Policy including notifying appropriate law enforcement agencies of any illegal activities.

IX. AFFECTED AREAS AND EXCEPTIONS:

A. This Policy is applicable system-wide. It applies to all individuals who use or manage Beaumont computing or information assets, including, but not limited to, physical assets, such as equipment and supplies, information, and information technology.

B. There are no exceptions to this Policy. Risk to Beaumont associated with non-compliance must be accepted and assumed by the applicable Department.

X. REVIEW CYCLE:

A. This Policy will be reviewed annually by the ISO and the IAPSC. Additional reviews may be triggered by major changes in corporate strategy, the regulatory environment, or other conditions.

XI. EFFECTIVE DATE:

A. This Policy is effective on the date indicated in the header and supersedes all previous versions and/or other policies that cover the same subject matter.

XII. INQUIRIES

A. Questions pertaining to this policy should be directed to the Information Security team.

XIII. REFERENCES:

A. Compliance with Federal and State Privacy Laws and Regulations
B. Confidentiality & Computer Systems Usage Agreement
C. Information Security Policy
D. Code of Conduct

XIV. DOCUMENT CHANGE CONTROL

A. **Revision History**

Beaumont HEALTH

Title	Location	Functional Area
Acceptable Use Policy	**ALL Beaumont Health**	**Administration**
Policy Owner	Document Type	Effective Date
Director Corp Information Services	**Policy**	**02/09/2016**

Version #	Date Updated	Revision Author(s)	Summary of Major Changes Made
1.0	01-OCT-2015	Jim Fisher, Doug Copley	Creation of policy.
2.0	12-JAN-2016	Jim Fisher	Added reference links, updated section V.C.4.c to remove IronKey language.