Status **Active** PolicyStat ID **16925266**

Effective 10/2024
Next Review 10/2027

Owner Jose Muniz: Advisor, IS Risk Mgmt
Area Information Services
Applicability System-Wide AG

# Acceptable Use Policy, 4.1



# I. POLICY

This policy is outlined for the use of each person with access to the Baptist Health Information Systems and should be adhered to by each user.

## No Expectation of Privacy

**Baptist Health users shall have no expectation of privacy in anything stored, sent or received on Baptist Health's information systems and/or electronic resources. Baptist Health reserves the right to monitor, limit or restrict the use of information systems and/or electronic resources based on Baptist Health's business missions and patient safety and quality of care goals, business reasons, technical priorities, and financial considerations, as well as when it is presented with evidence of a violation of Baptist Health's policies, contractual agreements, or local, state, federal or applicable international laws. Baptist Health reserves the right to actively monitor, restrict, use, and dispose of e-mail messages, other electronic communications, and/or personal stored files to properly maintain and manage the security of Baptist Health's information systems and/or electronic resources.**

# II. PURPOSE

The purpose of this Acceptable Use Policy is to establish the parameters for the use of Baptist Health's information systems and/or electronic resources to ensure:

- Baptist Health information systems and/or electronic resources are used for Baptist Health business purposes.
- Baptist Health information systems and/or electronic resources are not used inappropriately.
- Protection of Baptist Health information systems, electronic resources and information assets to ensure their confidentiality, integrity and availability.

- Maintain confidentiality of privileged or protected information and Baptist Health's proprietary information.
- The Health Insurance Portability and Accountability Act (HIPAA) security rule is followed to protect the confidentiality, integrity and availability of patient information housed on information systems and/or electronic resources.
- The Florida Information Protection Act of 2014(FIPA) is being followed and covers the expanded definition of "personal information" to include individuals' first name or first initial and last name, in combination with any one of the following: passport number; medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional; or health insurance policy number, subscriber identification number, or any unique identifier health insurers use to classify individuals.

# III. DEFINITIONS

**Acceptable Use Policy-** An acceptable use policy (AUP) is a policy that a user must agree to follow in order to be provided with access to information systems and/or electronic resources. It provides a core component of Information Security by establishing practices to protect the confidentiality, integrity, and availability of Baptist Health technology resources in the course of day-to-day business activities.

**Artificial Intelligence (AI) -** Artificial intelligence generally refers to the development of computer systems that can perform tasks that typically require human intelligence, such as perception, reasoning, learning, and decision-making.

**Baptist Information Services Service Desk –** Technical support area within Baptist Health to assist end users with technology questions or problem resolution.

**Bandwidth –** The amount of data that can be transmitted in a fixed amount of time. For digital devices, the bandwidth is usually expressed in bits per second (bps) or bytes per second. For analog devices, the bandwidth is expressed in cycles per second, or Hertz (Hz).

**Broadcast Electronic Communication** – Communication sent to the entire Baptist Health organization or sent to distribution lists containing greater than 100 names.

**Cloud computing -** Cloud computing has been defined by the National Institute of Standards and Technology (NIST)as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or cloud provider interaction.

**Denial of Service** – Denial of service is an attempt to make a machine or network resource unavailable to its intended users.

**Electronic Data** - The definition of "Electronic data" includes any and all items or files stored on computer hard disks, floppy disks, CD-ROM discs or removable storage.

**Electronic Resource** – Any resource used for electronic communication, including but not limited to Baptist Health network, internet, e-mail, cloud services and social media

**File Sharing -** is the practice of distributing or providing access to digitally stored information, such as computer programs, multimedia (audio, images and video), documents or electronic books. It may be

implemented through a variety of ways. Common methods of storage, transmission and dispersion include manual sharing utilizing removable media, centralized servers on computer networks, WorldWide Web-based hyperlinked documents, and the use of distributed peer-to-peer networking.

**Health Insurance Portability and Accountability Act (HIPAA) -** US law designed to provide privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals and other health care providers. Developed by the Department of Health and Human Services, these standards provide patients with access to their medical records and more control over how their personal health information is used and disclosed. They represent a uniform, federal floor of privacy protections for consumers across the country. HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs. HIPAA also requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers.

**Information Asset** - a piece of information, such an employee record, a customer list, or a financial report, that is valuable to a company or organization.

**Information System -** a personal computer, workstation, laptop, server, or other equipment owned and managed by Baptist Health used for the electronic storage, processing of any data or information asset.

**Large Language Models (LLM)** - Large language models, in simple terms, are advanced computer programs that have been trained to understand and generate human-like language. These models are built using a type of artificial intelligence (AI) called deep learning.

**Peer-to-Peer File Sharing** - Peer-to-Peer (P2P) technology is a way to share music, video and documents, play games, and facilitate online telephone conversations. The technology enables computers using the same or compatible P2P programs to form a network and share digital files directly with other computers on the network.

**Protected Health Information (PHI)** – Protected Health Information is health information that can be used to identify an individual and includes health information. Examples include, but are not limited to: first name or first initial and last name, SS#, address, diagnosis codes, dates of service, etc.

**Personally Identifiable Information (PII)** - is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. Examples include but are not limited to: first name or first initial and last name, in combination with any one of the following: passport number; medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional; or health insurance policy number, subscriber identification number, or any unique identifier health insurers use to classify individuals

**Social Networking -** Generally includes all types of postings and/or interaction on the internet, including, but not limited to, social networking sites, (such as Facebook©, MySpace© or LinkedIn©), blogs and other online journals and diaries, discussion boards and chat rooms, microblogs such as Twitter©, 3rd party rating sites such as Yelp©, smartphone applications, multimedia host sites (such as YouTube© or Flickr©) and similar media.

**Software Assets** – applications, data and programs used to run an infrastructure.

**Software Asset Management** - all of the infrastructure and processes necessary for the effective management, control and protection of the software assets throughout all stages of their usable life.

# IV. PROCEDURES

A. **Information Technology and Security**

**RULES OF BEHAVIOR / USER ACCEPTABLE USE**

All users should maintain the protection of Baptist Health's confidential information assets. This requires users to exercise precautions to protect confidential data.

Baptist Health users should use reasonable precautions to prevent unauthorized access to electronic data while using Baptist Health's information systems, information assets, and/or electronic resources.

B. **Access and Passwords**

Baptist Health-issued user ID's and passwords are the property of Baptist Health. No person may use a user ID or password that has been issued to another person. Never share your password with anyone. Never save Baptist Health work related passwords in an internet browser or web site. If an internet browser asks to save your password (e.g. when logging into Outlook Web or the Physician's Portal) you will need to select, "No," or "Never save passwords for this site." If you suspect that your password is known by another, change it immediately. Passwords will be subject to minimum requirements provided in the Baptist Health Password Policy 4.12. If you suspect your password has been compromised without your permission, notify your manager and contact the Baptist Information Services Service Desk immediately.



C. **Roles and Responsibilities**

The following are the responsibilities of management, end users, and Information Services:

1. **Corporate Officer and Director:**
    a. Maintain and promote a climate of security to protect corporate assets, employee information and patient confidentiality.
    b. Enforce this Acceptable Use policy and administer disciplinary action as necessary.
2. **Manager, Supervisor and Team Leader:**
    a. Disseminate this Acceptable Use policy to all authorized users.
    b. Ensure adherence to this Acceptable Use policy and to report any violations to their supervisor and Information Services.
    c. Promptly provide Information Services with user changes (e.g. transfers, terminations, etc.).
3. **Information Services Responsibilities:**
    a. Monitor user's activity to ensure compliance with corporate policy.

b. Report all violations and suspicious activity to the manager or director of Information Services.

4. **End User Responsibilities:**
    a. Compliance with this Acceptable Use policy.
    b. Report any violations, suspicious activity and/or security incidents to their supervisor and Information Services.

D. **Authorized Use**

1. **Authorized users**
   An authorized user is any individual who has been granted authority by Baptist Health to access its information systems, information assets, and/or electronic resources.
2. **Unauthorized use is strictly prohibited**
   If a user ceases being authorized to use Baptist Health's information systems, information assets, and/or electronic resources, or if such user is assigned a new position and/or responsibilities, any use for which that user is not specifically authorized in their new position or circumstances shall cease.
3. **Personal Use**
   Baptist Health information systems, information assets, and/or electronic resources are for Baptist Health business use only.



E. **Unacceptable Use**

Under no circumstances are Baptist Health's users authorized to engage in any activity that is illegal under local, state, federal or applicable international law while using Baptist Health's information systems, information assets, and/or electronic resources. Replace "Create, download, view, store, copy or transmit materials related to gambling, illegal weapons, terrorist activities, illegal activities or activities otherwise prohibited."

The lists below include, but are not limited to, the categories of unacceptable and prohibited use when using Baptist Health information services and/or electronic resources.

**Ethical Use** -No user may act in unethical ways. Examples of unethical behavior include, but are not limited to, invading the privacy of others and engaging in acts of conflict of interest.

**Baptist Health's Reputation** – Publicly posting defamatory comments (including but not limited to email, Internet instant messaging, chat rooms, websites, blogs, social networking or social media sites), about the organization, co-workers or patients could create a liability for yourself and/or the organization and could lead to disciplinary action. For more detail, reference policy 1.2.19 Social Media

**Forgery of Communications** - Altering electronic communications to hide identity or impersonate another person is considered forgery and is prohibited while using Baptist Health's information systems, information assets, and/or electronic resources.

**Soliciting Business** - Users may not use Baptist Health's information systems, information

assets, and/or electronic resources for soliciting business, selling products, or otherwise engaging in commercial activities other than those expressly permitted by Baptist Health management.

**Fraud** - Users may not use Baptist Health's information systems, information assets, and/or electronic resources to make fraudulent offers for products, items, or services, or make statements about warranty, expressly or implied.

**Disruptions** - Users may not engage in activities that cause disruption to the workplace environment while using Baptist Health's information systems, information assets, and/or electronic resources.

**Excessive Use of System Resources** - Excessive use of Baptist Health's network bandwidth or other electronic resources that may degrade network capacity or performance is not permitted. All users should refrain from acts that waste Baptist Health information services and/or electronic resources or prevent others from using them. Examples include but are not limited to video streaming or downloads and music streaming and downloads.

**Prohibited Information System and/or Electronic Resources Activities** - The following activities are strictly prohibited on Baptist Health's information systems and/or electronic resources, except where explicitly authorized by the SVP CDIO or VP CISO of Information Services:

- Purposely introducing malicious programs into the electronic communication systems (e.g., viruses, worms, Trojan horses, E-mail bombs, root kits, etc.)
- Purposely bypassing Information System security measures (such as security scanning, disabling antivirus or firewall, asset inventory, etc.)
- Purposely attempting to bypass Internet activity monitoring by using a browser anonymizer or other method of anonymity.
- Possessing or using tools such as password cracking or network sniffing on your information system.
- Any activity which can cause a security breach or disruption of electronic communication is prohibited. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a system or account that the user is not expressly authorized to access.
- Baptist Health's information systems and/or electronic resources shall not be used in any manner that violates the Harassment Policy (1.2.7) or Bullying in the Workplace Policy (1.2.17).
- Illegally obtaining or distributing copyrighted material that is not authorized for reproduction or distribution.
- Using peer-to-peer file sharing.
- Accessing home computers or non-Baptist Health devices remotely without authorization.
- Copying or storing BH "confidential" or "internal use only" data to unauthorized third parties including, but not limited to, unauthorized cloud storage providers, grammar

checkers, or Artificial Intelligence (AI), Large Language Models (LLM) (Google Docs, Dropbox, Yammer, Grammarly, ChatGPT, etc.) or personal computers.

- Printing BH "confidential" or "internal use only" data to unauthorized printers.
- Gambling in any form, including Internet casino gambling.
- Connecting a Baptist Health computer to two or more networks at the same time (doing so could bypass Baptist Health network protections or compromise the corporate network)
- Connecting a Baptist Health computer to the Baptist Health public wireless (when a Baptist Health computer is in a Baptist Health facility, it is only permitted to connect to the Baptist Health standard corporate network)
- Auto-forwarding of Baptist Health emails to personal non-Baptist Health email accounts (e.g., Yahoo, Gmail, etc.)
- Using out-of-office or auto-replies within Outlook to non-Baptist Health email addresses when you are out of the office
- Connecting a Baptist Health computer to Wi-Fi Hot Spot while the Baptist Health computer is in a Baptist Health facility (when a Baptist Health computer is in a Baptist Health facility, it is only permitted to connect to the Baptist Health standard corporate network)
- Leaving your computer unlocked while unattended. You must lock your device when you walk away. Clinical workstations this means “tapping” out and regular user workstations this means locking your Windows session. Contact the service desk if questions on procedure.



F. **General Use**

1. **Internet Use**
   Baptist Health is not responsible for material viewed, downloaded, or received by users via the Internet. Responsible attitudes and appropriate behavior are essential in using this resource. To protect personal safety and privacy, Internet users should not give out Baptist Health information to others on public resources, without taking into consideration the risks of doing so. Users access the Internet with Baptist Health facilities at their own risk.

   NOTE: Information Services routinely monitors Internet use to ensure compliance.

2. **Non-Baptist Health Hardware**
   Only Baptist Health owned and managed devices or equipment are permitted on or connected to the BH corporate network. Non-BH owned devices, or equipment may ONLY be connected to authorized BH guest networks. Any exceptions to this require advance Information Services review as well as approval from an IS Director or above, which may take up to 14 days.

3. **E-mail use**
   All personnel who use email shall use email for appropriate business-related activities only. When sending business email containing "confidential" information, the email must be encrypted if sending to non-Baptist Health recipients. Baptist

Health routinely audits email to ensure compliance.

Baptist Health reserves the right to restrict personnel from accessing personal email accounts (e.g., Yahoo, Gmail, etc.) from any Baptist Health information system and/or electronic resource.

For additional information, including email guidelines, please see policy 4.7 Electronic Mail (email).

4. **Texting**
   Text messaging BH Confidential information is prohibited unless done using the BH secure text message solution. For additional information, including texting guidelines, please see policy 4.6 Text Messaging Policy.
5. **Instant Messaging**
   Instant messaging BH Confidential information is prohibited unless done using the BH standard and secure text message solution. For additional information, please see policy 4.32 Instant Messaging Policy.
6. **Mobile Devices (Smartphones/Tablets/Laptops)**
   Mobile devices are important tools for the organization and their use is permitted in support of Baptist Health's mission and core values. However, these devices also represent a significant risk to Baptist Health confidential data and systems if appropriate controls are not applied. Therefore, the following policy aspects must always be adhered to. For further information, please refer to 4.10 Mobile Device Policy and the Baptist Health IS Mobile Device Standard.
   - All mobile devices, regardless of being Baptist Health owned or personally owned, that are used to access Baptist Health information systems and/or electronic resources must adhere to the 4.10 Mobile Device Policy and the Baptist Health IS Mobile Device Standard. For any personally owned mobile device, PHI/PII and/or Baptist Health confidential data may not be accessed and/or stored on devices at any time unless using an approved Baptist Health application as set forth in the Baptist Health IS Mobile Device Standard.
   - Any inappropriate access, storage, use or disclosure of Baptist Health data identified as a result of any monitoring or audit conducted pursuant to this Policy shall be promptly reported to the Information Services Director.
   - Users are prohibited from connecting personal devices to USB ports on any Baptist Health system.
   - Baptist Health applications and Baptist Health data on mobile devices will be remotely deleted if you leave employment by Baptist Health or if the device is lost, stolen or replaced.
   - Users are responsible to immediately report to the Baptist Health Service Desk all lost or stolen devices including personally-owned devices configured to connect to the Baptist Health network or access Baptist Health information.
   - Email access on mobile devices is permitted using only authorized

applications. For details, please see the 4.7 Electronic Mail Policy.

- Social Networking may be accessed by users, using Baptist Health owned or personally owned devices on personal time or during breaks, but not around patients, in patient care areas, or in waiting areas. A personally owned device may only access Social Networking using either cellular service on the device or by connecting to the following Baptist Health Wi-Fi networks: Baptist Health Public Internet or bhpvtpub.
- Photographing any Baptist Health confidential data inclusive of PII and PHI data is strictly prohibited and is subject to the same requirements detailed in 6.5.11 Patient Privacy – Use of Cameras, Camera phones & other Audio-Visual Equipment policy.
- Baptist Health reserves the right to wipe personal devices if necessary, however all efforts will be made to avoid this while still maintaining the protection of Baptist Health data.

7. **Removable Storage & Media**
   Only authorized personnel may access, modify or transfer Baptist Health data stored on removable media. Transportation of media outside of Baptist Health controlled facilities will be restricted to only authorized personnel and will be required to have authorization prior to removal as well as maintain a record of all authorized removals. The connection of privately owned USB data storage devices to Baptist Health computers is not permitted. For additional information please see 4.23 Removable Media Protection Policy.
8. **Cloud Storage Services**
   Baptist Health prohibits the copying or storing of any BH confidential or "internal use only" data to unauthorized third parties including but not limited to cloud storage providers (Google Docs, Dropbox, Yammer, etc.) or personal computers.
9. **Faxing Documents**
   All Facsimile (fax) transmissions must contain the Baptist Health-approved approved cover sheet with the standard HIPAA and privacy notice. Fax cover sheets are located on the Intranet at the following path: Home/ Support Departments /Marketing/ Marketing and Public Relations/Templates/Stationery/Templates.

G. **Software**

1. All software purchased by BH is protected under U.S. copyright laws.
2. Only approved BH software may be installed on BH devices. All software installs must be completed by Information Services.
3. Users may not loan or give Baptist Health-owned software to anyone.
4. Software is not transferrable if employee transfers or leaves a department.

H. **Sanctions**

Failure to adhere to this policy may result in the enforcement of the Progressive Discipline Policy (Baptist Health Policy 1.2.11) and/or Immediate Discharge policy (Baptist Health policy 1.2.10), up to and including termination.

# V. REFERENCES AND AUTHORITATIVE STANDARDS

1. HIPAA Security Rule
    a. 45 CFR §164.308(a)(3)(ii)(A) - Authorization and/or supervision
    b. 45 CFR §164.310(b) – Workstation Use
    c. 45 CFR §164.310(c) – Workstation Security
2. ISO/IEC 27001:2005 and ISO/IEC 27002:2005
    a. A.7.1.3 – Acceptable Use of Assets
    b. A.9.2.7 – Removal of property
    c. A.10.7.1– Electronic Messaging
    d. A.11.7.1– Mobile computing andcommunications
    e. A.11.7.2– Teleworking
    f. A.15.1.5- Prevention of misuse of information processing facilities
3. 4.6 Text Messaging Policy
4. 4.7 Electronic Mail Policy
5. 4.10 Mobile Device Policy
6. 4.12 Password Policy
7. 4.23 Removable Media Protection Policy
8. 1.2.19 Social Media Policy
9. 1.2.7 Harassment Policy
10. 1.2.17 Bullying in the Workplace Policy
11. 1.2.11 Progressive Discipline Policy
12. 1.2.10 Immediate Discharge Policy



*This policy/procedure is only intended to serve as a general guideline to assist team members in the delivery of patient care; it does not create standard(s) of care or standard(s) of practice. The final decision(s) as to patient management shall be based on the professional judgment of the health care provider(s) involved with the patient, taking into account the circumstances at that time. Any references to sources, some parts of which were reviewed in connection with formulation of the policy/procedure are for informational purposes only. The references are not adopted in whole or in part by the hospital(s).*

## Approval Signatures

| Step Description | Approver | Date |
|---|---|---|
| SVP, Chief Digital Info Officer | Aaron Miri: SVP,Chief Digital Info Officer | 10/2024 |
| Chief Info Security Officer | James Case: Chief Info Security Officer | 10/2024 |
| | Jose Muniz: Advisor, IS Risk Mgmt | 10/2024 |

## Applicability

BMC Beaches, BMC Clay, BMC Jacksonville, BMC Nassau, BMC South, Baptist Health System, Baptist MD Anderson, Baptist Medical Group, Baptist Primary Care, Wolfson Childrens Hospital

## Standards

Standard Body: IM.01.01.01 EP02

Chapter: Information Management (IM)

Standard Body: IM.02.01.01 EP01

Chapter: Information Management (IM)

Standard Body: IM.02.01.03 EP01

Chapter: Information Management (IM)

Standard Body: IM.02.02.07 EP02

Chapter: Information Management (IM)