



**SJH P14 EMPLOYEE MANUAL ADMINSTRATIVE POLICY AND PROCEDURE SJH-HCP**  
**SUBJECT: SJH HIPAA Compliance Policy and Procedures**  
**APPLIES TO: All Employees and volunteers    EFFECTIVE DATE: January 1, 2026**

**POLICY**

It is the policy of SJH to comply with the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and Protected Health Information (PHI) regulations.

**PRACTICE**

SJH has implemented the following policy regarding the use and disclosure of PHI. This policy may be amended from time to time to ensure compliance with HIPAA and other applicable Federal and state law.

The Executive Director has been designated as the St Joseph's Helpers Group Benefit Plan Medical Privacy Officer. The Medical Privacy Officer ensures that all employees having access to PHI have been properly trained, understand these policies and understand the importance of protecting PHI.

The Human Resource Manager has been designated as the DMW Group Benefit Plan Medical Privacy Officer. The Medical Privacy Officer ensures that all employees having access to PHI have been properly trained, understand these policies and understand the importance of protecting PHI.

Protected Health Information is documentation that identifies an individual and relates to the individual's treatment or medical condition. Examples of PHI include, but are not limited to: physician notes that include a diagnosis or work restriction, medical leave of absence applications and Family Medical Leave of Absence documents. Documentation submitted for proof of dependent eligibility is not considered PHI.

**MANAGEMENT RESPONSIBILITY**

All PHI files must be segregated and secure. File drawers containing PHI must be secured and access restricted to trained and authorized personnel. The file cabinet located in the President's office, where PHI is filed, shall be locked. Only authorized employees shall be given access

to PHI records. The Medical Privacy Officer is knowledgeable of all employees having access to PHI.

No employee shall leave work files that contain PHI on his/her desk when the employee is not at his/her desk. No employee shall leave his/her desk when PHI is on his/her computer screen.

Fax transmissions containing PHI are transmitted from the confidential fax located in the office area. Each authorized employee will follow the instructions listed below regarding fax usage:

- Use a confidential fax cover sheet for distributing PHI containing the following statement at the bottom of the facsimile cover page:
- "CONFIDENTIALITY NOTICE" This facsimile message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply facsimile and destroy all copies of the original message."
- Make sure the fax cover sheet contains standard information including date and time of the fax; sender's name, address, telephone number and fax number; the authorized recipient's name, telephone number and fax number; and number of pages transmitted.
- When expecting the arrival of a fax containing PHI, coordinate timing with the sender so you can promptly retrieve the fax.
- Faxes with PHI should be deposited in a secure/confidential place when they are delivered and not, for example, left in an in-box that passersby could see.
- Confirm the accuracy of fax numbers (and security of recipient machines) by calling the intended recipients to double-check the numbers, verify the security of their machines, notify them that your fax is on the way, and request verification of its receipt.
- Verify each outgoing transmission is transmitted successfully.
- In the event of a misdirected fax, ensure improperly faxed documents are either immediately returned or destroyed by the recipient. Document that the fax was misrouted, and take (and document) steps to prevent a recurrence of the error.
- When disposing of PHI in paper form, all paper should be shredded. In no event shall PHI in paper form that has not been shredded be thrown in trashcans or recycling bins

All e-mails that contain PHI must include the following message:

**“CONFIDENTIALITY NOTICE” This e-mail message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply e-mail and destroy all copies of the original message.”**

When disclosing PHI to anyone, you must only disclose the PHI that is the minimum necessary to accomplish the purpose of the disclosure.

Before disclosing PHI by telephone, the Human Resource representative must verify the caller's identification and that the disclosure is in accordance with HIPAA guidelines.

A copy of all PHI received will be retained in accordance with HIPAA requirements. Electronic records, e-mails, etc. may be maintained in password-protected file share folders pending capture by back-up tape; paper records may be stored in a manner consistent with HIPAA document management policies.