

Safeguards Matrix

for Protecting Patient Information



As a member of the Baptist Health South Florida workforce, you may be accessing, using and/or disclosing protected health information to do your job. Listed below are examples of steps you MUST take in order to safeguard and secure the information entrusted to you:

Administrative Safeguards

- Avoid discussing patient information in open or semi-private areas whenever possible. If unavoidable, lower the tone of your voice, remain attentive of your surroundings and patient's wishes;
- In the event a patient or employee wishes to exercise one of his or her privacy rights, contact the Privacy Office or the Office of Patient Experience;
- Verify in the patient's record if a patient has opted out of the facility directory prior to releasing any information;
- Provide the minimum amount of patient information necessary in nontreatment situations;
- Use best professional judgment to ensure that the person requesting patient information is involved in the patient's care and treatment or responsible for payment:
 - If the request is from a family member or friend who would like information about a patient's condition, and the patient is awake, alert and oriented, consult the patient for approval (provided he or she has not opted out of the facility directory);
 - If the request comes to the nursing unit, you may ask questions to determine if the requestor is involved in the care and treatment of the patient, which would allow information to be provided;
 - If the patient is incapacitated, and there is a healthcare proxy/surrogate involved in the care and treatment of the patient, you may direct the requestor to talk to the health care proxy or designated surrogate; and
 - If the request is made to Patient Financial Services and is regarding account information, someone from financial services should ask for the requestor's information to determine if disclosure is appropriate.
- Always ensure the patient has consented to you discussing protected health information in front of friends and family; and
- If you need to notify family and friends of the patient's location or condition and the patient is incapacitated, please use your best professional judgment. Remember to always do what is in the best interest of the patient.

Physical Safeguards

- Safeguard all documentation containing protected health information:
 - Documents containing protected health information may not be removed from your department unless you have received prior approval from your leader;
 - Ensure that all original documentation is sent to the appropriate department(s) or scanning into the electronic medical record;

- Never leave patient charts in areas where they can be viewed by visitors, or others not part of care and treatment;
 - Always dispose of paper documents and labels in the designated bins;
 - Before handing any patient information to a patient, and/or family members, carefully review the documents to ensure you are providing the right information to the right person;
- Baptist Health South Florida employees must always wear their ID badge when on the premises of a Baptist Health facility;
 - Ensure all non-Baptist Health employees working on your unit are properly identified by the facility and have the proper identification prior to reviewing records; know who is in your area and the reason;
 - Tilt or move your computer screens so that information is not visible to the public; and
 - Communicate the concern for privacy to patients and family members in a positive manner such as “to ensure your privacy,” or “in order to protect our patient’s privacy.”

Technical Safeguards

- Protect your credentials, username/passwords and never share them; it may help if you safeguard your passwords the same way you safeguard your personal ATM PIN, or banking information;
- Remember to ALWAYS log off or lock your computer before walking away, even for a few minutes;
- When using a shared computer, you MUST log off or end your session for any clinical applications after accessing patient information;
- When faxing, ALWAYS use a cover sheet and confirm the fax number to ensure a safe transmission; use a secure location for incoming faxes;
- Email communications containing any patient, financial or Baptist Health confidential information should remain within the Baptist Health email system. Ask your leader for further assistance if your job requires you to use email outside the Baptist Health email system;
- No personal electronic mobile devices should be used in patient care areas; (BHSF HR Policy 6400);
- Protected health information may not be stored on any electronic mobile devices such as laptops, USB (thumb drives), external hard drives, cell phones, tablets (iPads) or cloud storage;
- Protected health information may NEVER be shared, posted or otherwise disclosed on social media;
- You may never share, use or disclose protected health information in a text message using your personal phone; and
- You are only permitted to access, use or disclose protected health information to do your job.

