Confidentiality and Security Agreement

Note: this form is for use with SCLHS associates and workforce members.

I understand that SCL Health System (SCLHS), a SCLHS Care Site or operational unit (the "Company") for which I work, volunteer or provide services manages health information as part of its mission to treat patients. Further, I understand that the Company has a legal and ethical responsibility to safeguard the privacy of all patients and to protect the confidentiality of their patients' health information. Additionally, the Company must assure the confidentiality of its human resources, payroll, fiscal, research, internal reporting, strategic planning information, or any information that contains Social Security numbers, health insurance claim numbers, passwords, PINs, encryption keys, credit card or other financial account numbers (collectively, with patient identifiable health information, "Confidential Information").

In the course of my employment/assignment at the Company, I understand that I may come into the possession of this type of Confidential Information. I will access and use this information only when it is necessary to perform my job related duties in accordance with the Company's Privacy and Security Policies, which are available on the Company intranet (known as The Landing). I further understand that I must sign and comply with this Agreement in order to obtain authorization for access to Confidential Information or Company systems.

General Rules

1. I will act in the best interest of the Company and in accordance with its Code of Conduct at all times during my relationship with the Company.
2. I understand that I should have no expectation of privacy when using Company information systems. The Company may log, access, review, and otherwise utilize information stored on or passing through its systems, including email, in order to manage systems and enforce security.
3. I understand that violation of this Agreement may result in disciplinary action, up to and including termination of employment, suspension, and loss of privileges, and/or termination of authorization to work within the Company, in accordance with the Company's policies.

Protecting Confidential Information

4. I will not disclose or discuss any Confidential Information with others, including friends or family, who do not have a need to know it. I will not take media or documents containing Confidential Information home with me unless specifically authorized to do so as part of my job.
5. I will not publish or disclose any Confidential Information to others using personal email, or to any Internet sites, or through Internet blogs or sites such as Facebook or Twitter. I will only use such communication methods when explicitly authorized to do so in support of Company business and within the permitted uses of Confidential Information as governed by regulations such as HIPAA.
6. I will not in any way divulge, copy, release, sell, loan, alter, or destroy any Confidential Information except as properly authorized. I will only reuse or destroy media in accordance with Company Information Security Standards and Company record retention policy.
7. In the course of treating patients, I may need to orally communicate health information to or about patients. While I understand that my first priority is treating patients, I will take reasonable safeguards to protect conversations from unauthorized listeners. Such safeguards include, but are not limited to: lowering my voice or using private rooms or areas where available.
8. I will not make any unauthorized transmissions, inquiries, modifications, or purgings of Confidential Information.
9. I will not transmit Confidential Information outside the Company network unless I am specifically authorized to do so as part of my job responsibilities. If I do transmit Confidential Information outside of the Company using email or other electronic communication methods, I will ensure that the Information is encrypted according to Company Information Security Standards.

Protecting Patient Information

10. I will treat patient information, whether on paper, spoken, or in the computer, as confidential and protected. I understand that patient information is not to be discussed among co-workers except as required to do my job. I will treat patient information impersonally as part of the day's work. If I use or disclose information other than through prescribed procedures, I understand that disciplinary actions, up to, and including termination of employment may result.
11. I understand there are definite rules regarding the release of health information. Any party requesting a patient's health information should be referred to Release of Information in the Health Information Management department or to a supervisor. If I as a patient want to see my own health information, I understand there are policies governing this access, which are for my own protection. All requests to see my own health information or that of any member of my own family will be referred to the Release of Information area of HIM or to my supervisor.
12. I acknowledge and agree that I am responsible for all entries made and all access using my assigned user id and password, whether made by me or by another if I fail to log out or lock the computer when leaving my workstation. I will not share or attempt to learn another's user id or password and I will not access any applications using a user id and password other than my own. If I believe or suspect my password has been compromised, I will notify STSC and change my password immediately.
13. I acknowledge that my use of the SCLHS computer applications, including the electronic medical record, may be periodically monitored to ensure compliance with this agreement.

Following Appropriate Access

14. I will only access or use systems or devices I am officially authorized to access, and will not demonstrate the operation or function of systems or devices to unauthorized individuals.
15. I will only access software systems to review patient records or Company information when I have a business need to know, as well as any necessary consent. By accessing a patient's record or Company information, I am affirmatively representing to the Company at the time of each access that I have the requisite business need to know and appropriate consent, and the Company may rely on that representation in granting such access to me.

Using Portable Devices and Removable Media

16. I will not copy or store Confidential Information on removable media or portable devices such as laptops,Tablets, cell phones, CDs, thumb drives, external hard drives, etc., unless specifically required to do so by my job. If I do copy or store Confidential Information on removable media, I will encrypt the information while it is on the media according to Company Information Security Standards
17. I understand that any mobile device (Smart phone, Tablet, etc.) that synchronizes company data (*e.g.*, Company email) may contain Confidential Information and as a result, must be protected. Because of this, I understand and agree that the Company has the right to:
    a. Require the use of only encryption capable devices.
    b. Prohibit data synchronization to devices that are not encryption capable or do not support the required security controls.
    c. Implement encryption and apply other necessary security controls (such as an access PIN and automatic locking) on any mobile device that synchronizes company data regardless of it being a Company or personally owned device.
    d. Remotely "wipe" any synchronized device that: has been lost, stolen or belongs to a terminated employee or affiliated partner.
    e. Restrict access to any mobile application that poses a security risk to the Company network.

    See Mobile Security Computing Policy for more information.

Doing My Part – Personal Security

18. I understand that I will be assigned a unique identifier (*e.g.*, User ID) to track my access and use of Confidential Information and that the identifier is associated with my personal data provided as part of the initial and/or periodic credentialing and/or employment verification processes.
19. I will:
    a. Use only my officially assigned User-ID and password.
    b. Use only approved licensed software.
    c. Use a device with virus protection software.
    d. Practice safe Internet usage.
    e. Contact help desk if I receive any suspicious email.
20. I will not:
    a. Disclose passwords, PINs, or access codes.
    b. Use tools or techniques to break/exploit security measures.
    c. Open suspicious emails or emails from untrusted persons.
    d. Connect unauthorized systems or devices to the Company network.
21. I will practice good workstation security measures such as locking the workstation in my absence, using screen savers with activated passwords, positioning screens away from public view, and never connecting unauthorized systems or devices to the SCLHS network, e.g. USB drives.
22. I will immediately notify my manager, Enterprise Security, or the STSC help desk if:
    a. my password has been seen, disclosed, or otherwise compromised;
    b. media with Confidential Information stored on it has been lost or stolen;
    c. I suspect a virus infection on any system;
    d. I am aware of any activity that violates this agreement, privacy and security policies; or
    e. I am aware of any other incident that could possibly have any adverse impact on Confidential Information or Company systems.

Upon Termination

23. I agree that my obligations under this Agreement will continue after termination of my employment, expiration of my contract, or my relationship ceases with the Company.
24. Upon termination, I will immediately return any documents or media containing Confidential Information to the Company.
25. I understand that I have no right to any ownership interest in any Confidential Information accessed or created by me during and in the scope of my relationship with the Company.

By signing this document, I acknowledge that I have read this Agreement and I agree to comply with all the terms and conditions stated above.

I have read or had explained to me, this Confidentiality and Security Agreement, and will support and uphold the confidentiality of Confidential Information including patients' health information, and any other confidential or proprietary information belong to SCL Health System or my Care Site.

Printed Name: _____

Signature: _____

Date: _____