

## Information Access Security and Patient Confidentiality Agreement

### The undersigned agrees and commits to the following statement:

Tallahassee Memorial HealthCare, Inc. ("TMH") respects the confidentiality of our patients' medical information. We believe that patients have the right to have their medical information used appropriately for their care and to expect that caregivers will carefully protect the privacy of that information. The HIPAA Privacy and Security Standards, HITECH Act of 2009, Florida Statutes, and the related TMH Privacy and Security policies and procedures ("P&P's") (on the TMH Intranet) place certain restrictions on the processing, use, and disclosure of individuals' and patients' Protected Health Information ("PHI") and other Confidential Information. During the performance of duties, colleagues (employees), students, volunteers, and certain contract staff may have access to and/or be involved in the processing of Confidential Information, including but not limited to: patient PHI and electronic PHI ("ePHI") to include medical records; indexes of medical information; patient demographics, billing, and appointment history; confidential communications for diagnosis and treatment purposes; Human Resources ("HR") records; and other business, financial, corporate and proprietary information. TMH expects that all individuals who have been granted authorized access to Confidential Information will do so in a manner consistent with regulatory requirements, laws, and established TMH P&P's related to the transmission, use, and disclosure of Confidential Information and the security of TMH information systems and data.

### I understand and agree to adhere to the following:

1. All information related to a patient's past, present, or future healthcare and treatment in any facility, department, or unit of TMH is considered "protected health information" (PHI). This information can only be accessed and shared with those who have a "need to know" while performing duties related to treatment, payment, and healthcare operations ("TPO"). While performing my duties, I may have access to information concerning all TMH patients; however, only the minimal amount of information necessary to adequately perform my specific job responsibilities will be accessed.
2. No information concerning TMH patients will be used, disclosed, or discussed outside of TMH unless specifically authorized by the patient, permitted by the HIPAA Privacy Rule, or required by law. If I have any questions about the appropriateness of disclosure, prior to disclosure, I will make inquiry to the appropriate supervisor or the HIPAA Privacy or HIPAA/Information Security Officer.
3. Patient information will not be discussed openly in a public environment, such as elevators, corridors, hallways, cafeterias, or at any other location where others may overhear comments. Discussions necessary for the care of the patient will be conducted as discreetly as possible.
4. Only authorized personnel may release copies of the patient's medical record and only in accordance with TMH policy and consistent with state and federal regulations. Patient information, such as name, date of birth, address, and/or social security number, will not be recorded on any documents which are removed from my work area or from the facility. Patient information may not be photocopied for personal or school-related use.
5. Telephone inquiries concerning a patient's condition must be referred to individuals who are authorized to respond to such inquiries. Disclosure of PHI over the telephone will be done in a manner that reasonably ensures protection of the information, to the greatest extent practicable, without interfering with the intended purpose of the communication.
6. Unless subpoenaed or court ordered to do so, I shall not assist any attorney, plaintiff or prospective plaintiff nor provide testimony against TMH, regardless of whether such testimony is paid or voluntary, relative to litigation in which TMH is or may become involved.
7. I will be the sole user of my user identification code (user ID) and password in connection with my authorized access to information. I will take all necessary steps to prevent anyone from gaining knowledge or use of my password. I understand that my password is recognized as my personal signature on each computer function. For security purposes, I understand that if my account is inactive for 90 days or more, it will be disabled until notice is given by the authorized user or supervisor to reactivate.
8. Computer passwords will be kept confidential. Inappropriate use of or failure to maintain the confidentiality of any computer password will be cause for disciplinary action.
9. I am responsible and accountable for all entries made and all records retrieved under my username and password.
10. Under no circumstances will I utilize TMH information or communication resources for personal financial benefit or gain; to solicit or distribute personal goods or services; or, for any other purpose harmful to TMH. I understand that inappropriate (non-business) use of these resources that negatively impact my performance may result in disciplinary action.
11. I acknowledge that e-mail communications, computer systems, and any other information resources are not private and may be monitored by TMH to ensure that there is no unauthorized use of the company's systems. I also acknowledge that use of TMH information and communications resources for illegal purposes or in violation of the law; or, to convey offensive, harassing, vulgar, obscene or threatening information, including disparagement of others based on race, national origin,

## Information Access Security and Patient Confidentiality Agreement

marital status, sex, sexual orientation, age, disability, pregnancy, religious or political beliefs, or any other characteristic protected under federal, state or local law, is strictly prohibited and can result in termination.

12. I will respect laws regarding copyrighted software and not make unauthorized copies of software, even when the software is not physically protected against copying.
13. I acknowledge that my obligations and responsibilities continue after termination of employment, contract or affiliation with TMH.
14. I will ensure that Anti-virus software is installed or removed only by authorized Information Technology ("IT") department staff on any TMH computer or information system. I understand that I am not authorized to bypass this step.
15. I will sign off and/or physically secure a terminal or computer when leaving it unattended in an area open to unauthorized individuals.
16. I will not load copyrighted software, shareware, and/or freeware (software programs that are not protected by copyright) on any TMH computer without prior approval by the IT department.
17. I will protect terminals, network devices and personal computers from theft and physical damage.
18. If it is my responsibility to correct colleagues' time in the time and attendance system, I must follow hospital policies set forth in the TMH HR P&P's (on TMH Intranet). I understand that failure to pay colleagues in accordance with hospital policy and procedure can and will result in disciplinary action up to and including termination.
19. I will follow the process established for patients to access patient records and accounts, and I will not access patient records or accounts for myself or family.
20. I will protect from loss or theft any TMH mobile device, to include laptops, PDAs, or storage medium, (such as, CDs, thumb drives, USB sticks) assigned to me or in my possession. Should such a loss or theft occur, I will immediately report it to the TMH IT Service Desk at 431-5272 or servicedesk@tmh.org and to TMH Security.
21. I will report any violation of the TMH HIPAA/Information Security or TMH HIPAA Privacy P&P's to my supervisor, the TMH Security Officer, or the TMH Privacy Officer.
22. I understand that violations of security and/or privacy rules and P&P's, whether due to carelessness or malicious intent, are causes for appropriate corrective action in accordance with HR P&P's, up to and including discharge.
23. I understand this agreement will not expire and will be reviewed and signed annually.
  - All TMH colleagues' access is subject to be renewed at their annual review to re-enforce TMH's HIPAA Privacy and Security P&P's (on TMH Intranet).
  - All Non-TMH employees must review and sign this Confidentiality Agreement prior to acquiring TMH system access and annually thereafter or at the beginning of a new engagement and/or contract when a break in continuous service is greater than two months, or as determined by the appropriate manager.
24. I acknowledge my access privileges are subject to periodic review, revision, renewal, or revocation and that I am obligated to maintain the confidentiality of any new information or systems I am granted access to in order to perform my specific job responsibilities.

\_\_\_\_\_  
Colleague Name (print)

\_\_\_\_\_  
Department

\_\_\_\_\_  
Signature

\_\_\_\_\_  
I.D. #

\_\_\_\_\_  
Company or School Affiliation (if applicable)

\_\_\_\_\_  
Date