THE HIPAA PRIVACY and SECURITY REGULATIONS in a NUTSHELL

In 1996 Congress passed a law called the Health Insurance Portability and Accountability Act (HIPAA). That law required a set of federal regulations on Privacy and Security.

The Privacy Regulations
These regulations require all "Covered Entities (CEs) to give their patients a Notice of Privacy Practices telling how a patient's confidential health; billing and demographic information (called "Protected Health Information" or PHI) is protected by the Covered Entity. A "Covered Entity" is a health plan (such as an HMO), a clearinghouse (like WebMD), or a health care provider who submits bills electronically. Providers include private practitioners like doctors and dentists as well as hospitals and other health care facilities. The University of Michigan Health System and its providers are a Covered Entity.

Once the CE provides the Notice of Privacy Practices, it asks the patient to acknowledge receipt. The CE can then provide treatment, bill the patient for the treatment and perform core operations (such as infection control, quality assurance, sending reminder letters, accreditation, teaching, etc.). If a practitioner wants to do research involving the patient or the patient's records, the patient needs to authorize this use.

The Privacy regulation is intended to increase the patient's control over who can see or use the patient's PHI. So, while CEs can use or disclose the PHI for treatment, billing, and core operations, they need a written authorization for most other purposes (however, a patient can verbally tell a health care professional which of the patient's family members the provider may talk to about the patient's care, and inpatients in a facility can simply say whether they want to be listed in the facility directory).

Where a disclosure is required by law, for example reporting child abuse and certain diseases to public health authorities, no authorization is necessary.

The regulations give patients the right to access their PHI, request amendments to anything they feel is not correct, and obtain information about some disclosures made without their authorization. They also require CEs to be careful how they handle PHI: for example, we have to use it only for permissible purposes, provide only the minimum necessary information, verify the identity and authority of people who ask to see it, and take security precautions to protect it. If we fail to do these things, we can be subject to civil and criminal penalties.

The Security Regulations
As you will not have access to UMHS information systems during your visit, we are not required to educate you on security processes. However, should you observe any information security problems (including physical security of information systems or storage media), please report them to your host or to the UMHS Compliance Office at 615-4400

What Does UMHS Do?
Our patients' privacy is critically important to us. We have a Privacy Office that works to ensure compliance with the regulation. It can be contacted at hipaa-questions@med.umich.edu. We have a Notice of Privacy Practices posted in various locations throughout the Health System and on the Web at www.med.umich.edu/hipaa. Educational materials are available at http://www.med.umich.edu/u/hipaa (a different website, accessible only from within our network) if you would like to learn more. We have detailed policies and procedures setting forth our approach to protection of our patients' information. If these affect your visit at UMHS, they will be provided to you and you will be required to follow them. We require anyone who has access to our patients' PHI to sign a Confidentiality and Security Agreement. We also take appropriate disciplinary action if anyone wrongly uses or discloses PHI.

Why Are We Telling You This?
You must be educated before you can have access to any PHI so you can understand how important privacy is to us and to our patients. You must agree to strictly follow the regulations and our policies. If you are uncertain about what to do you must seek guidance before you look at or gain access to any PHI. If you have any questions, please talk to your host or supervisor, look at the website, or contact the Privacy Officer.

I agree to fully comply with the regulations outlined above.

Name (Print): _____ Signature_____ Date:_____

Clinical Department Visited: _____