Attachment C

UNIVERSITY OF ROCHESTER
Strong Memorial Hospital

Patient's Rights

The New York State Department of Health requires that a copy of the Patient's Rights be posted in designated areas, and given to patients upon admission, or when receiving outpatient or emergency care. Hospitals make this information available in different languages, Braille, and in a signed format.

A designated person must meet with the patient about his/her rights, and document that the patient has received all the information needed to understand their rights. It is the responsibility of the hospital staff to safeguard and preserve the patient's rights.

The **Patient's Bill of Rights** assures each patient has the right to:

1 Understand and use these rights. If for any reason they do not understand or they need help, the hospital must provide assistance, including an interpreter.

2. Receive treatment without discrimination as to race, color, religion, gender, gender identity and expression, national origin, disability, sexual orientation, or source of payment.

3. Receive considerate and respectful care in a clean and safe environment free of unnecessary restraints.

4. Receive emergency care if they need it.

5. Be informed of the name and position of the doctor who will be in charge of their care in the hospital.

6. Know the names, positions, and functions of any hospital staff involved in their care and refuse their treatment, examination, or observation.

7. A no smoking room. (SMH is a smoke free institution)

8. Receive complete information about their diagnosis, treatment, and prognosis.

9. Receive all the information they need to give informed consent for any proposed procedure or treatment. This information shall include the possible risks and benefits of the procedure or treatment.

10. Receive all the information they need to give informed consent for an order not to resuscitate. They also have the right to designate an individual to give this consent for them if they are too ill to do so. If they would like additional information, a copy of the pamphlet "Do Not Resuscitate Orders – A Guide for Patients and Families" should be provided.

11. Refuse treatment and be told what effect this may have on their health.

12. Refuse to take part in research. In deciding whether or not to participate, they have the right to a full explanation.

13. Privacy while in the hospital and confidentiality of all information and records regarding their care.

14. Participate in all decisions about their treatment and discharge from the hospital. The hospital must provide them with a written discharge plan and written description of how they can appeal their discharge.

15. Review their medical records and obtain copies of their medical records, (for which the hospital can charge a reasonable fee). They cannot be denied a copy solely because they cannot afford to pay. (See SMH Policy 6.2.1.)

16. Receive an itemized bill and explanation of all charges.

17. Formulate advance directives and appoint a health care proxy.

18. Participate in the consideration of ethical issues that arise in their care.

19. Authorize those family members and other adults who will be given priority to visit consistent with their ability to receive visitors.

20. Make known their wishes in regard to anatomical gifts. Patients may document their wishes in their health care proxy or on a donor card, available from the hospital.

21. Receive timely assessment and treatment of pain, including education about how to manage their pain.

22. Complain without fear of reprisal about the care and services they are receiving and to have the hospital respond to them and, if they request it, a written response. They should first speak to the nurse or doctor caring for them and if they are not satisfied with the hospital's response, they can request review by The Grievance Committee or complain to the New York State Department of Health. The hospital must provide them with the Department of Health phone number. If concerns cannot be resolved through the hospital or Department of Health patients may contact The Joint Commission at 1-800-994-6610 or via e-mail at complaint@jointcommision.org.

23. Inpatients who have been admitted from, or are awaiting readmission to, a residential health care facility have the right to meet with designated ombudsmen, unless such meeting is medically contraindicated.

24. The hospital recognizes the special needs of dying patients and their families and the importance of receiving care that optimizes the comfort and dignity of the patient. This includes treating primary and secondary symptoms as desired by the patient or the patient's representative, effectively managing pain and addressing psychosocial and spiritual concerns.

Patient Privacy and Confidentiality

Our patients trust us with some of their most personal health information. **HIPAA**, the Health Insurance Portability and Accountability Act, provides rules to protect the privacy and security of that information. These requirements apply to any form of health information including oral communication and paper or electronic records. All healthcare providers as well as organizations that bill or pay for medical care (such as insurance companies) are mandated to follow HIPAA and train their employees in these regulations. We all share in the obligation to keep protected health information private and secure.

Protected Health Information (PHI) is defined as information that relates to:

- The past, present or future physical or mental health or condition of an individual
- The provision of healthcare to the individual
- The payment for the provision of healthcare to that individual.

An identifier is any information that can be linked to an individual patient. Examples of identifiers are name, birth date, address, medical record number or any other data that can identify a specific patient.

During your observational experience, you are responsible for making sure you do not release PHI to anyone who does not need to know it as part of his or her work. You must also protect PHI that is kept in an electronic format (ePHI) by safeguarding any computer, hand-held electronic device, digital camera or other device that you are responsible for so that PHI is not seen by anyone who does not need the information as part of their job. There are many security policies and procedures organizations must adhere to in order to safeguard the electronic storage and transmission of ePHI. You also have a responsibility to access or release only the **minimum necessary information** (the least amount needed for the purpose) to that person or organization that needs it to do their job.

Under HIPAA, a Patient:

- Must be given a Notice of Privacy Practices explaining how their healthcare information (PHI) may be used
- Has a right to view or receive a copy of their medical record
- Has a right to amend (change) incorrect/incomplete information in their record
- Must give authorization before information is released (with some exceptions)
- Has a right to file a complaint if they feel their privacy was not protected

Uses and Disclosures of PHI

PHI may be used **without** the patient's authorization:

- To provide treatment
- To send bills for that treatment
- For healthcare operations, such as quality improvement activities

Patient authorization is **required** to release PHI in most other circumstances, such as:

- To an attorney
- To an employer
- For research , such as drug trials

In certain limited circumstances PHI may be released **unless the patient directs us not to**, such as:

- If a patient is listed in the facility's directory, his or her name, location and condition can be released to those who ask for the patient by name.

- If a patient chooses to declare a religious affiliation, the religious clergy can receive limited directory information.

- To a family member or person identified by the patient as being involved in the patient's care.

PHI is released **regardless** of a patient's wishes when required by law:

- Child abuse is suspected
- Public Health issues are identified
- Specified law enforcement purposes
- Medical devices/supplies are recalled

Both HIPAA and New York State have laws concerning confidentiality of patient information. When they differ, we must comply with the law that is either *more protective* of patient privacy, or gives patients *more access* to their PHI. For example, the release of HIV information requires a special authorization form required by the State. There are also special federal and state protections for records pertaining to genetic testing and treatment for substance abuse.

Breaches of Unsecured PHI

Unauthorized access, use, disclosure or acquisition of unsecured PHI may be a breach, including:

- Looking up PHI without a job-related reason
- Misdirected faxes or e-mails containing PHI
- Discussing patient care on a social networking site
- Loss or theft of PHI
- Improper disposal of PHI (computer files, paper, etc.)

There are both civil and criminal penalties for violations of the HIPAA regulations. A confidentiality violation may also result in a Type I recommendation from JCAHO and a citation from CMS.

REMEMBER … any information related to a patient's health cannot be used unless authorized by either the patient or someone acting on the patient's behalf, or unless permitted by regulation.

FOUR ACTIVITIES TO WATCH AS YOU WORK WITH PHI

SEEING – What might others see?

- ✓ You have a schedule on a clipboard in the open?
- ✓ You send a fax containing PHI?
- ✓ Your computer screen is faced outward?
- ✓ Printed material is not hidden?
- ✓ Schedules are on public walls?
- ✓ Patient charts are not face down on your desk?
- ✓ You leave a copier unattended?
- ✓ You are discarding confidential records?

TALKING – What might others hear when?

- ✓ You communicate PHI in an open area?
- ✓ You don't ask to whom you are speaking on the phone?
- ✓ You share information with someone who doesn't have a need to know?

- ✓ You leave a message containing details regarding tests?

HEARING – What might you hear when?

- ✓ Overhead pages say names and facts?
- ✓ Others do not speak softly or in private places?
- ✓ Others are speaking about patients in an open area?

MEDICAL RECORDS – How might others see PHI when

- ✓ Access is used to find out non-work related information?
- ✓ Your password is not a secret?
- ✓ You do not check the ID of a person you do not know?
- ✓ Your file rooms or cabinets are not kept locked?
- ✓ Your computer files are open on your screen?

Confidentiality of Patient Related Information

Every patient has a right to privacy and a right to know that the hospital personnel providing care will not share medical information with persons or students not involved in that care. Any information concerning the patient including source of payment, facts documented in the medical record, and information learned from other sources, is to be kept confidential.

Any patient information to which you are exposed during your observational experience may not be discussed with anyone who is not part of that experience.

It is the healthcare worker's responsibility to respect the patient's privacy, and to understand that the patient's right to confidentiality is protected by federal and state statute. Failure to maintain confidentiality can result in disciplinary measures being taken by the hospital. Refrain from discussing patients in public areas or social settings such as corridors, elevators, and cafeterias. It is also the healthcare worker's responsibility to report to the Department Manager any breach of confidential information they encounter.

Confidentiality of HIV-Related Information

The following persons are required to understand legal requirements prohibiting unauthorized disclosure of HIV-related information:

- Those who order HIV-related tests.
- Those who receive confidential HIV-related information in the course of providing any health or social services.
- Those who receive confidential HIV-related information pursuant to a release.
- Those who disclose any confidential HIV-related information in the course of providing any health or social services.

It is required that hospitals have a policy that includes the following provisions:

- Confidential HIV-related information must be recorded in the medical record so that it is readily accessible to provide proper care and treatment.
- No person who obtains confidential HIV-related information, in the course of providing any health or social service or prior to obtaining a release of confidential HIV-related information, may disclose or be compelled to disclose such information, except as permitted by law.
- All employees, contracted individuals, students, or affiliated persons at the hospital who may have HIV-related information disclosed to them in the course of their duties will receive inservice education regarding the policy.
- A list of job titles and specific employee functions within those titles for which employees are authorized to access such information is maintained by hospital administration. This describes the limits of such access to information, and employees receive this information during orientation, as required by law.
- Only employees, contracted employees, and students who have received such inservice education will be allowed access to confidential HIV-related information while performing authorized functions at a hospital.

The New York State Department of Health is now HIV-testing all newborn PKU samples. This requires hospitals to have a mechanism for written consent by the mother for the testing and the release of information.

Patients are entitled to have pre- and post-test counseling and may choose to have confidential or anonymous HIV testing. **Patients must sign a written consent for HIV testing and release of HIV-related information.** There are some exceptions when testing is done without patient consent such as court-ordered testing or testing prior to organ and/or tissue donation.

COMMUNITY-WIDE PLAIN LANGUAGE CODES (updated)

In an effort to standardize emergency code terminology, all Rochester Area Healthcare organizations have adopted emergency plain-language codes.

Each facility has specific procedures and phone numbers that will be utilized in the occurrence of any of the conditions below.

Plain Language	Condition
Fire Alert (followed by location	Fire alarm received
Fire Alert confirmed (followed by location)	Actual fire condition
Code Team (followed by location)	Adult cardiac/respiratory emergency
Code Team Pediatric (followed by location)	Pediatric cardiac/respiratory emergency
AMBER Alert (followed by infant, child, adolescent, then age)	Child under 18 years taken without authorization or suspected abduction
Assistance Needed STAT (followed by location)	Behavioral/Uncontrolled person incident
Critical Security incident (followed by location)	Critical security incident (weapon, bomb threat, active shooter)
Command Center activated (staff to implement disaster plans. Leadership or Command Team to report to designated area)	Disaster (Internal or community, natural or manmade)
Utility Alert	Major utility disruption
MERT	Non-life threatening medical emergency patient or non patient
All Clear	Situation resolved

SMH Specific

Purpose: Staff will be able to contact University Security Services for the purpose of reporting emergency and non-emergency incidents.

Objective: Upon completion of this section, staff will use the correct numbers to contact Security at both facilities.

Content: University Security Services can be contacted 24 hours a day, 7 days a week.

☏ **To Contact University Security Services:**

Emergencies	x 13 from inside UR or any Blue Light Emergency Phone
Non-emergencies	x 5-3333 (from inside UR). May use any (Blue Light Emergency Phone) located on or near pathways, parking lots, and each level of the MC ramp garage. 275-3333 (outside UR)

Regardless of the facility you are in, incidents that involve personal safety of students, volunteers, patients, employees and visitors should be reported to the appropriate Security service immediately. Other incidents include but are not limited to:

- Disturbances
- Structural failure
- Fire/explosion
- Utility emergency
- Chemical/biological/radiological contamination
- Medical emergencies
- Bomb threat
- Injuries
- Loss of inventory
- Traffic conditions/accidents
- Suspicious persons or activities
- Abduction
- Patient disappearance
- Physical crimes
- Theft/ weapons