Center of Special Care, Inc.

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.). 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 or reporting child abuse. When you receive a request to release records from an outside party that is not a normal part of providing treatment, arranging for payment, or other business operations, and there is no clear **written authorization** to release the PHI, refer the request to the HIM Department or Privacy Officer. We will work with the party to obtain proper authorization.

What are my Responsibilities to Protect PHI?

- **Paper records** cannot be left unattended. Once you are done using a paper chart, return it to the proper location.
- **Shred** paper documents that contain PHI once they are no longer needed. Look for the gray "Shred-it" bins located on patient care units and in other locations.
- Unattended offices and workstations need to be locked or otherwise protected from access by members of the public. 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 6 or more letters and symbols) and do not share it. Use screensaver protection or log off when you are away from your computer/portable device.
- Follow **role-based access** for both paper records and electronic systems – this means that you access or share only the PHI 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 has been punished by criminal charges in other states.
- Always wear and protect your **ID badge** from loss.
- 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 Acknowledgment

- **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 contact the HIPAA Security Officer if you suspect electronic PHI has been lost or accessed by an unauthorized user. We are required to review any loss of electronic PHI and fix the problem to the best of our ability.
- **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, or services you provide to a patient, is prohibited on Facebook or other types 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 or HIPAA Privacy Officer. 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 post 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.

If you need further information, we maintain a set of specific **HIPAA Policies and Procedures** on the Hospital's intranet, which provide detailed instructions and procedures to protect patients' PHI. A copy of the CSC Confidentiality Policy and CSC Password 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.