

Safeguards Matrix for Protecting Patient Information

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

Administrative Safeguards

- Lower the tone of your voice when discussing a patient's condition in an open area
- Avoid discussing patient information in open areas whenever possible;
- Listen to your patients and families;
- Remain attentive to time, place and tone;
- Contact Patient and Guest Services or the Privacy Office in the event a patient or employee wishes to exercise one of their privacy rights;
- Verify in the patient's record, with registration/admitting or with the hospital operator to determine if a patient has **opted out** of the facility directory prior to releasing any information;
- Provide the minimum amount of PHI necessary in non treatment situations;
- Use best professional judgment to ensure that the person requesting PHI is treating the patient;
- When receiving a request for information via telephone, verify the requestor is either the patient or someone involved in their care or 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, pass the call through to the patient (provided they have not opted out of the facility directory)
 - If the call comes to the nursing unit, the nurse may ask questions to determine if the caller is involved in the care of the patient, which would allow information to be provided
 - If the request is regarding care or treatment of the patient, ask if the person is the treating physician. You may ask a treating physician to fax a note on their letterhead if necessary
 - If the patient is incapacitated, and there is a health care proxy/surrogate involved in the care or treatment of the patient, you may direct the caller to talk to the health care proxy or designated surrogate
 - If the request is made to Patient Financial Services and is regarding account information, ask for identifiers such as who the caller is, account number, date of service, date of birth, address, phone number on record, etc.
- Remember, if a patient is incapacitated or in emergent situation, please use your best professional judgment when determining whether to notify family and friends of the patient's location or condition. Ask yourself, would the notification be in the best interest of the patient?

Physical Safeguards

- Safeguard the integrity of the paper record;
- Never leave patient charts in areas where they can be viewed by visitors;
- Always dispose of paper documents and labels in the designated bins;
- Documents containing PHI may not be removed from the your department unless you have received prior approval from your leader;
- Before handing any patient information to a patient, and/or their family, 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 BHSF facility;
- 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";
- Tilt or move your computer screens so that information is not visible to the public;
- Keep paper patient information in a secure location out of view of the public;
- Ensure all non BHSF 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;
- If there is any doubt or, in the case of shared rooms, ask the patient's permission before disclosing any PHI.

Technical Safeguards

- Protect your passwords and never share them, it may help if you safeguard your passwords the same way as you safeguard your personal ATM PIN, or banking information;
- Remember to ALWAYS log off 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; as well as using a secure location for incoming faxes;
- Email communications containing any patient, financial or BHSF confidential information should remain within the Baptist Health/Bethesda email system. Ask your Supervisor 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.
- PHI may NEVER be shared, posted or otherwise disclosed on Social Media
- You may never share, use, or disclose PHI in a Text Message using your personal phone.