

## EXHIBIT A

### STATEMENT OF RESPONSIBILITY

For and in consideration of the benefit provided the undersigned in the form of experience in a clinical setting at one or more of St. David's Healthcare Ambulatory Surgery Division Surgery Centers ("Surgery Centers"), the undersigned and his/her heirs, successors and/or assigns do hereby covenant and agree to assume all risks and be solely responsible for any injury or loss sustained by the undersigned while participating in the Program operated by: Austin Community College ("School") at Surgery Centers unless such injury or loss arises solely out of Surgery Center's gross negligence or willful misconduct.

\_\_\_\_\_  
Signature of Program Participant/Print Name

\_\_\_\_\_  
Date

\_\_\_\_\_  
Parent or Legal Guardian  
If Program Participant is under 18 / Print Name

\_\_\_\_\_  
Date

## **EXHIBIT B**

### **Confidentiality and Security Agreement**

I understand that the Surgery Center or business entity (the "Surgery Center") for which I work, volunteer or provide services manages health information as part of its mission to treat patients. Further, I understand that the Surgery Center 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 Surgery Center 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 Surgery Center, 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 Surgery Center's Privacy and Security Policies, which are available on the Surgery Center intranet (on the Security Page) and the Internet (under Ethics & Compliance). I further understand that I must sign and comply with this Agreement in order to obtain authorization for access to Confidential Information or Surgery Center systems.

#### **General Rules:**

1. I will act in the best interest of the Surgery Center and in accordance with its Code of Conduct at all times during my relationship with the Surgery Center.
2. I understand that I should have no expectation of privacy when using Surgery Center information systems. The Surgery Center 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 Surgery Center, in accordance with the Surgery Center's policies.

#### **Protecting Confidential Information:**

1. I understand that any Confidential Information, regardless of medium (paper, verbal, electronic, image or any other), is not to be disclosed or discussed with anyone outside those supervising, sponsoring or directly related to the learning activity.
2. 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. Case presentation material will be used in accordance with Surgery Center policies.
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 sites such as Facebook or Twitter. I will only use such communication methods when explicitly authorized to do so in support of Surgery Center business and within the permitted uses of Confidential Information as governed by regulations such as HIPAA.
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 Surgery Center Information Security Standards and Surgery Center record retention policy.

5. 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. Whether at the School or at the Surgery Center, such safeguards include, but are not limited to: lowering my voice or using private rooms or areas (not hallways, cafeterias or elevators) where available.
6. I will not make any unauthorized transmissions, inquiries, modifications, or purgings of Confidential Information. I will not access data on patients for whom I have no responsibilities or a need-to-know the content of the PHI concerning those patients.
7. I will not transmit Confidential Information outside the Surgery Center network unless I am specifically authorized to do so as part of my job responsibilities. If I do transmit Confidential Information outside of the Surgery Center using email or other electronic communication methods, I will ensure that the Information is encrypted according to Surgery Center Information Security Standards.

Following Appropriate Access:

1. 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.
2. I will only access software systems to review patient records or Surgery Center information when I have a business need to know, as well as any necessary consent. By accessing a patient's record or Surgery Center information, I am affirmatively representing to the Surgery Center at the time of each access that I have the requisite business need to know and appropriate consent, and the Surgery Center may rely on that representation in granting such access to me.

Using Portable Devices and Removable Media:

1. I will not copy or store Confidential Information on removable media or portable devices such as laptops, personal digital assistants (PDAs), 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 Surgery Center Information Security Standards
2. I understand that any mobile device (Smart phone, PDA, etc.) that synchronizes Surgery Center data (e.g., Surgery Center email) may contain Confidential Information and as a result, must be protected. Because of this, I understand and agree that the Surgery Center 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 Surgery Center data regardless of it being a Surgery Center 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 Surgery Center network.

Doing My Part – Personal Security:

1. I understand that I will be assigned a unique identifier (e.g., 3-4 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.
2. I will:

- a. Use only my officially assigned User-ID and password (and/or token (e.g., SecurID card)).
  - b. Use only approved licensed software.
  - c. Use a device with virus protection software.
3. I will never:
  - a. Disclose passwords, PINs, or access codes.
  - b. Use tools or techniques to break/exploit security measures.
  - c. Connect unauthorized systems or devices to the Surgery Center network.
4. I will practice good workstation security measures such as locking up diskettes when not in use, using screen savers with activated passwords, positioning screens away from public view.
5. I will immediately notify my manager, Surgery Center Information Security Official (FISO), Director of Information Security Operations (DISO), or Surgery Center or Corporate Client Support Services (CSS) 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 Surgery Center systems.

Upon Termination:

1. 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 Surgery Center.
2. Upon termination, I will immediately return any documents or media containing Confidential Information to the Surgery Center.
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 relationship with the Surgery Center.

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.

Signature	Surgery Center Name and COID	Date
Printed Name	Business Entity Name	