Beaumont
HEALTH

Title	Location	Functional Area
Information Security Policy	**ALL Beaumont Health**	**Information Technology**
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 Information Security Policy (Policy) is to establish the high-level direction for properly managing the use, privacy, security, retention and disposal of Beaumont Health (Beaumont) information, as defined herein, so that the principles of confidentiality, integrity and availability are satisfied in accordance with applicable laws and regulations and healthcare industry guidance.

This Policy is modeled and structured in alignment with the ISO 27000-series Security Framework, which is a cross-industry standard. The requirements in this Policy along with the associated security standards and baselines are aligned with regulatory requirements and industry recommended practices for information security, such as those issued by the Office for Civil Rights (OCR), the PCI Security Standards Council, the National Institute of Standards and Technology (NIST) and the International Organization for Standardization.

III. SCOPE:

This Policy is applicable to Beaumont and its subsidiaries, including all Departments, employees and members of the workforce (collectively, Beaumont Health), including physicians, students and volunteers, and any third parties or business associates who provide services or host information or systems on behalf of Beaumont. This Policy applies to all Beaumont information including the information that is hosted or generated through purchased services or suppliers on behalf of Beaumont.

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 a variety of forms including, but not limited to, paper, microfilm, electronic storage media, photograph, video or voice recording. Beaumont information is owned by Beaumont, wherever it exists, regardless of location or storage medium.

A Department may choose to impose additional requirements that reflect information security control requirements appropriate or necessary to support conditions or activities unique to the particular Department; however, those requirements must meet or exceed the requirements specified in this Policy and the supporting standards.

Beaumont
HEALTH

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

IV. POLICY STATEMENT:

Beaumont has developed this Policy to safeguard, retain and properly dispose of Beaumont information. This Policy is supported by associated standards, which establish the minimum administrative, physical and technical security requirements necessary for the implementation of appropriate security controls across all Beaumont information systems including systems hosted or administered by service providers. In turn, baselines establish the minimum security controls to achieve conformance to the standards. All Beaumont information or system owners and custodians, including Beaumont employees, contractors, agents, and service providers, are individually and collectively responsible for safeguarding, retaining, and properly disposing of the Beaumont information entrusted to their care in accordance with this Policy and other applicable Beaumont policies.

Beaumont strives to protect Beaumont information by adhering to the following key security principles:

1. **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.
2. **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.
3. **Availability** – Assurance that information and information systems required by the business are accessible when necessary.
4. **Accountability** – Maintaining processes and controls necessary to trace actions to their source. Accountability supports the concepts of non-repudiation, deterrence, security monitoring, recovery, and legal admissibility of records.
5. **Assurance** – Addresses the controls used to develop confidence that technical and operational security measures work as intended. Assurance highlights the notion that secure systems provide the intended function while preventing undesired actions.

All Beaumont information or system owners and custodians, including Beaumont employees, contractors, agents, and Beaumont third party service providers, must be able to demonstrate due diligence in protecting information and the computing environments in which it resides. Illegal, unauthorized, or unethical disclosure, modification, misuse or destruction of Beaumont information is strictly prohibited.

A. Information Security Program

1. Information Security management is accountable for setting a clear direction for the security of Beaumont information in line with business objectives and demonstrating

Beaumont HEALTH

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

support for, and commitment to, information security through the issuance and maintenance of this policy and supporting standards and baselines.

a. Failure to comply with this Policy and associated standards may result in the termination of access to Beaumont information or the Beaumont computing environment, and possible further disciplinary action, up to and including termination of employment or termination of contract. Beaumont must also comply with all applicable laws in relation to potential violations of this policy including notifying appropriate law enforcement agencies of any suspected illegal activities.
b. Beaumont workforce members and Beaumont third parties may be held responsible for damages to Beaumont's information and Information Technology (IT) assets caused by their non-compliance with this Policy.
c. Beaumont Information Security retains authority to enforce the requirements in this Policy and associated standards.

B. **Information Security Risk Assessment and Management**

1. Beaumont Security is accountable for maintaining an ongoing information security risk assessment program in order to effectively identify, assess and mitigate information risk to Beaumont. Risk assessments must be performed according to the requirements defined in the Information Security Standards and Baselines.
2. Identified risks must be assessed and decisions made to accept, avoid or mitigate them. Risk assessment efforts and conclusions must be appropriately documented.

Required security controls are defined in the Information Security Risk Assessment and Management Standard.

C. **Organization of Information Security**

1. Beaumont's information security organization, led by the Information Security Officer (ISO), is responsible for the administration and execution of the Information Security Program across Beaumont.
2. The Beaumont ISO ensures the implementation of information security across Beaumont is reviewed for adequacy, and directs appropriately segregated assignments and co-coordination of information security roles.
3. Additional information regarding the Information Security team can be found in the Information Security Program documentation which can be requested from the Information Security Officer.

Required security controls are defined in the Organization of Information Security.

D. **Human Resources Security**

1. Required security background check and controls are defined in the Beaumont Human Resource Policies.
2. Applicable Beaumont Human Resources (HR) and IT policies must be followed for on-boarding and off-boarding any Beaumont employees, contractors and Beaumont third parties. Roles and responsibilities must be defined, documented and conveyed so that Beaumont employees, contractors and Beaumont third parties understand their information security responsibilities prior to employment or contract commitment, as well as after termination of employment or contract, as applicable. Code of Conduct,

Beaumont HEALTH

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

Confidentiality and Acceptable Use Policies must be included in the employee offer package and must be signed by new hires and non-employees prior to accessing Beaumont information systems.

3. Information Security management is accountable for establishing an Information Security Awareness Program to provide assurance that Beaumont employees, contractors and Beaumont third parties are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support Beaumont security requirements in the course of their normal work. The Information Security Awareness Program provides ongoing security training and awareness activities that include, but are not limited to new employee training, publication of information security awareness articles, awareness posters, lunch & learn sessions and departmental security and privacy sessions.
4. Disciplinary processes must be in place to take action against employees who have committed an information security breach.

E. **Asset Management**

1. All Beaumont Information assets must be identified, have a designated owner and an inventory of these assets should be drawn up and maintained.
2. All information systems must be identified, have a designated owner and an inventory of these assets should be drawn up and maintained.
3. Rules for the acceptable use of information and information systems must be identified, documented, communicated and implemented.
4. Beaumont information, when created or acquired, must be properly managed and controlled in a manner consistent with Beaumont policies, standards and baselines.
5. Beaumont information owners are accountable for proper classification, management and protection of Beaumont Information according to the information security requirements defined in this Policy and the Information Security Standards and Baselines.

Required security controls are defined in the Information Classification and Handling Standard.

F. **Access Control**

1. Access to Beaumont information and the computing environments must be appropriately controlled. Information or system owners are responsible for establishing effective processes to properly administer access rights to prevent the unauthorized access, compromise, or theft of Beaumont information and Beaumont IT Assets.
   a. Effective authentication methods must be implemented based on the level of business risk. Appropriate encryption methods must be used to protect authenticators (credentials) in transmission and storage.
   b. Access to both internal and external networks must be secured through multiple layers of access controls to protect against unauthorized access.
   c. Security controls must be implemented to restrict access to the operating systems of all system components, applications and infrastructure based on the principle of least privilege.

Beaumont HEALTH

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

d. Security and operational requirements must be defined and implemented to secure remote access to and from Beaumont network. Strong authentication and encryption must be in place to secure remote communications.

Required access controls are defined in the Identity and Access Management Standard.

G. **Cryptographic Controls**

1. Consistent with the sensitivity of the information, Cryptographic controls (encryption) must be used to protect the confidentiality, integrity and availability of all Beaumont information assets.
2. Transmitting sensitive Beaumont information, including Protected Health Information (PHI), Personally Identifiable Information (PII) and Payment Card Information (PCI) over the public internet without using a Beaumont approved encryption method is prohibited.

Required security controls are defined in the Physical Security policies.

H. **Operations Security**

1. In coordination with IT where appropriate, departmental management is accountable for defining operational procedures and responsibilities for the proper management and operation of all Information Systems.
   a. Operational processes and procedures must be established, documented and tested prior to their acceptance and production use to verify the confidentiality, integrity and availability of all information systems.
   b. Information system activities must be regularly monitored to identify policy violations and anomalous behavior and to protect Beaumont information, including protected health information.
   c. Information about technical vulnerabilities of information systems being used should be obtained in a timely fashion, the organization's exposure to such vulnerabilities must be evaluated and appropriate measures taken to address the associated risk.
2. Changes to business processes, physical facilities and information systems that affect information security must be controlled.
3. Beaumont must verify that the implementation of Information Systems by Beaumont third parties or operational services delivered by Beaumont third parties meet information security and service delivery requirements in accordance with Beaumont standards and/or third party service delivery agreements as appropriate.
4. Information storage media (physical and electronic) must be controlled and protected to prevent unauthorized disclosure, modification, removal or destruction of Beaumont information.

Required security controls are defined in the IT Communication and Operations Management Standard, the Electronic Communication Standard and the IT Segregation of Duties Standard.

I. **Communications Security**

1. In coordination with IT where appropriate, departmental management is accountable for defining and implementing system and operational requirements to ensure the security,

Beaumont HEALTH

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

integrity and accountability of electronic communications and electronic commerce transactions, including the information involved in those processes.

2. Beaumont networks must be managed and controlled to protect information in information systems.
3. Groups of information services, users and information systems must be appropriately segregated on networks.
4. Formal transfer policies, procedures and controls must be in place to protect the transfer of information across all types of communications.
5. Information transfers to third parties must be assessed for security and compliance, and formal agreements must be in place between Beaumont and the third party receiving or processing the information. Agreements involving the transfer/access/storage of PHI must include a Business Associate Agreement addendum.

Required security controls are defined in the IT Communication and Operations Management Standard, the Electronic Communication Standard and the IT Segregation of Duties Standard.

J. **Information Systems Acquisition, Development and Maintenance**

1. Applications and infrastructure components must be created or implemented using a Beaumont approved development or implementation process. Security control requirements must be defined and processes must be established so that information systems are developed, acquired, and maintained with appropriate security controls.
2. Appropriate controls must be designed into information systems to prevent the unauthorized access, use, modification, or disposal of information. All security requirements must be identified at the requirements phase of a project and justified, agreed and documented as part of the overall business case for an information system.
3. Without a documented and approved exception by Beaumont Information Security, all information systems in the Beaumont environment are subject to monitoring, including but not limited to vulnerability scanning, event log monitoring, system configuration monitoring and access control monitoring. All changes to IT-managed information systems must follow the approved IT Change Management Process.

Required IT and security controls are defined in the Information Systems Acquisition, Development and Maintenance Standard.

K. **Third Party Services Management**

1. Departments are responsible for exercising appropriate due diligence in selecting service providers and in consultation with Information Security, must verify service providers have implemented adequate security controls to safeguard any applicable Beaumont information.
2. Risks to Beaumont information and computing environments from business processes involving external parties must be identified and appropriate controls implemented before granting any external party access to Beaumont information and/or Beaumont computing environments.
3. Any third party information possessed by Beaumont must be protected in accordance with the terms of any agreements between Beaumont and the third party.

Beaumont HEALTH

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

Required security controls are defined in the Third Party Services Security Standard.

L. **Information Security Incident Management**

1. Per the Information Security Incident Response Plan, responsibilities, processes and procedures must be defined by Departments to respond to, and report actual or suspected information security events and weaknesses in a timely manner.
2. All Beaumont workforce members are required to report any information security events and weaknesses as quickly as possible. Information Security is accountable for communicating information security incident reporting procedures to Beaumont workforce members.

Required security controls are defined in the Information Security Incident Response Management Standard.

M. **Business Continuity and Disaster Recovery Management**

1. A periodic business impact assessment must be completed to identify business-critical information systems and prioritize their continuity and recovery needs.
2. In coordination with IT where appropriate, departmental management is accountable for maintaining business continuity and disaster recovery plans and processes to mitigate the risk and impact of interruptions to business activities, and to protect critical business processes from the effects of disasters or major failures of information systems.

Detailed requirements are defined in the Disaster Recovery Standard.

N. **Compliance**

In combination, the Corporate Compliance Policies and Corporate Compliance Department provide the framework for the management of compliance risk at Beaumont.

1. Departments must comply with Beaumont security policies and associated standards. The security of information systems must be regularly reviewed, monitored and audited to determine/verify compliance with Beaumont policies and regulatory requirements.
2. Technical compliance checking must be implemented on system platforms to support compliance verification.

V. STANDARDS, PRACTICES AND PROCEDURES

A. Applicable Laws and Regulations

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, including the 2013 provisions in the Omnibus HIPAA rules
   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. State of Michigan IDENTITY THEFT PROTECTION Act 452 of 2004 MCL 445.63(o)
   d. Payment Card Industry Data Security Standard (PCI DSS)
   e. Federal Trade Commission's Identity Theft Prevention Red Flags Rule (16 CFR § 681.2)

Beaumont HEALTH

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

2. The Beaumont Legal Staff is responsible for identifying, interpreting, and communicating legal and regulatory requirements (and any changes to them) applicable to this Policy.

B. **Information Security Standard and Baselines**
1. This Policy is supplemented by the Beaumont Information Security Standards and Baselines published on the Beaumont intranet.
2. Any inconsistencies between this Policy and any other statements regarding information security are governed by this Policy.

VI. ACCOUNTABILITY AND MONITORING

A. This Policy will be reviewed and renewed annually by the ISO and the Beaumont Information Access, Privacy and Security Committee (IAPSC). Additional reviews may be triggered by major changes in Beaumont strategy or the applicable regulatory environment.

B. This Policy and any material revisions to it are subject to review and approval by the IAPSC. The ISO may approve immaterial changes to this policy. The ISO is responsible for the review and implementation of this Policy and any subsequent revisions. The ISO is responsible for having in place a defined governance process for review and approval of this Policy and any subsequent revisions. The IAPSC reviews and approves the publication of Information Security Standards and Baselines. 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.

C. Supplementary Information Security Standards and Baselines may be issued so that Beaumont information is protected in compliance with this Policy and applicable local laws, regulations and, as appropriate, best practices.

D. Departments are responsible for implementing this Policy and requiring that all Beaumont employees, contractors and workforce members who have access to, use or create Beaumont information comply with this Policy and any supplementary security standards issued by Information Security. Departments are responsible for requiring suppliers and Beaumont third party service providers who have access to or use Beaumont information, or create information for Beaumont, to comply with this Policy and any supplementary security standards issued by Information Security.

E. IT and other business review functions will validate compliance with this Policy.

VII. COMMUNICATION

A. This Policy and any updates to it are accessible on the Policies page on the Beaumont Health intranet.

B. This Policy will be communicated to all affected Beaumont employees, contractors, workforce members and Beaumont third party service providers. Training and awareness for the Policy will be provided by Information Security via Policy Release Communications, Employee News on Inside Beaumont Online homepage, Information Security Poster and PowerPoint Presentations, etc. Annual Information Security training is mandatory.

VIII. RISK AND ESCALATION

Beaumont HEALTH

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

A. There are no exceptions to this Policy. Information Security has established the Information Security Program to monitor non-compliance and to work with the business areas on risk management plans where necessary.
B. Any deficiencies and areas of non-compliance with this Policy will be reported to management of the Department and escalated to executive and governance functions as appropriate. Information owners or system owners, in consultation with Information Security, are responsible for developing and executing remediation action plans.
C. Any violation of this Policy is subject to disciplinary action, up to and including termination of employment or contract and the possibility of civil and criminal liability.

IX. DEFINITIONS:

A. **Beaumont Information:** 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. This includes patient Protected Health Information (PHI) created, accessed, stored, processed or transmitted on Beaumont systems.
B. **IT Asset:** All hardware, software, data files and documentation used to support Beaumont business.
C. **Beaumont Third Parties:** Joint Ventures (JVs), Alliances and Business Process Outsourcing (BPOs), Application Service Providers (ASPs), Infrastructure Technology Outsourcing (ITOs) and all other Beaumont suppliers and service providers acting for, on behalf or in support of, Beaumont.
D. **Business Associate:** A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information (PHI) on behalf of, or provides services to, Beaumont. A member of Beaumont's workforce is not a business associate. The types of functions or activities that may make a person or entity a business associate include, but are not limited to: claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; and re-pricing. Business associate services are: legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; and financial.
E. **Department:** Those organization groups that combine or consolidate certain required support services, some of which may be responsible for policy making or governance, including such functions as audit, compliance, communications, legal, finance, human resources, and information technology, as well as clinical services.
F. **Information Custodian:** Individual responsible for the day-to-day handling and protection of Beaumont information. The information custodian must protect information according to the information owner's requirements. The information owner at all times remains accountable for the information and its protection.
G. **Information Owner:** The individual whose business responsibilities are supported by the Beaumont 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.

Beaumont HEALTH

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

H. **Information System (System):** The computer systems and information resources used by Beaumont to support its business operations.
I. **Least Privilege (Need-to-Know):** A control principle that grants an entity (e.g., user, computer processes) only that amount of access or authority necessary to complete the required job function or task.
J. **Policy:** Policies are high-level management statements of intent, instructions or business rules that provide guidance to enable individuals to make present and future decisions. Policies are mandatory. This definition is used specifically for this Policy.
K. **Procedure:** Procedures are specific operational steps or manual methods that support a policy or standard. For example, a policy could describe the need for back-ups. A standard could define the software to be used to perform back-ups and how to configure this software. A procedure could describe how to use the back-up software, the timing for making back-ups, etc. This definition is used specifically for this Policy.
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. For information handling purposes, a patient's social security number will also be treated as PHI and will only be obtained, used, or disclosed as necessary to execute treatment, payment or health care operations.
M. **Security Baseline (Baseline):** The defined minimum set of security requirements for specific processes or technologies. Security baseline requirements are mandated by, and support, the policy and standards. This definition is used specifically for this Policy.
N. **Security Standard:** Standards are mandatory. They are the next level below policies and include details such as: implementation parameters, systems design concepts, software interface specifications, technologies used and other specifics. This definition is used specifically for this Policy.

X. REFERENCES:

A. The policies listed below may be in varying stages of publication and implementation and are found on the Policies page on the Beaumont Health intranet.
   1. Identity and Access Management Standard
   2. Acceptable Use Policy
   3. Disaster Recovery Standard
   4. IT Communication and Operations Management Standard
   5. Corporate Compliance Policies
   6. Electronic Communication Standard
   7. Human Resources Policies
   8. Information Classification and Handling Standard
   9. Information Disposal Security Standard
   10. Information Security Risk Assessment and Management Standard
   11. Information Systems Acquisition, Development and Maintenance Standard

Beaumont HEALTH

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

12. IT Segregation of Duties Standard
13. Third Party Services Security Standard
14. Information Security Incident Response Management Standard

XI. DOCUMENT CHANGE CONTROL:

A. Revision History

Version #	Date	Revision Author(s)	Summary of Major Changes Made
1.0	30-SEPT-2015	Danielle Lia, Doug Copley	First information security policy for Beaumont Health.