



| | | | |
|---|---|--|---|
| | <u>Effective Date</u> | | |
| | July 2007 | | |
| | <u>Number</u> HP 016 | <u>Replaces Policy</u> NEW | |
| <u>Title</u> Security Agreement | <u>Date Revised</u> July 2007 | <u>Date Reviewed</u> | <u>Next Scheduled Review Date</u> July 2010 |
| <u>Signature</u> _____ | <u>Scope of Responsibility</u> HIPAA/Compliance | | |
| Chief Privacy Officer | | | |

PURPOSE: To provide awareness of the importance of information security and confidentiality and to authorize and require agreements with individuals and external entities to protect IMH information resources, including confidential patient information.

POLICY:

1. Information Confidentiality and Security Agreements with Individuals

- a. All IMH Team Members and other individuals granted access to IMH information systems must sign and abide by the IMH Confidentiality and Security Agreement (Agreement). The Agreement acknowledges specific responsibilities the individual has in relation to information security and the protection of sensitive information, including confidential patient information, from unauthorized disclosure.
- b. A physician practice, vendor, or other external entity may make and shall enforce such Agreements on behalf of employees working off-site (e.g., contracted transcription service, electronic claims submissions support contractor, physician office practice), if stipulated in IMH's contract with the external entity (see 2. below). Each individual working on IMH premises accessing IMH and/or patient information must sign an Agreement.
- c. The HIPAA Team reviews recommended changes to the Agreement, publishes, and maintains the Agreement. The Agreement is an official IMH document and may not be altered in any manner without prior approval from the HIPAA Team.

2. Contracts with Business Partners

- a. Relationships with an external entity involving access to IMH information systems or the exchange, transmission, or use of sensitive IMH information requires a formal contract including provisions to protect the confidentiality and security of the information and/or systems.
- b. IMH Administration is authorized to approve access to IMH information systems and/or the disclosure of sensitive IMH information after the execution of the Contract.
- c. The Contract must include provisions governing the entity's information security policies and practices, as well as requirements to support IMH compliance with regulatory requirements.

3. Contracts for IT Services - All contracts for services will include appropriate standard security language approved by IMH and MBT.

4. Sanctions - Violations of this policy could lead to disciplinary measures up to and including termination of employment or business relationship. Violations may be reported to the Chief Privacy Officer at extension 5609, the Chief Compliance Officer at extension 6684 or the Compliance Hotline at 1-800-273-8452.

5. Policy Exceptions - Exceptions to Security Policy shall be submitted to the HIPAA Team for review and approval.

6. PROCEDURE:

- a. The Confidentiality & Security Agreement form is posted and maintained as an attachment to this policy.
- b. Each IMH employee must sign the Agreement at the time of employment. The completed Agreement will be maintained in the individual's personnel folder.
- c. Each physician and allied health professional must sign the Agreement at the time he or she is initially appointed to IMH's medical staff. Completed Agreements will be maintained in the individual's credentials file.
- d. Each volunteer must sign the agreement before beginning his or her service. The agreement signature process can be completed during Orientation. The completed agreement will be maintained with IMH's records of the volunteer's service.

Policy: Security Agreement

Policy Number: HP 016

- e. Physician office staff must sign the Agreement at the time information access is granted. Completed Agreements must be maintained in a central location by the Medical Staff Coordinator.

- f. Representatives of vendors and other external entities must sign the Agreement at the time information access is granted. Completed agreements must be maintained in the individual contract folder by the Contract Coordinator.

CONFIDENTIALITY AND SECURITY AGREEMENT

I understand that Ivins Memorial Hospital (IMH) and its associated business entity, Medicine Bow Technologies (MBT), for whom I work, volunteer or provide services, or for which the entity (e.g. physician practice) for which I work has a relationship (contractual or otherwise) involving the exchange of privileged health information (PHI), has a legal and ethical responsibility to safeguard the privacy of all patients and to protect the confidentiality of their patients' health information. Additionally, IMH must assure the confidentiality of its Human Resources, payroll, fiscal, research, internal reporting, strategic planning, communications, computer systems and management information (collectively, with patient identifiable health information, "Confidential Information").

In the course of my employment / assignment at IMH/MBT, 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 IMH's Privacy and Security Policies, which are available on the IMH intranet. 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. It is not acceptable to discuss Confidential Information even if the patient's name is not used.
 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 IMH/MBT.
 6. Upon termination, I will immediately return any documents or media containing Confidential Information to IMH/MBT.
 7. I understand that I have no right to any ownership interest in any information accessed or created by me during my relationship with IMH/MBT.
 8. I will act in the best interest of IMH/MBT and in accordance with its Code of Conduct at all times during my relationship with IMH/MBT.
 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 IMH/MBT, in accordance with IMH'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 IMH/MBT information systems. The facility 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 diskettes 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 .
 - b. Use only approved licensed software.
 - c. Use a device with virus protection software.
 15. I will never:
 - a. Share/disclose user-IDs or passwords.
 - b. Use tools or techniques to break/exploit security measures.
 - c. Connect to unauthorized networks through the systems or devices.
 16. I will notify my manager, The Chief Privacy Officer, or the Information Technology Security Officer 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 IMH systems containing patient identifiable health information (e.g. CPCS/Meditech):**
17. I will only access software systems to review patient records when I have that patient's consent to do so. By accessing a patient's record, I am affirmatively representing to IMH at the time of each access that I have the requisite patient consent to do so, and IMH may rely on that representation in granting such access to me.
 18. I will insure that only appropriate personnel in my office will access IMH's software systems and Confidential Information and I will annually train such personnel on issues related to patient confidentiality and access.
 19. I will accept full responsibility for the actions of my employees who may access IMH's software systems and Confidential Information.
- Signing this document, I acknowledge that I have read this Agreement and I agree to comply with all the terms and conditions stated above.

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.

Policy: Security Agreement

Policy Number: HP 016

3. I will not discuss Confidential Information where others can overhear the conversation. It is not acceptable to discuss Confidential Information even if the patient's name is not used.
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 IMH/MBT.
6. Upon termination, I will immediately return any documents or media containing Confidential Information to IMH/MBT.
7. I understand that I have no right to any ownership interest in any information accessed or created by me during my relationship with IMH/MBT.
8. I will act in the best interest of IMH/MBT and in accordance with its Code of Conduct at all times during my relationship with IMH/MBT.
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 IMH/MBT, in accordance with IMH'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 IMH/MBT information systems. The facility 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 diskettes 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.
 - b. Use only approved licensed software.
 - c. Use a device with virus protection software.
15. I will never:
 - a. Share/disclose user-IDs or passwords.
 - b. Use tools or techniques to break/exploit security measures.
 - c. Connect to unauthorized networks through the systems or devices.
16. I will notify my manager, the Chief Privacy Officer, or the Information Technology Security Officer 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 IMH systems containing patient identifiable health information (e.g. CPCS/Meditech):

17. I will only access software systems to review patient records when I have that patient's consent to do so. By accessing a patient's record, I am affirmatively representing to IMH at the time of each access that I have the requisite patient consent to do so, and IMH may rely on that representation in granting such access to me.
18. I will insure that only appropriate personnel in my office will access IMH's software systems and Confidential Information and I will annually train such personnel on issues related to patient confidentiality and access.
19. I will accept full responsibility for the actions of my employees who may access IMH's software systems and Confidential Information.