HIPAA Privacy and Security

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is an important federal law that affects how you and the University of Florida College of Medicine (COM) must handle confidential patient health information. For the most current University policies related to HIPAA, please see the University Privacy Office web site at http://privacy.health.ufl.edu/.

1. Scope of HIPAA. HIPAA is a broad federal statute that addresses numerous health care related topics. Of the various titles in HIPAA, the Administrative Simplification title of HIPAA has the greatest impact on the COM and Shands, its affiliated hospital in Jacksonville. One of the primary goals of the Administrative Simplification title of HIPAA is to protect the security and confidentiality of health information. Four (4) primary sets of federal regulations have been drafted to further the goals of the Administrative Simplification title:
    a. Electronic Transactions and Code Sets Rules on and Identifier Rules for Employers, Health Plans and Individuals - both of these regulations require that certain standard electronic formats be used when sending health related billing claims. Each regulation is intended to streamline administrative and financial health care transactions conducted electronically.
    b. Security Rules – these regulations contain administrative, procedural and technical standards that healthcare entities must comply with in order to protect the security of individually identifiable “electronic” health information. Under the Security Rules, a healthcare entity is required to assess its own security needs and risks and devise and implement appropriate security measures to address these risks; the Security Rules were effective in April of 2005.
    c. Privacy Rules – the Privacy Rules (effective 4/14/03) require healthcare entities to implement significant measures to protect the confidentiality and privacy of patient medical information.
    d. National Provider Identifiers. A National Provider Identifier (NPI) is a unique identifier that is required of all providers effective May 2007. The Office of Educational Affairs will obtain an NPI on your behalf. This number will be used to identify you in billing transactions. You will have this number throughout your career.

For most UF, UFJHI and UFJPI employees, the implementation of the Electronic Transactions and Code Set Rules and the Identifier Rules will remain transparent since these changes are largely technical changes to network and computer systems. The Security and Privacy Rules however, will touch virtually everyone on the Jacksonville campus.

Important aspects of both the Privacy and Security Rules: The remainder of this section addresses your compliance obligations with respect to both the Privacy and Security Rules.

2. Who Must Comply with the Privacy and Security Rules? The Privacy and Security Rules apply to three types of “covered entities”: health care providers, health plans, and health care clearinghouses. The COM is considered a provider and is therefore required to comply with both the Privacy and Security Rules. Both the University of Florida and Shands JAX have separate and independent compliance obligations. Additionally, both Jacksonville support organizations (UFJHI & UFJPI) are also required to comply with the Privacy and Security Rules. In fact, the University of Florida, UFJHI and UFJPI have elected under the Privacy and Security Rules to be treated as one entity for compliance purposes.
3. What do the Privacy Rules apply to? – The fundamental premise under the Privacy Rules is to protect “Patient Health Information”. “Patient Health information” is broadly defined in the Privacy Rules to include any oral, written or electronic individually identifiable information relating to (i) the past, present, or future physical or mental health of an individual; (ii) the provision of health care to the individual; or (iii) the

payment for health care. On our JAX-campus this means that virtually all patient related information is subject to the protections of the Privacy Rules. Consequently, it is vital that you fully comprehend your obligations to protect this information in accordance with our HIPAA Policies and Procedures.

4. What do the Security Rules apply to? The Security Rules apply to patient health information in electronic format. However, the UF HSC has elected to apply its security policies and standards to other information beyond just patient information. There are four categories of information subject to the UF HSC Security Policies that include: restricted information, critical information, operational information and unrestricted information. The only information in the restricted category, which requires the greatest protection, is patient information and certain types of employee information such as social security numbers. For more information on the other categories of information refer to UF HSC Security Standard GP-0001 http://security.health.ufl.edu/policies/index.shtml
5. Deadlines – Compliance with the Privacy Regulations was required on April 14, 2003. The Security Regulations were effective in April of 2005.
6. Compliance – In order to assist you in complying with the Privacy and Security Rules, below is a summary of many of the important requirements set forth in our HIPAA Policies and Procedures:
   a. Privacy Policies and Procedures. The COM has developed comprehensive policies and procedures to implement the requirements under the Privacy Rules. You are responsible for conducting your actions in accordance with these Policies. You are responsible for familiarizing yourself with these policies and understanding what is required of you when you use, access or release/disclose patient health information. Should you fail to abide by the COM HIPAA Policies and Procedures, disciplinary action may be brought against you by UF, including dismissal. Additionally, you may be sued personally by a patient whose privacy rights you have breached. A copy of the full text of the UF HIPAA Policies and Procedures may be found on-line at http://privacy.health.ufl.edu/policies/.
   b. Security Policies and Standards. The UF Health Science Center (UF HSC) has sponsored the development of comprehensive security policies and standards. These policies and standards may be referenced at the following web site: http://security.health.ufl.edu/. These policies include specific requirements concerning the use of desktop computers as well as portable computing devices such as PDAs and laptop computers. You are responsible for complying with these policies whenever you use a desktop or portable computing device.
   c. Access to /Use and Disclosure of Patient Health Information. You may use patient health information for treatment purposes, payment support purposes and for our internal operations (such as quality assurance and quality improvement activities) however, for all other purposes, you will either need the patient's express written permission to use the health information or an applicable exception must apply. You must refer to the UF HIPAA "*Permitted Uses and Disclosures*" Policy to determine whether and to what extent you may have access to, use or disclose patient health information.
   d. Research. If you conduct research on this campus (which would involve using/ accessing or disclosing any medical records of any patient of ours) you will need to coordinate your research activities with the Jacksonville Institutional Review Board (JAX IRB). Researchers have no right to use or even access a patient's health information without first either obtaining the patient's written permission or the approval of the JAX IRB. You may obtain further information on the JAX IRB and its requirements, functions, processes and forms at http://www.hscj.ufl.edu/irb/

e. Patient Rights. In order to protect patient privacy rights, the Privacy Rules provide patients with a multitude of new patient rights**.** These rights include the right to request an amendment to their medical records; the right to access and review their original medical records in our facility; the right to require us to provide them with a written accounting of each entity to whom we have disclosed their health information to in the last six years as well as many other new rights. Consequently, while you may not be responsible for overseeing the process by which these rights are administered, you should nonetheless be aware of these rights as they may indirectly affect your role and responsibilities on this campus. You should review the "*Patient Rights*" UF HIPAA Policies for further information on patient rights (See http://privacy.health.ufl.edu/policies/hipaamanual/operational.shtml).

f. Security. The UF HSC Security Policies and Standards require that we have in place significant technical and physical safeguards to protect our medical records and electronic systems which contain patient information. These security requirements have required us in conjunction with Shands to enforce strict security measures with respect to log-on passwords, system auditing, e-mailing, faxing, physical locks and physical access to electronic devices containing PHI, as well as strict policies regarding the use of desktop computers and portable computing devices.. Specifically, in accordance with the UF HIPAA Privacy and HSC Security policies you must comply with the following:

   i. Passwords. You may not share or loan log-on passwords to any computer application on the JAX-Campus with anyone. You will be responsible for any unauthorized access to our electronic systems with your password; your password to the network and any application you access should be a strong password. An example of a weak password is "james1", a strong password is "j3flk23kl29".

   ii. Identification. You must at all times wear your security/ID badge while on campus.

   iii. Use of Laptop computers. If you use a laptop computer for the storage of patient information, you will need to have a strong password installed to access the computer as well as to the application where the patient information is stored AND you must encrypt the patient information AND you must have written authorization from your Department Chair to have patient information on your portable computing device. If you store patient information on your portable computing device, you should only store the minimum amount of information necessary. In addition, you should purge and delete any information as soon as it is no longer useful. Please refer to UF Technical Security Policy TS 0010 for details: https://security.health.ufl.edu/isa_ism/policies.shtml

   iv. Reporting lost computing devices. If you lose a computing device with patient information stored on it, you must immediately inform your supervisor as well as the Jacksonville HIPAA Office and the Jacksonville Unit ISM – who is also the UFJP Director of IS.

   v. Use of Desktop Computers and your physical workstation. You must ensure the physical security of your desktop computer and workstation is at all times maintained. This means that you need to make sure that if your desktop is in your office that you lock you door when you leave your office.

   vi. Saving patient information on your computer. You should not save any patient information to the C: Drive of your desktop computer. All patient information should be saved to a secure server.

vii. E-mail. In the event you e-mail patient health information to any party for any reason – you will be required to ensure that the e-mail is either to another person with a "@jax.ufl.edu" e-mail address or that the e-mail is encrypted. Patients who wish to communicate with you via e-mail must sign an authorization allowing you to communicate with them via e-mail. (See UF HIPAA "*E-Mail*" Policy - http://privacy.health.ufl.edu/policies/hipaamanual/operational.shtml)

viii. Access to Computer Systems. In an effort to monitor access to electronic medical information Shands, UF and UFJHI/PI will be auditing their computer systems. Consequently, any time you access any patient information on a computer system on the JAX –Campus, you should ensure that you have the right to access that information for an appropriate business-related purpose (i.e., treatment of the patient, health care operations – such as quality assurance, etc. . .) (See the UF HIPAA "*Permitted Uses and Disclosures*" Policy). If you are inappropriately accessing patient information without a proper business need-to-know you will be subject to discipline up to and including termination. This means that you should at no times access your own personal patient information in our patient computer systems or that of your neighbor, spouse, friend, relative, etc. . . . unless you are the treating provider or you have a business need-to-know for that information.

ix. Physical Locks. In the event you have access to a secure area with a key or through an access code, you may not provide your key or code to any other individuals. You will be held responsible for any unauthorized access by an individual who uses your key or code.

x. Faxing. If you are faxing patient health information to any other party you will need to take appropriate steps to make sure that the information is properly sent to the appropriate party. (Refer to UF HIPAA "*Fax*" Policy http://privacy.health.ufl.edu/policies/hipaamanual/operational.shtml).

xi. Verification of Identity. Any time you speak (in person or over the phone) with a patient, patient representative, insurer, community physician or any other party about patient health information and you do not know the party to whom you are speaking personally, you will need to verify the identity of the person to whom you are speaking. Verification of the identity of the person to whom you are speaking may only mean verifying that they know the patient's date of birth, last date of service, social security number, etc. . . . You should refer to the UF HIPAA "*Verification of Identity*" Policy for additional information.

7. Penalties - There are serious civil and criminal penalties for HIPAA noncompliance. A violation of the HIPAA Privacy and Security Regulations can result in fines up to $250,000 and can also result in imprisonment for up to 10 years. Additionally, you can be sued personally for violating a patient's privacy. Other risks of noncompliance include increased exposure to lawsuits for breach of confidentiality, negative publicity, potential loss of accreditation (i.e., ACGME, JCAHO), HHS audits/investigations and harm to business interests. Additionally, committing a violation may result in your termination of employment and/or dismissal.

8. Reporting Violations. In the event you suspect or have knowledge of a violation by any member of our workforce including another faculty member, resident, staff member or other employee, you should immediately report the violation to the UFJHI/PI HIPAA Compliance Manager. You may contact the UFJHI/PI HIPAA Compliance Manager at

(904) 244-6229 or if you wish to file a complaint anonymously, you may call 1- (877) 876-4472.

9. Questions. Should you have any questions concerning your compliance obligations with the Privacy Rules or Security Rules, you may contact the UFJHI/PI HIPAA Compliance Manager at (904) 244-6229.
10. What Should You Do To Comply With the US Security and Privacy Regulations? You should make sure that you understand to what extent the scope of your employment here requires compliance with certain privacy and security related policies and procedures. If you have access to, use or disclose patient health information for any purpose you will need to be familiar with several important policies on the protection and security of patient information. Please make sure you discuss with your supervisor whether and to what extent you need to become familiar with our privacy and security policies to protect patient information.