TOTAL CLINICAL PLACEMENT SYSTEM℠

Seeking Best Practices in Clinical Onboarding

Confidentiality and Security Agreement for Students & Faculty

I understand that all my assigned clinical organizations (such as hospitals, clinics, home care, long term care, physician offices, emergency medical services, etc.) provide services and manage health information as part of patient care delivery. Further, I understand that these organizations have a legal and ethical responsibility to safeguard the privacy of all patients and to protect the confidentiality of their patients' health information (PHI) including name, address (other than state and first 3 digits of zip code), birthdate, all specific dates of healthcare delivery (such as admission, discharge, and death dates), telephone and fax numbers, email addresses, social security number, medical record and encounter numbers, health plan numbers, account numbers, certificate/license numbers, medical device identifiers, vehicle identifiers, Internet Universal Resource Locaters (URLs), biometric identifiers such as voice print or finger prints), full face photographs, or any other unique identifier, characteristic, or code unless explicitly permitted by law.

Additionally, these organizations must also assure the confidentiality of their organizational information such as human resources, payroll, fiscal, research, internal reporting, strategic planning information, credentialing, intellectual property, or any information that contains Social Security numbers, health insurance claim numbers, passwords, PINs, encryption keys, credit card or other financial account numbers related to patients and employees.

During my assignment in clinical organizations, I understand that I may come into the possession of patient and organizational confidential information. I will access and use this information only when it is necessary to perform my job-related duties in accordance with the organizations' privacy and security policies. I further understand that I must sign and comply with mandates of this Agreement to obtain authorization for access to confidential patient or organizational information in paper or digital format.

General Rules

1. I will follow the organization's Code of Conduct always during my clinical assignment.
2. I understand that I should have no expectation of privacy when using organizational information systems. Organizational security may track my logins, access and review of information, and any other information stored on or passing through its systems, including email, to manage systems and enforce security.
3. I understand that violation of this Agreement may result in disciplinary action, up to and including suspension from the clinical organization, loss of privileges, and/or termination of affiliation agreements between schools and the clinical organization. Violation may also result in my dismissal from my clinical program of study, in accordance with my school's policies.

Protecting Confidential Information

1. I will not disclose or discuss any confidential information with others, including friends or family, who do not have a need to know it.
2. I will not print or take media or documents containing confidential information home with me unless specifically authorized by the clinical organization to do so as part of my clinical assignment.

3. I will not publish or disclose any confidential information to others using personal email, or to any Internet sites, or through Internet blogs or social media sites such as Facebook or Twitter.
4. 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 organizational information security standards and organizational record retention policy.
5. While treating and caring for patients, I may need to orally communicate health information to or about patients. While I understand that my first priority is patient care, 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.
6. I will not make any unauthorized transmissions, inquiries, modifications, or deletions of confidential information.
7. I will not transmit confidential information outside the organizational network unless I am specifically authorized to do so as part of my clinical assignment responsibilities. If I do transmit confidential information outside of the clinical organization using email or other electronic communication methods, I will ensure that the information is encrypted according to organizational information security standards.

Appropriate Access

1. I understand that I may be assigned a unique identifier (User ID and Password) or security token (such as an ID badge or other related device) to track my access and use of confidential information. This unique identifier is associated with my personal data and provided as part of the initial and/or periodic security credentialing related to clinical assignments.
2. 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.
3. I will only access information systems to review patient records or organizational information when I have a clinical or business need to know, as well as any necessary consent.
4. I will never:
    a. Disclose my personal or organizational passwords, PINs, or access codes.
    b. Allow another individual to use my digital identity (User ID & Password) to access, modify, or delete data and/or use an information system.
    c. Use tools or techniques to break/exploit information technology security measures.
    d. Connect unauthorized systems or devices to the organizational network.
5. I will practice good workstation security measures such as positioning screens away from public view and logging off devices when not in use.
6. I will immediately notify my instructor, preceptor, other facility leader or Privacy Officer if:
    a. My User ID and/or Password has been seen, disclosed, or otherwise compromised;
    b. Media or devices with confidential information stored on it has been lost or stolen;
    c. I am aware of any activity that violates this agreement, privacy and security policies; or
    d. I am aware of any other incident that could possibly have any adverse impact on confidential information or organizational information systems.

Using Mobile Devices, Portable Devices and Removable Media

1. I will only use mobile technology in the healthcare environment that has been approved for use by the facility. The use of personal smart phones, tablets, and laptops must be approved by the host facility and in keeping with facility policy.
2. I will not copy or store confidential information on mobile devices, portable devices or removable media., unless specifically required or allowed to do so by my clinical assignment within the organization. If I do copy or store confidential information on removable media, I will encrypt the information while it is on the media according to organization information security standards.

3. I understand that any mobile device (Tablet, Smart phone, PDA, etc.) that synchronizes data (e.g., organizational email) and may contain confidential information and as a result, must be protected as required by organizational information security standards.

Upon Completion of My Clinical Assignment

1. I agree that my obligations under this Agreement will continue after my clinical assignment ceases with the organization.
2. On the last day of my clinical assignment, I will immediately return any ID badges, documents or media containing confidential information to the organization.
3. 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 clinical assignment with the clinical organization.

Legal Impact of Disclosures

1. I understand that my assigned clinical organization may be obligated to report my unauthorized access and use of PHI or confidential organizational information to federal authorities and local and federal law enforcement officials.
2. I understand that I may face fines, penalties, and even imprisonment should I willfully disclose confidential information from the healthcare setting.
3. I agree to protect, defend and hold harmless, the clinical organization and its affiliates, (and their respective members, trustees, officers, directors, employees and agents) from and against any claim, cause of action, liability, damage, fine, penalty, cost, or expense, including attorneys' fees and costs arising out of or about my unauthorized or prohibited use or disclosure of organizational information systems, PHI, or any other breach of this agreement.