EXHIBIT B

HIPAA PRIVACY RULE TRAINING FOR STUDENTS

INTRODUCTION

As a student in a clinical training program at the University of Wisconsin Hospitals and Clinics ("UWHC"), you are required to learn about the health information privacy requirements ("Privacy Rule") of a federal law called HIPAA (**H**ealth **I**nsurance **P**ortability and **A**ccountability **A**ct). The purpose of this document is to summarize relevant UWHC policies dealing with protecting patient's health information.

PROTECTED HEALTH INFORMATION

The Privacy Rule defines how health care providers, staff in health care settings, and students in clinical training programs can access, use, disclose, and maintain confidential patient information called "**P**rotected **H**ealth **I**nformation" ("**PHI**"). PHI includes written, spoken, and electronic information. PHI means any information that identifies a patient, including demographic, financial, and medical, that is created by a health care provider or health plan that relates to the past present or future condition, treatment, or payment of the individual. The Privacy Rule very broadly defines "identifiers" to include not only patient name, address, and social security number, but also, for example, fax numbers, email addresses, vehicle identifiers, URLs, photographs, and voices or images on tapes or electronic media. **When in doubt, you should assume that any individual health information is protected under HIPAA.** The following lists ways in which you are permitted and prohibited from accessing, using, and disclosing PHI while on clinical rotation at UWHC.

GUIDELINES FOR PROTECTING PHI WHILE AT UWHC

1. Using and Disclosing PHI for Training Purposes Only

As a student in a clinical training program, you are permitted to access, use, and disclose PHI *only* as is *minimally necessary* to meet your clinical training needs (you are only accessing, using, or disclosing, the minimum amount of information needed for your training purposes). You are not permitted to disclose PHI to anyone outside of UWHC or your training program, without first obtaining written patient authorization or de-identifying the PHI. **This means that you may not discuss or present *identifiable* patient information with or to anyone, including classmates or faculty, who are not part of your training, unless you first obtain written authorization from the patient.** Therefore, it is strongly recommended that whenever possible, you de-identify PHI (discussed below) before presenting any patient information outside UWHC. If you are unable to de-identify such information, you must discuss your need for identifiable information with the faculty member supervising your training and the HIPAA Privacy Officer at your training site, to determine the appropriate procedures for obtaining patient authorization for your use and disclosure of PHI.

2. De-identified Information

In order for PHI to be considered de-identified, all of the following identifiers of the patient or of relatives, employers, or household members of the patient, must be removed:

a. Name;
b. Geographic subdivisions smaller than a state (i.e., county, town, or city, street address, and zip code) (note: in some cases, the initial three digits of a zip code may be used);
c. All elements of dates (except year) for dates directly related to an individual (including birth date, admission date, discharge date, date of death, all ages over 89 and dates indicative of age over 89)
d. Phone numbers;
e. Fax numbers;
f. E-mail addresses;
g. Social security number;
h. Medical record number;
i. Health plan beneficiary number;
j. Account number;
k. Certificate/license number;
l. Vehicle identifiers and serial numbers;
m. Device identifiers and serial numbers;
n. URLs;

o. Internet protocol addresses;
p. Biometric identifiers (e.g., fingerprints);
q. Full face photographic and any comparable images;
r. Any other unique identifying number, characteristic, or code; and
s. Any other information that could be used alone or in combination with other information to identify the individual, such as a picture of a face

3. Safeguarding PHI

Below are common sense steps to take to protect PHI when using it, such as:

- If you see a medical record in public view where patients or others can see it, cover the file, turn it over, or find another way to protect it
- When you talk about patients as part of your training, try to prevent others from overhearing the conversation. Whenever possible, hold conversations about patients in private areas
- When medical records are not in use, store them in offices, shelves or filing cabinets
- Remove patient documents from faxes and copiers as soon as you can
- Make sure you throw away documents containing PHI in UWHC confidential bins for shredding
- Never remove the patient's official medical record from the training site
- Log out of electronic systems containing PHI when you are done using them
- Avoid removing copies of PHI from the training site; if you must remove copies of PHI from the training site, e.g., to complete homework, take appropriate steps to safeguard the PHI outside of the training site and properly dispose of the PHI when you are done with it. You should not leave PHI out where your family members or others may see it. All copies of PHI should be shredded when they are no longer needed for your training purposes.

4. Disclosure of PHI to Family Members or Friends Involved in the Care of the Patient

Care must be taken when discussing PHI in front of or with a family member or friend who is involved in the care of the patient. Generally you can assume that the patient does not object you to talking about them with such a person, however, if you have any reason to believe that the patient would object (discussing a "sensitive" diagnosis or procedure and etc.) then you should either ask the person to step out of the room or ask the patient if it is okay to talk to that person.

5. E-mailing

Because of potential security risks, you are not permitted to e-mail PHI to anyone.

6. Requests for Access to or Copies of Medical Records

HIPAA grants patients the right to access to and obtain copies of their medical records. However, please refer all such requests to the patient's primary health care provider (e.g., nurse) to ensure that proper procedures are followed.

7. Requests for PHI by Law Enforcement

Requests for PHI by law enforcement officers (e.g. police, sheriff) must be referred to the patient's primary caregiver (e.g. nurse) to ensure that proper procedures are followed.

FAILURE TO FOLLOW UWHC POLICIES GOVERNING PHI

Failure to follow polices governing access to, and use and disclosure of PHI will result in being denied access to UWHC facilities and clinical sites.

Failure to follow polices governing access to, and use and disclosure of PHI may also result in civil and criminal penalties under federal law.

UWHC'S HIPAA PRIVACY OFFICER

If you have any questions or concerns regarding the information in this document, you may contact the UWHC HIPAA Privacy Officer: UWHC HIPAA Privacy Officer, 600 Highland Ave., Room H4/852, Madison, WI 53792 Telephone: 608-203-4631

EXHIBIT C

CONFIDENTIALITY AGREEMENT

The University of Wisconsin Hospitals and Clinics Authority ("UWHC") provides learning experiences for health science students from outside our settings. These students have the opportunity to observe and participate in the care of UWHC patients. Federal and state laws, accreditation standards, and professional ethics require that all health science students maintain the confidentiality of patient information to the greatest extent possible. The purpose of this agreement is to establish the following understanding between UWHC and the health science student regarding confidentiality of patient information.

I understand that I am responsible for reading and understanding the attached HIPAA training document. Should I have questions regarding the content, I will consult with my clinical supervisor and/or the UWHC HIPAA Privacy Officer.

I understand that during my participation in my clinical experience, I may come in contact with the PHI of UWHC patients. PHI means any information that identifies a patient, including demographic, financial, and medical, that is created by a health care provider or health plan that relates to the past present or future condition, treatment, or payment of the individual.

I understand that PHI includes all patient identifiable information in any medium, including, but not limited to oral, written, hard copy, and electronic (whether retrieved on screen or contained on a computer disc).

I understand that PHI is to be held in strict confidence and I agree that I will not:

1. Review any individually identifiable information not directly related to my participation in an educational experience.
2. Discuss any PHI with anyone who does not have a legitimate, professional need-to-know the information.
3. Disclose the information to any person or organization outside UWHC without proper, written authorization from the patient.

I understand that the obligations outlined above will continue after my participation in this educational experience.

I understand that violation of any of the above will result in termination from participation in the educational experience and may lead to civil and/or criminal penalties pursuant to the Health Insurance Portability and Accountability Act of 1996.

_____ _____

Signature of Student Date