Confidentiality and Security Agreement

I understand that the facility or business entity named below (the "Company") in which or for whom I work, volunteer or provide services, or with whom the entity (*e.g.*, physician practice) for which I work has a relationship (contractual or otherwise) involving the exchange of health information (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, communications, computer systems and management information (collectively, with individually identifiable health information and protected 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 not use company systems to access patient information if it is not necessary to perform my job related duties. This includes NOT accessing my own health information or that of my child or person's for which I am personal representative via the company systems. The Company's Privacy and Security Policies available on the Company 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.

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 in any way divulge, copy, release, sell, loan, alter, or destroy any Confidential Information except as properly authorized.
3. I will not discuss confidential information where others can overhear the conversation, even if the patient's name is not used. I will make every reasonable attempt to refrain from practices that might lend itself to unintended breach of patient confidentiality.
4. I will not make any unauthorized transmissions, inquiries, modifications, or purgings of Confidential Information.
5. 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.
6. Upon termination, I will immediately return any documents or media containing Confidential Information to the Company.
7. I understand that I have no right to any ownership interest in any information accessed or created by me during my relationship with the Company.
8. 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.
9. 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.
10. 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.
11. 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 e-mail, in order to manage systems and enforce security.
12. I will practice good workstation security measures such as locking up electronic media devices when not in use, using screen savers with activated passwords appropriately, and position screens away from public view.
13. I will practice secure electronic communications by transmitting Confidential Information only to authorized entities, in accordance with approved security standards.
14. 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.
15. I will never:
    d. Share/disclose user-IDs, passwords or tokens.
    e. Use tools or techniques to break/exploit security measures.
    f. Connect to unauthorized networks through the systems or devices.
16. I will notify my manager, Local Security Coordinator (LSC), or appropriate Information Services person if my password has been seen, disclosed, or otherwise compromised, and will report activity that violates this agreement, privacy and security policies, or any other incident that could have any adverse impact on Confidential Information.

The following statements apply to physicians using any Company systems containing patient identifiable health information (e.g. HMS, Meditech, eCW):

17. 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.
18. I will accept full responsibility for the actions of my employees who may access the Company software systems and Confidential Information.
19. I have no intention of varying the volume or value of referrals I make to the Company in exchange for Internet access service or for access to any other Company information.
20. I have not agreed, in writing or otherwise, to accept Internet access in exchange for the referral to the Company of any patients or other business.
21. I understand that the Company may decide at any time without notice to no longer provide access to any systems to physicians on the medical staff unless other contracts or agreements state otherwise. I understand that if I am no longer a member of the facility's medical staff, I may no longer use the facility's equipment to access the Internet.

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

Employee/Consultant/Vendor/Office Staff/Physician Signature	Facility Name and COID HighPoint Health System 16750\16751\16753	Date
Employee/Consultant/Vendor/Office Staff/Physician Printed Name	Business Entity Name (Your facility or office name)	