hfsc Hospital for Special Care

HIPAA Privacy & Security Education and Acknowledgement

HIPAA is a set of federal laws that requires the health care industry to protect patients' "Protected Health Information" (PHI). HIPAA applies to all PHI, whether the information is stored in paper records or electronic databases (such as lab results). HIPAA even covers PHI that is shared verbally. All health care providers, and those that do business with them, are expected to take patient privacy seriously.

What is PHI?
Protected Health Information (PHI) is information that contains any individual identifier (such as date of birth, medical record number, address, etc.) of a patient. PHI includes more than the medical chart – it includes any other paper or electronic information related to the patient's health care or payment for that care.

We may share medical information internally among caregivers, volunteers, administrative/fiscal departments, and medical staff **on a need to know basis**. Health care providers may also share PHI with outside providers, insurance companies/government payers, and others that need a patient's information for an authorized purpose, such as research, monitoring patient care as in the case of DCF, or reporting elder or child abuse. If you receive a request to release records from an outside party that is not a routine part of your role related to treatment, arranging for payment, or other related business operations, refer the request to the Health Information Management (HIM) Department. HIM will work with the party to obtain proper authorization.

What are my Responsibilities to Protect PHI?

- **Paper records** cannot be left unattended. Paper records should be returned to the proper secure location when no longer needed.

- **Do NOT dispose of paper records containing PHI in normal garbage cans. Use a gray Shred-It bin to dispose of any paper containing PHI that doesn't need to be retained.**

- Unattended offices and workstations need to be locked or otherwise protected from access by people who have no need to access them. Computer screens should not be visible to the public. Documents should not be left on FAX machines, but should be filed or delivered promptly.

- **Protect Electronic PHI** – Desktop computers, laptops and portable devices that have access to our electronic software systems must have password-protection. Do not interfere with or disable password protections – use a strong password (combination of 12 or more letters and symbols). Use screensaver protection or log off when you are away from your computer/portable device. **Do NOT share your password!**

- Follow **role-based access** for both paper records and electronic systems – this means that you access or share only the patient information that is needed to carry out your specific responsibilities, and the recipient receives only the information needed to carry out his/her job responsibilities. "Surfing" patient records out of curiosity is prohibited and may be punishable by criminal charges.

- Always wear and protect your **ID badge** from loss. **NEVER share your badge; it is attached to your identity!**

- Respect **physical safeguards** – areas that are locked or require badge-access are meant for access only by those with an authorized purpose.

HIPAA Privacy & Security Education and Acknowledgement

- **Think before you speak.** PHI includes casual conversations (even if these conversations are for good intentions to help care for the patient or resolve a problem). Be careful to keep voices low, discuss only information that is necessary to provide good patient care or customer service, and use professional judgment and common sense. Do not discuss patient information in public areas such as the cafeteria, waiting areas, or outside of the facility.

- Always immediately contact the HelpDesk (x4791) or email the HIPAA Privacy and Security Officers at privacysecurityoffice@hfsc.org if you suspect malicious activity or that electronic PHI has been accessed by an unauthorized user. After normal business hours and weekends, please use IT On Call process.

- **Honor the rights of patients** to access their own health records – refer such requests to the HIM department.

- A patient's PHI may be shared with individuals (such as family members) that are involved in the patient's care, unless the patient objects or otherwise indicates that he or she does not want a particular person to be involved or receive that medical information.

- Any discussion related to a patient is prohibited on any type of **social media**.

- **Reporting a Breach of PHI -** All employees and workforce members (including students, volunteers and contracted staff) are responsible for reporting a potential HIPAA violation to the HIM Director/HIPAA Privacy Officer (x4822 or at privacysecurityoffice@hfsc.org). Contact the Help Desk **immediately** (x4791) if you suspect a problem with IT systems or data so that immediate action can be taken. After normal business hours and weekends, please use IT On Call process. You will not be reprimanded or otherwise discriminated against for reporting a HIPAA problem. We strongly encourage you to ask your supervisor or any of the contact persons listed below if something does not seem right, even if it seems unimportant!

We are required to publish a **Notice of Privacy Practices** to ensure patients know their rights and understand how their PHI may be used or disclosed. This Notice is posted in the main lobby, on our website at www.hfsc.org, and is given to patients at admission. You may refer patients and their families to this Notice if they ask for information related to their medical records.

All workforce members must abide by specific **HIPAA Policies and Procedures** which are available on the Hospital's intranet. These policies provide detailed instructions and procedures to protect patients' PHI. A copy of the CSC Confidentiality Policy and CSC Password Management Policy are also available from your manager.

I have read, understand and will abide by the above information:

Please Print Name: _____ **Department/Program:** _____

Signature: _____ **Date:** _____

These individuals work together to carry out our HIPAA Program:

Felicia DeDominicis, Compliance Officer/Chief Legal Officer - (860) 827-4807
Stan Jankowski, Security Officer/VP Information Technology/CIO - (860) 827-4830
Karen Lawler, Privacy Officer/Corporate Director Health Information Management– (860) 827-4822

Any of these individuals is available to answer questions or concerns about HIPAA.