PRIVACY OF HEALTH INFORMATION

TABLE OF CONTENTS

HIPAA 1

What Is HIPAA? 1
The Privacy Regulation 1
The Transaction & Code Sets And Security Regulations 1
Differences Between the Privacy and Security Regulations 1
Government Enforcement And Penalties 2
How Will the HIPAA Privacy Regulation Impact MCW? 2

THE PRIVACY REGULATION – GENERAL 3

Definitions 3
General Provisions of the Privacy Regulation 4
1. Individual 4
2. Treatment, Payment or Operations 4
3. Incidental Uses or Disclosures 5
4. Authorization 5
5. Agreement or Objection From Individual 5
6. Other Specific uses or Disclosures 5

THE PRIVACY REGULATION – FOCUS TOPICS 6

Focus Topic: Notice of Privacy Practices 6
Focus Topic: Research 6
Focus Topic: Minimum Necessary 7
Focus Topic: Residents 7
Focus Topic: Medical Students 7
Focus Topic: Affiliated Organizations 8
Focus Topic: Fundraising Activities 8
Focus Topic: Business Associates 8
Focus Topic: Psychotherapy Notes 8
Focus Topic: State Law Preemption 9
Focus Topic: Security in the Privacy Regulation 9

ADDITIONAL RESOURCES 10

HIPAA Website 10
If You Need Additional Information 10

PRIVACY QUIZ ANSWERS 13

Return to Table of Contents

MEDICAL COLLEGE OF WISCONSIN

HIPAA

WHAT IS HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) was the result of a bill sponsored by Senators Nancy Kassenbaum (R-KS) and Ted Kennedy (D-MA), which was signed into law in August 1996.

HIPAA was primarily designed to protect Americans who were previously ill from losing their health insurance when they changed jobs. Another component of HIPAA was to adopt criminal and civil fraud and abuse regulations. Finally, HIPAA was intended to streamline the health care system through the adoption of consistent standards for transmitting uniform electronic health care data between providers of health care services (e.g. MCW) and payers (e.g. Medicare). In order to adopt transmission standards, it became necessary to adopt standards for securing the storage of that information and for protecting an individual's privacy.

The three HIPAA regulations that immediately impact MCW are:

- Privacy Regulation
- Transaction and Code Sets Regulation
- Security Regulation

This booklet will describe the Privacy and Security Regulations and highlight areas that have the greatest impact on our day-to-day activities at the Medical College of Wisconsin (MCW). Now that all of the HIPAA regulations are fully in place and implemented, it is believed that the health care industry has a standardized way of transmitting electronic claims and other health care transactions, with increased privacy and security of all health care information.

THE PRIVACY REGULATION

The HIPAA statute required the Secretary of the Department of Health and Human Services (DHHS) to publish privacy regulations. These regulations are effective **April 14, 2003**. The Privacy Regulation governs who has access to use and disclose an individual's health information.

This Privacy of Health Information booklet will summarize the key components of the Privacy Regulation that you need to know when using or disclosing health information as part of your job at MCW.

THE TRANSACTION & CODE SETS AND SECURITY REGULATIONS

In addition to the Privacy Regulation, two other regulations must be mentioned.

The first, often referred to as the "Transaction & Code Sets Regulation," requires standard formatting of electronic transactions for certain specified financial and administrative purposes such as health care claims, or inquiries about health plan eligibility or health plan coverage. The effective date for this regulation is October 16, 2003.

The second is referred to as the "Security Regulation." The Security Regulation addresses the physical and technical safeguards necessary when storing or transmitting health information. MCW was required to adopt policies and procedures to ensure compliance with the Security Regulation requirements. This will impact e-mail systems, research databases, clinical information systems, paper medical records, and any other systems where health information is stored or transmitted. The effective date for this regulation is April 20, 2005.

DIFFERENCES BETWEEN THE PRIVACY AND SECURITY REGULATIONS

The Privacy Regulation focuses on the application of effective policies, procedures, and business associate agreements to control who has access to use and disclose health information.

The Security Regulation focuses on an organization's physical infrastructure such as access to offices, files, and computers to ensure

Return to Table of Contents

secure and private maintenance and communication of health information. The Security Regulation focuses on how the information is stored and transmitted.

GOVERNMENT ENFORCEMENT AND PENALTIES

Compliance with the HIPAA regulations is mandatory to maintain our patients' trust in MCW. In addition, there are significant penalties for non-compliance. The DHHS Office for Civil Rights is charged with educating health care organizations on the requirements of the Privacy and Security Regulations and enforcing any actions taken as a result of non-compliance. If a health care provider fails to implement the steps necessary to comply with the Privacy and Security Regulations, or uses or discloses health information in a manner that is not allowed in the regulations, the penalties may include:

- Administrative action taken by the DHHS Office for Civil Rights.
- Civil Penalties of between $100 and $50,000 or more for each violation, with the total amount imposed on the person for all violations during a calendar year not to exceed $1,500,000.
- Criminal Penalties of up to $250,000, imprisonment for up to 10 years, or both if the conduct involves the intent to sell, transfer, or use identifiable health information for commercial advantage, personal gain or malicious harm.

HOW WILL THE HIPAA PRIVACY REGULATION IMPACT MCW?

Although MCW has always placed a high priority on safeguarding patient health information and ensuring confidentiality, the Privacy Regulation will formalize this commitment. In general, the Privacy Regulation has required MCW to:

- Provide information to patients about their privacy rights and how their health information will be used and/or disclosed. This is accomplished with a "Notice of Privacy Practices."
- Adopt Privacy Policies and Procedures.
- Educate employees so that there is a common understanding of the appropriate uses and disclosures of health information. This "Privacy of Health Information" booklet is one method of conducting this education.
- Develop "Business Associate Contracts" with all entities that perform a function or activity on behalf of MCW, where health information is involved.
- Modify requirements for using health information in research activities. This includes changes to the patient "Informed Consent" language, and additional steps researchers must take to obtain a waiver of a patient's consent/authorization to use health information in research.
- Designate an individual to be responsible for ensuring that all Privacy Policies and Procedures are adopted by MCW, and followed.

Although this booklet provides a summary of the Privacy Regulation, the implementation details can be found in the MCW HIPAA Privacy Policies and Procedures. These Policies and Procedures may be found at the MCW HIPAA Website:

http://infoscope.mcw.edu/hipaa/

Please use this site to reference, read, understand and adhere to the HIPAA Privacy Policies and Procedures. In addition, this site contains other HIPAA information, answers to frequently asked questions, and the latest governmental updates on HIPAA regulations.

Return to Table of Contents

MEDICAL COLLEGE OF WISCONSIN

THE PRIVACY REGULATION – GENERAL

DEFINITIONS

The Privacy Regulation specifies all allowable uses and disclosures of health information. This regulation contains terminology that must be understood for proper implementation and use in your day-to-day activities at MCW. This section contains some important Privacy Regulation definitions.

Covered Entity – a health plan, a health care clearinghouse, or a health care provider. MCW is a covered entity, as is each affiliate hospital or health care organization in which we see patients or conduct business.

Protected Health Information (PHI) – any information, oral or recorded in any medium; relating to the past, present or future, physical or mental condition of an individual, and includes any additional information that identifies an individual (see below).

Identifiers – when linked with Health Information, creates Protected Health Information. Identifiers include the following: name; all geographic subdivisions smaller than a state except for 3-digit zip codes; dates; telephone numbers; fax numbers; e-mail addresses; social security numbers; medical record numbers; health plan beneficiary numbers; any account numbers; certificate or license numbers; automobile related numbers; medical device identifiers; web addresses; internet protocol addresses; biometric identifiers including finger/voice prints; full face or comparable photographic images; any other unique identifying number, characteristic or code.

Use of Health Information –the sharing, employment, application, utilization, examination, or analysis of such information within a covered entity (MCW) that maintains the information.

Disclosure of Health Information –the release, transfer, provision or access to, or divulging in any other manner of information outside the covered entity holding the information. Any flow of information between MCW and affiliates or payers is a disclosure.

Treatment - the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

Payment - the activities undertaken by a health care provider or health plan to obtain or provide reimbursement for the provision of health care including but not limited to billing, claims management, collections activities and related health care data processing; and utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services.

Operations - any of the following activities:

- ✓ Quality assessment and improvement
- ✓ Outcomes evaluation and clinical guidelines
- ✓ Protocol development
- ✓ Case management
- ✓ Evaluation of providers
- ✓ Accreditation, certification, licensing, credentialing
- ✓ Training programs (e.g. medical students)
- ✓ Medical review, legal, auditing
- ✓ Business planning and development

Research –a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

Return to Table of Contents

GENERAL PROVISIONS OF THE PRIVACY REGULATION

There are six general provisions in the Privacy Regulation that specify allowable uses or disclosures of protected health information. These six allowable uses or disclosures form the basis of the regulation: 1. to the individual who is the subject of the information; 2. treatment, payment or operations; 3. incidental uses or disclosures; 4. authorization; 5. agreement or objection from individual; 6. other specific uses or disclosures. These six general provisions are described in this section.

1. INDIVIDUAL

In most cases, MCW is allowed to disclose protected health information to the individual who is the subject of the information. For MCW, an individual is most frequently a patient or a research participant.

For purposes of the Privacy Regulation, personal representatives as defined in state law are treated as the "individual." The only protected health information an individual does generally not have a right to access is information compiled in anticipation or use for a civil, criminal or administrative action.

2. TREATMENT, PAYMENT OR OPERATIONS

Uses of Protected Health Information

In general the Privacy Regulation allows MCW to **use** protected health information for our own treatment, payment or health care operations activities. This allows MCW to see patients, generate bills and collect payments, and conduct all operational activities as listed in the definition of "operations."

There are no "minimum necessary" restrictions on uses for treatment activities, however minimum necessary restrictions apply for all payment and operations activities. For further information on minimum necessary requirements, please see the section in this booklet titled "Focus Topic: Minimum Necessary."

Disclosures of Protected Health Information

The Privacy Regulation allows MCW to **disclose** protected health information for the treatment, payment and health care operations activities of other covered entities with a few restrictions. Conversely, other covered entities are allowed to disclose protected health information to MCW for these same purposes with the same restrictions.

Treatment – information is allowed to flow between covered entities for treatment purposes. This means there are no restrictions for a "minimum necessary" disclosure for treatment purposes, including consultations or referrals, or any other activities related to treating the individual (patient).

Payment – information is allowed to flow between covered entities, including providers (e.g. physicians' offices and hospitals) and health plans (e.g. HMOs) for payment purposes. The primary restriction on the flow of information is that only a "minimum necessary" amount of information may be shared to accomplish the intended purpose.

Operations – information is allowed to flow between covered entities, including providers and health plans, for certain specified health care operations activities. A first restriction on the flow of information is that only a "minimum necessary" amount of information can be shared to accomplish the intended purpose. A second restriction is that both covered entities must have some relationship with the individual (patient). A third restriction is that information can be shared for only specific operational activities as follows:

- ✓ Quality assessment and improvement
- ✓ Outcomes evaluation and clinical guidelines
- ✓ Protocol development
- ✓ Case management
- ✓ Evaluation of providers
- ✓ Accreditation, certification, licensing, credentialing
- ✓ Training programs (e.g. medical students)

or for:

- ✓ Compliance activities

Return to Table of Contents

3. Incidental Uses or Disclosures

An incidental use or disclosure of protected health information may occur as a result of performing our day-to-day activities. These uses or disclosures are generally considered "acceptable" if the following criteria are met:

- It is limited in nature
- It cannot be reasonably prevented
- It occurs as a byproduct of an allowable use or disclosure

In addition, for an incidental use or disclosure to be considered allowable, MCW must make sure that only a "minimum necessary" amount of protected health information is used for our activities as required, and that we employ "reasonable security" measures for the storage and transmission of protected health information. Please see the sections in this booklet titled "Focus Topic: Minimum Necessary" and "Focus Topic: Security in the Privacy Regulation" for additional information on these subjects.

Examples of incidental uses or disclosures may include sign-in sheets in waiting rooms, patient charts at a bedside, or overheard conversations that could not be kept private.

4. Authorization

In most other day-to-day situations at MCW that involve the use or disclosure of protected health information that was not described above, an authorization from the patient is required. An authorization is a document that contains specific information, and is signed and dated by the individual (patient). The authorization must contain the following information:

- ✓ A description of the information to be used or disclosed
- ✓ Name of the requestor
- ✓ Name of the individual (patient)
- ✓ A description of each purpose of the requested use or disclosure
- ✓ Expiration date or event
- ✓ Several other required statements
- ✓ Signature of individual (patient) and date

For research purposes an authorization may be considered synonymous with an informed consent. However, to use the informed consent document for research purposes, the language of the consent must be modified to incorporate the Privacy Regulation components. The MCW HIPAA Website contains information on the required authorization language and the corresponding informed consent language provisions.

5. Agreement or Objection From Individual

The HIPAA Privacy Regulation allows for the disclosure of information if the individual (patient) has an opportunity to either agree to, or object to the disclosure. This includes disclosures to family members, relatives and friends. In general there are two scenarios where this applies – either the individual is present, or not.

- If the individual is present he/she must be given the opportunity to agree or object to the disclosure, or the disclosure can be made if it can be inferred that the individual does not object. This includes allowing patient visitors in rooms, discussions with family members, and similar situations.
- If the individual is NOT present the regulation requires that practitioners and other health care staff use professional judgment and common accepted practices. Examples where the individual is not present when protected health information is disclosed include situations where family members are picking up prescriptions or supplies, or transporting X-rays.

In both cases above, all MCW faculty and staff are to use professional judgment and common past accepted practices. The overriding factor in these situations is to consider what is in the best interest of the patient.

6. Other Specific uses or Disclosures

The Privacy Regulation lists 12 other uses or disclosures that are allowed in specific circumstances:

- ✓ Required by Law
- ✓ Public Health Activities
- ✓ Disclosures about victims of abuse, neglect or domestic violence
- ✓ Heath Oversight Activities

Return to Table of Contents

- ✓ Judicial and Administrative Proceedings
- ✓ Law Enforcement Purposes
- ✓ Decedents – coroners, medical examiners
- ✓ Cadaveric Organ, Eye or Tissue Procurement
- ✓ IRB Approval/Waiver for Research Purposes
- ✓ To Avert a Serious Threat to Health or Safety
- ✓ Specialized Government Functions
- ✓ Workers' Compensation

The application of these circumstances in our day-to-day activities various depending on your job duties. For additional information on these circumstances please visit the MCW HIPAA Website, speak with your supervisor, or call the appropriate contact listed at the end of this booklet.

MEDICAL COLLEGE OF WISCONSIN

THE PRIVACY REGULATION – FOCUS TOPICS

The prior section provided the general provisions of the Privacy Regulation, however there are several specific focus topics that require further explanation. This is especially true given the diverse nature of MCW's mission in the areas of education, research, patient care, and community service, and our interaction with affiliate hospitals.

FOCUS TOPIC: NOTICE OF PRIVACY PRACTICES

The Medical College of Wisconsin (MCW) is required to provide a Notice of Privacy Practices to all patients, research participants and other individuals with whom we use or disclose protected health information. MCW and Froedtert Hospital (Froedtert) have developed a Joint Notice of Privacy Practices for use at all Froedtert and MCW locations. Children's Hospital of Wisconsin and the Veterans Administration Medical Center have developed similar notices, and have incorporated the necessary language to reflect the appropriate use and disclosure of protected health information by MCW faculty and staff at these institutions.

The MCW and Froedtert Joint Notice of Privacy Practices is available on the main MCW Internet Site, and the MCW HIPAA Website.

The Notice must be provided to individuals no later than the first date of service that takes place on or after April 14, 2003. In addition, MCW is required to make a good faith effort to obtain a written acknowledgement of the receipt of the notice. For clinical patient care, this will typically take place at the time of registration. For research activities (e.g. clinical trials) this will typically take place during the participant enrollment process.

FOCUS TOPIC: RESEARCH

The HIPAA Privacy Regulation will impact MCW's research activities and processes. The Privacy Regulation defines research as "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge."

Frequently faculty physicians and MCW staff may use protected health information to conduct internal quality assurance studies, develop clinical guidelines or assess patient outcomes. If there is no intent to publish or present results, these activities are defined in the Privacy Regulation as "operations" and not "research." Consequently these activities may be conducted without patient authorization or an Institutional Review Board (IRB) waiver of authorization.

In general there are six pathways to using protected health information in research as described below.

1. Patient Authorization – For most clinical trials or other research involving human participants, the Principal Investigator and his/her research team will receive informed consent from the research participant. As part of this informed consent document, or in a separate document, the Principal Investigator must obtain the patient's authorization to use protected health information in research. This is true if the IRB has not granted a waiver of authorization (see next section).

Return to Table of Contents

2. Waiver of Authorization – Occasionally the Principal Investigator may seek, and the IRB may grant, a waiver of the requirement to obtain a patient's authorization for use or disclosure of protected health information in research. Examples where this waiver may be granted include research involving retrospective data analysis or chart reviews.

3. Research on Decedent's Information – If data is required to conduct research on a decedent's protected health information; it is possible to receive an expedited approval for the study. The researcher must apply for and receive approval for conducting research on decedents' protected health information.

4. Reviews Preparatory to Research – If data is required to prepare a research protocol or otherwise conduct a review of protected health information in preparation for a research study, it is possible to receive an expedited approval for the study. The researcher must apply for and receive approval for using protected health information in conducting a review preparatory to research.

5. Limited Data Set and Data Use Agreement – A limited data set is protected health information that excludes all of the identifiers defined in the "Definitions" section of this document, but it may contain the full 5-digit zip code and/or all applicable dates (e.g. admission date, birth date, date of service). The "recipient" of the limited data set (e.g. Principal Investigator and his/her research team) must enter into a Data Use Agreement with MCW or the appropriate affiliate hospital prior to receiving the information.

6. De-Identified Data – Health Information that excludes all of the identifiers listed in the "Definitions" section of this booklet is not considered protected health information. As a result, this type of information may be used/disclosed if there is no method or key to "re-identify" or "re-link" the health information with the individual or patient who is the subject of the information.

The contents of the patient authorization, waiver of authorization, and approvals for the use protected health information in research for the other pathways are specific and unique to the Privacy Regulation. Additional information on these processes and forms can be found on the MCW HIPAA Website.

Focus Topic: Minimum Necessary

MCW must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use or disclosure. This "minimum necessary" requirement may be met by policies and procedures for routine uses or disclosures, or by review on a case-by-case basis.

Minimum necessary does not apply for disclosures to the individual who is the subject of the information, for treatment purposes, or for disclosure made as a result of an authorization (see Focus Topic: Research).

An overriding factor to consider in many day-to-day situations for all payment and operations activities (and although the regulation does not require it, for treatment activities as well) is to ask "Is this health information necessary for me to do my job?" If the answer is "yes", you probably are fulfilling the minimum necessary requirements and complying with this part of the Privacy Regulation.

Focus Topic: Residents

Residents practicing under the Medical College of Wisconsin Affiliated Hospitals (MCWAH) are considered "health care providers" in the Privacy Regulation. MCW is allowed to "disclose" protected health information to MCWAH residents as specified in the General Provisions of the Privacy Regulation section of this booklet.

The six general provisions listed in this booklet that apply to MCW employees, also generally apply to residents as well. The clinical activities of residents are defined as "treatment." Any "research" use or disclosure of protected health information by residents must follow one of the six pathways defined in the "Focus Topic: Research" section of this booklet.

Focus Topic: Medical Students

The Privacy Regulation defines medical students' participation in patient care or other activities as a part of a "training program"; consequently this type of education is considered "operations" and not "treatment."

Return to Table of Contents

Because medical student activities are considered operations, the minimum necessary standards must be met. That is, medical students may access only that protected health information that is necessary for conducting their educational and learning activities, and no more.

Any "research" use or disclosure of protected health information by medical students must follow one of the six pathways defined in the "Focus Topic: Research" section of this booklet.

Focus Topic: Affiliated Organizations

Froedtert Hospital, Children's Hospital of Wisconsin, the Veterans Administration Medical Center, and other affiliate hospitals and organizations are all "covered entities" under the Privacy Regulation. As covered entities, each is required to provide information to patients about privacy rights, adopt privacy policies and procedures, educate employees, develop business associate contracts, comply with the research provisions, designate a responsible individual for privacy concerns, and otherwise ensure compliance with the regulation.

MCW has worked closely with the three primary affiliate hospitals, and other affiliates as necessary, to monitor and where appropriate ensure a consistent approach to implementing the changes required by the HIPAA Privacy Regulation.

Focus Topic: Fundraising Activities

The Privacy Regulation allows MCW to only use demographic information (name, address) of an individual and dates of service, for purposes of fundraising activities, when an authorization is received in advance from the patient. Without written authorization from the patient, MCW cannot use a patient's condition, diagnosis, clinic name where services were received, or specialty of the treating physician, to identify or assemble mailing lists for fundraising or promotional purposes.

The contents of the patient authorization are specific and unique to the Privacy Regulation. Additional details on fundraising and a model authorization form can be found on the MCW HIPAA Website.

Focus Topic: Business Associates

A Business Associate is defined as any individual or organization that performs, or assists in the performance on behalf of MCW of a function or activity involving the use or disclosure of individually identifiable health information. Business Associates also are individuals or organizations that provide certain specific services involving the disclosure of individually identifiable health information from MCW to the business associate. Examples of services that may make an individual or organization a Business Associate include consulting, data aggregation and transcription services.

It is important to note that a person or organization that provides services for MCW, but is not paid for these services, may still be considered a Business Associate. It is the function of the individual or organization that determines whether there is a Business Associate relationship.

MCW is required to have signed contracts with specific terms for all Business Associates. Additional details on the standard MCW Business Associate contract and information to help department administration determine if a Business Associate relationship exists with an individual or organization can be found on the MCW HIPAA Website.

Focus Topic: Psychotherapy Notes

Psychotherapy Notes are defined as notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separate from the rest of the individual's (patient's) medical record.

Psychotherapy Notes exclude medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date. These exclusions are intended to allow for the use and disclosure of a sufficient amount of information for pre-authorization of services, billing, and other activities regarding treatment, payment and operations.

Authorization by the patient is required to use/disclose psychotherapy notes (as defined above) in all cases, unless it is to the originator of the

Return to Table of Contents

notes, for use in training programs (e.g. medical students) or in legal action brought by the individual (patient).

***FOCUS TOPIC*: STATE LAW PREEMPTION**

The State of Wisconsin has always had stringent patient privacy laws. HIPAA law however preempts (replaces or overrides) State law, unless State law is "more stringent." For purposes of the Privacy Regulation, more stringent means:

- With respect to a use or disclosure, that law which provides the greater restrictions or prohibitions.
- With respect to patient rights, that law which provides greater access or amendment.
- With respect to information released to the patient, that law which provides the greater amount of information.

HIPAA sets a national privacy protection "floor." The comparison of State law to the federal HIPAA Privacy law is complicated and dependent on specific circumstances. Because Wisconsin has traditionally had relatively stringent privacy protection regulations, the impact of the federal HIPAA Privacy Regulation in Wisconsin is not as great as in other states.

***FOCUS TOPIC*: SECURITY IN THE PRIVACY REGULATION**

The Privacy Regulation primarily addresses "who" can access protected health information, while the Security Regulation addresses "how" that information must be secured in storage and transmission. There are general security requirements in the Privacy Regulation however. MCW is required to reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the regulation. In addition, MCW is required to reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise allowed use or disclosure.

There are common and readily accessible security steps that all MCW faculty, staff, residents and medical students should take to help secure protected health information:

- Be aware of your surroundings when carrying on conversations in elevators or other public areas.
- Discard protected health information in a locked bin or shred it.
- Place interoffice mail containing protected health information in sealed confidential envelopes.
- If possible, avoid leaving messages on answering machines regarding a patient's condition or test results unless the patient approves or requests this.
- Determine if the protected health information should be faxed, or if another method of sending the information is more appropriate. Examples of acceptable reasons for faxing information include emergent patient care situations, pre-authorization for services, or diagnostic test results sent to the ordering physician.
- Make sure to validate the fax number prior to sending.
- If possible, avoid using patient identifying information in the subject line of e-mails.
- NEVER give out your computer password.
- Use a screen saver to lock your computer workstation, or log off the system before walking away.
- Password protect portable devices (e.g. PDAs, laptops).

Return to Table of Contents

MEDICAL COLLEGE OF WISCONSIN

ADDITIONAL RESOURCES

HIPAA WEBSITE

Policies and procedures, forms and other information referenced in this booklet may be found on the MCW HIPAA Website:

http://infoscope.mcw.edu/hipaa/

IF YOU NEED ADDITIONAL INFORMATION

Should you have questions on the information contained in this booklet, reference the MCW HIPAA Website and/or speak to your supervisor. In addition you may contact one of the following offices for additional information:

MCW Privacy Information – Corporate Compliance Office, 414-955-4099

Medical Records – MCW Medical Records, 414-805-6200

Research/Human Research Protection Program, 414-456-8422

Fundraising – Office of Institutional Advancement, 414-955-4400

Business Associate Contracts – Office of General Counsel, 414-955-8203

Transactions & Code Sets – Clinical Information Systems, 414-456-5079

Froedtert Privacy Information – Compliance Office, 414-805-2895

Children's Privacy Information – Compliance Office, 414-266-2215

VAMC Privacy Information – Compliance Office, 414-384-2000 x42139/x41021

MEDICAL COLLEGE OF WISCONSIN

PRIVACY QUIZ

1. **Confidentiality and privacy are important concepts in health care because:**
   a. They help protect health care organizations from lawsuits.
   b. They allow patients to feel comfortable sharing information with their doctors.
   c. They avoid the confusion of having people other than physicians seeing information about a patient.
   d. Both A and B.

2. **MCW is implementing the HIPAA regulations in the following order:**
   a. Administrative Simplification; Privacy; Security
   b. Privacy; Transaction & Code Sets; Security
   c. Transaction & Code Sets; Privacy; Security
   d. Privacy; Administrative Simplification; Security

3. **The Privacy Regulation addresses oral and paper healthcare information, while the Security Regulation addresses electronic healthcare information.**
   True or False?

4. **Which of the following is not considered part of health care operations?**
   a. Using PHI to credential physicians.
   b. Using PHI to analyze reimbursement patterns of a health insurance company.

Return to Table of Contents

c. Using PHI to identify candidates who may be eligible for a clinical trial.
d. Using PHI to train medical students.

5. **You are a practitioner responsible for treating patients. When are you allowed to repeat protected health information that you hear on the job?**
   a. After you no longer work at MCW.
   b. After the patient dies.
   c. Only if you know the patient won't mind.
   d. Only when it's necessary to do your job.

6. **Your sister's friend is having surgery at one of the local hospitals, but she is not sure which one. She wants to send flowers and asks you to find out if her friend is at your facility. What should you do?**
   a. Tell your sister that you cannot find out for her but that she can call the hospital information desk and ask whether her friend is staying there.
   b. Search for the friend's name in the registration database.
   c. Find a list of patients having surgery and look for the friend's name.
   d. Find out the condition of your sister's friend, and look at the names on the patient rooms to see if you can find her.

7. **Physicians are permitted to see all information about every patient.**
   True or False?

8. **MCW is required to have a separate Business Associate contract for each department and/or potential use of protected health information by the Business Associate.**
   True or False?

9. **You are cleaning up the nurse's station and find an open recycling bin full of paper. You can easily see names, addresses, and phone numbers on the paper. What should you do?**
   a. Nothing. You can't be sure the information has anything to do with patients.
   b. Show it to your supervisor in case the information is protected health information.
   c. Ask the nurses who work there what information is on the paper.
   d. None of the above.

10. **Patient information should not be thrown away in unlocked bins unless it has been shredded or destroyed.**
    True or False?

11. **Which of the following is <u>not</u> a common way that employees can protect the security of protected health information?**
    a. Never share your password to any system.
    b. Place interoffice mail containing protected health information in a sealed, confidential envelope.
    c. Use 1024 bit RSA encryption on all e-mail messages you send.
    d. Password protect laptops and PDAs.

12. **Which area is NOT addressed by HIPAA?**
    a. Insurance portability
    b. Single payer healthcare system
    c. Fraud enforcement
    d. Administrative simplification

13. **Confidentiality and privacy protections cover not just a patient's health related information such as why they are being treated, but also such information as address, age, social security numbers and telephone numbers.**
    True or False?

14. **What are the two kinds of sanctions under HIPAA?**
    a. Egregious and inadvertent
    b. Criminal and civil
    c. Warranted and unwarranted
    d. Security and Privacy

Return to Table of Contents

15. **Which organization is charged with enforcing the Privacy Regulation?**
    a. The Office for Civil Rights
    b. The Office of Homeland Security
    c. The Healthcare Financing Administration
    d. The Federal Bureau of Investigations

16. **What kind of individually identifiable health information does HIPAA's privacy law protect?**
    a. Paper
    b. Electronic
    c. Oral
    d. All of the above

17. **When disclosing patient information to another provider for the provision of treatment, should you limit the patient information you provide?**
    a. No, you should provide whatever information the provider requests.
    b. Yes, you should provide only the amount of information necessary for treatment.

18. **Health Care workers can go to jail for selling patient information.**
    True or False?

19. **Minimum necessary in the Privacy Regulation applies to giving patients only enough information to select a treatment option, and no more than this.**
    True or False?

20. **What is one of the first questions that you should ask yourself before looking at patient information?**
    a. Would the patient mind if I looked at this?
    b. Do I need this information to do my job?
    c. Are there identifiers on this information?
    d. Am I curious?

21. **For purposes of the Privacy Regulation, neither residents nor medical students need to be concerned with the amount of information they are reviewing as long as it's related to treating a patient.**
    True or False?

22. **You are approached by an individual who tells you that he is here to work on computers and wants you to open a door for him or point the way to a workstation. How do you respond to his request?**
    a. Provide him with the information or access he needs.
    b. Ask him who has hired him and refer him to that person for assistance.
    c. Call the police.
    d. Call security.

23. **An authorization is always required in which situation?**
    a. When the patient registers in the clinic.
    b. To send mailers inviting patients to a fund raising event for "Transplant Survivors."
    c. For any research purpose.
    d. To send information to an insurance company.

24. **The following is an example of MCW disclosing protected health information.**
    a. Sending protected health information to a hospital for credentialing purposes.
    b. Using information to schedule a patient for a MCW clinic visit.
    c. Assembling MCW medical record information to help structure a research proposal.
    d. Analyzing MCW information to identify potential areas for improving the patient scheduling process.

25. **A research database that contains protected health information is acceptable to continue using after April 14, 2003, as long as you:**
    a. Encrypt the data.
    b. Haven't published any results yet.

Return to Table of Contents

c. Maintain the database on your own personal computer, and not on the LAN.
d. Obtain a waiver of authorization from the appropriate IRB.

PRIVACY QUIZ ANSWERS

1. D	2. B	3. FALSE	4. C	5. D
6. A	7. FALSE	8. FALSE	9. B	10. TRUE
11. C	12. B	13. TRUE	14. B	15. A
16. D	17. B *	18. TRUE	19. FALSE	20. B
21. FALSE	22. B	23. B	24. A	25. D

* You do not have to limit information for treatment under HIPAA. However, good practice is to consider what's being asked. That is, don't send the whole record if only the current medical problem is involved.