

**University Medical Center
Confidentiality Agreement
March 2003**

I acknowledge:

- ◆ All information contained within a patient's medical record is considered confidential (AR S 12-2291 et seq. and CFR 160 & 164). Patient specific clinical data contained in department or hospital computer or dictation systems or output from clinical and business information systems are likewise confidential.
- ◆ Aggregate data output by various parameters (diagnosis, procedure, service, specialty, physician, etc.) is also confidential.
- ◆ My password to any department or hospital computer system is confidential.
- ◆ Corporate and workforce data that is proprietary or privileged is confidential.

I agree:

I will protect to the fullest extent required by all state and federal laws and hospital policy the patient's right to confidentiality of all medical and personal information, UMC workforce's right to privacy, and UMC's right to confidentiality of proprietary or privileged corporate data.

I will not access for the purpose of inquiry, manipulation, deletion or alteration any data outside the scope of my responsibility. I will not use any data within my authorized access for any purpose outside the scope of my responsibility.

I will not discuss confidential patient, workforce, or corporate information in public areas, such as the cafeteria, hallways, or elevators, within the hearing of persons not entitled to hear the information.

I will not print, copy, or fax reports unless it is within the defined scope of my responsibility. I agree to protect patient, workforce, and corporate confidentiality by using care in handling printed reports or report copies and appropriately destroying non-permanent paper copies.

I will not intentionally damage, corrupt, or inappropriately delete data or computer programs or copy data or programs to other devices or media without authorization. I will not load software onto any UMC or UMC network-connected device without Information Systems' authorization and assistance will not disclose my password to anyone nor allow anyone to use my password after I have signed onto a system. I will not attempt to learn other user's passwords and will not use passwords other than my own. If my password becomes known or is lost, I will notify my supervisor immediately. I will notify my immediate supervisor or UMC Security upon witnessing any unauthorized persons accessing, tampering with, or removing any computer hardware or software.

I understand that improper disclosure of confidential patient, workforce, or corporate information, whether verbally or from a paper-based or a computer-based record, or tampering with any computer hardware or software can result in immediate dismissal without notice.

I acknowledge that any violation of any part of the above agreement may result in termination of medical record and/or computer access privileges or denial of physical access to UMC facilities and I may be subject to disciplinary action up to and including termination of my employment and/or legal action.

I understand that UMC has a legal and ethical responsibility to safeguard the privacy of all patients and to protect the confidentiality of their health information.

I am aware that as part of UMC's responsibilities, UMC provides privacy training to its staff.

I acknowledge that I have received privacy training provided by UMC.

I certify that I am familiar with UMC's policies and procedures regarding the privacy of health information and I agree to follow those policies and procedures.

I agree to attend future privacy training sessions, as and when requested by UMC.

I further agree that I will report promptly any known or suspected violations of UMC's policies and procedures regarding the privacy of health information to the UMC's Privacy Officer or to the UMC Alertline.

Printed Name: _____

School _____

**HIPAA Privacy
Session I**

Signature: _____

Date: _____