

January 21, 2008

Dear Applicant:

Subject: Schools of Allied Health Required Privacy, Confidentiality, Compliance and Infection Control Training.

To meet the HIPAA (Health Insurance Portability and Accountability Act) requirements, all members of our workforce must complete training regarding **Privacy, Confidentiality, Compliance and Infection Control** annually. This includes our employees, physicians, volunteers, students, contracted employees, and any agent involved in patient care.

Read the attached PowerPoint and Word modules, print the quizzes, complete the quizzes and bring them with you to your interview.

There is no on-line test for Infection Control yet. Please read the attached information, print off and complete the quiz, sign the back of the sheet and bring it with you the next time you come to volunteer. Give the quiz and signature sheet to the Patient Representative if I am not around.

If you should have any questions regarding this information, please do not hesitate to contact us.

Sincerely,

Doug Clarkston
Privacy Officer
248-551-5006

Edward Grima
Corporate Compliance Officer
Corporate Administration
248-551-0752

Manager/Chief: Ann F. Sosnowski

Department: Beaumont Schools of Allied Health

Phone

Number: 248-898-8047

Patient Confidentiality Training

For All Members of Beaumont Hospitals Workforce

Module 1

2008

Introduction

❖ This lesson provides information about the elements of Patient Confidentiality, why it is important, who is responsible and what are the responsibilities. Included are:

- Patient Confidentiality Training
- HIPAA Privacy and Security
- Beaumont Privacy Policies

Trust

Without assurances that their information will remain private, patients may withhold or alter crucial information which could affect the quality and outcome of their care.



Confidentiality is important

It is important that patients understand the information they share will not be accessed, disclosed or used in an unauthorized manner and will remain confidential.



Who is responsible for maintaining patient confidentiality?

❖ Anyone who...

- Cares for and consults with patients at/or for the health care organization
- Hears conversations about patients
- Has access to patient information



•Everyone

All health care workers who work or are affiliated with Beaumont are responsible for patient confidentiality.

❖ This includes...

- Patient caregivers
- Clerical and support staff
- Maintenance, housekeeping, and dietary staff
- Volunteers and students
- Agency employees involved in patient care activities



What are our responsibilities?

- ❖ We are obligated to keep all information about patients confidential
- ❖ Every health care worker must make a conscious effort to keep all personal information about the patient private



❖ If you see a coworker inappropriately sharing patient information, it is your responsibility to either talk directly to that person or to inform management.

❖ If you are asked to break confidentiality, it is your obligation to say "NO."



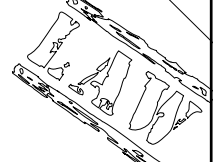
We Must Maintain a patient's privacy and confidentiality

❖ This information may include, BUT IS NOT LIMITED TO, the patient's:

- Physical condition
- Psychological or emotional status
- Financial situation



HHS
Office of Inspector General



Today Federal law mandates that ALL health care providers have ALL members of their work force participate in privacy training.



What is HIPAA?

HIPAA stands for the
Health
Insurance
Portability and
Accountability
Act of 1996



❖ The primary intent of **HIPAA** was to provide protections that would allow health insurance coverage for workers and their families when changing or leaving their jobs.

Protected Health Information

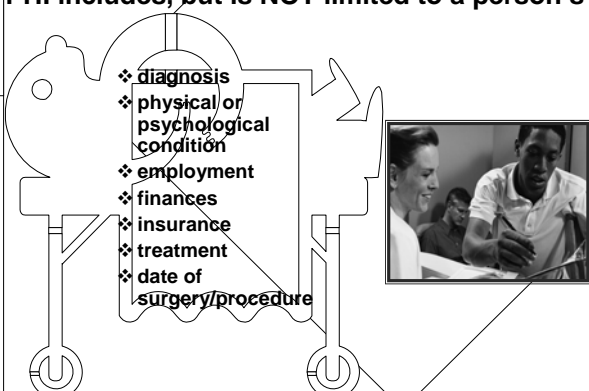
PHI: any protected health information linked to or leading to any personal identifying information

hSKI S KI

ePHI: any electronic form of protected health information linked to or leading to any personal identifying information

PHI includes, but is NOT limited to a person's

- ❖ diagnosis
- ❖ physical or psychological condition
- ❖ employment
- ❖ finances
- ❖ insurance
- ❖ treatment
- ❖ date of surgery/procedure



PHI is any health information that includes any of these identifiers:

- ❖ Name
- ❖ Address
- ❖ Employer
- ❖ Relatives' names
- ❖ Certificate/license number
- ❖ Telephone and fax numbers
- ❖ Date of Birth
- ❖ Date of Death
- ❖ All ages over 89
- ❖ Admission date
- ❖ Discharge date
- ❖ Social Security Number

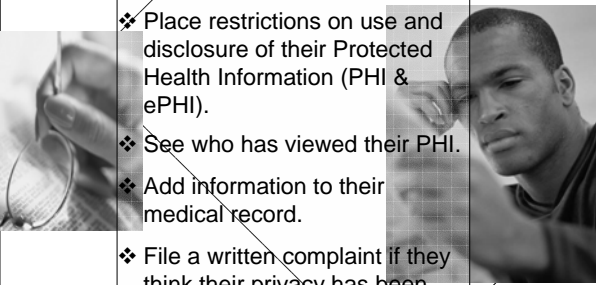
continued

PHI (continued)

- ❖ Health plan beneficiary numbers
- ❖ Member or account numbers
- ❖ Vehicle or other device serial numbers
- ❖ Any unique identifying number, characteristic, or code
- ❖ E-mail addresses
- ❖ IP addresses (Web URL)
- ❖ Medical Record Number
- ❖ Photos
- ❖ Photographic images

HIPAA Privacy Rules allow the patient to:

- ❖ Place restrictions on use and disclosure of their Protected Health Information (PHI & ePHI).
- ❖ See who has viewed their PHI.
- ❖ Add information to their medical record.
- ❖ File a written complaint if they think their privacy has been violated.

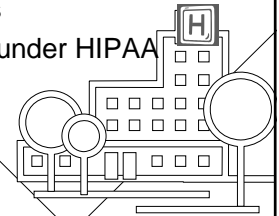


Notice of Privacy Practices

- ❖ **All** employees are expected to review the Hospital's Notice of Privacy Practices.
- ❖ The **Notice of Privacy Practices** explains the majority of what you need to know regarding HIPAA Policy.

Beaumont's Notice of Privacy Practices

- ❖ States how the Hospital can use a patient's PHI for purposes of:
 - Treatment
 - Payment and
 - Health Care Operations
- ❖ Describes patient rights under HIPAA
- ❖ Is available to all patients during the registration process



HIPAA Privacy Rules require:

- ❖ Safeguards and policies to protect PHI
- ❖ Policies and procedures to address breaches of patient's PHI
- ❖ A corrective action process if there is a breach of the patient's PHI
- ❖ A formal complaint process
- ❖ Designation of a Privacy Officer and an Information Security Officer
- ❖ Education/training

You may **NOT** reveal ANY patient information;

- **NO verbal**
- **NO written**
- **NO electronic**

without the patient's WRITTEN authorization.



HIPAA Compliance Structure at Beaumont

- ❖ The HIPAA structure follows the Corporate Compliance structure
- ❖ Each Department Compliance Coordinator has the HIPAA Privacy Compliance responsibility for their department

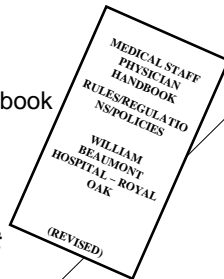
HIPAA Structure at Beaumont...

- Department Compliance Coordinators
- Privacy Officer
- Information Security Officer
- Corporate Compliance Officer

Beaumont Privacy Policies

❖ Privacy policies are included in the following:

- Management Manual
- Employee Handbook
- Medical Staff Physician Handbook Rules/Regulations/Policies
- Resident Handbook
- **Intranet – *Inside Beaumont***



HIPAA Related Policies

Confidentiality and Disclosure of Protected Health Information (PHI) Policy 314

- Release of information to outside agencies/general public
- Destruction of records
- Marketing
- Storage of inactive records
- Alias/Privacy status
- Subpoenas/Complaints
- Purchasing Policy
- News Media and police
- Code of Business Conduct
- Compliance education
- Compliance Audits
- Security Policy
- Internal communication
- Corrective action
- Informed consent
- Patient's rights and responsibilities

Maintaining Patient Privacy and Confidentiality is your

ETHICAL AND LEGAL OBLIGATION

Summary

- ❖ Trust is the key element in the relationships we have with our patients
- ❖ We all must maintain patient confidentiality as outlined in Policy #314, Confidentiality and Disclosure of PHI
- ❖ HIPAA has established Privacy Rules and introduced the terms, Protected Health Information (PHI) and electronic Protected Health Information (ePHI)

Summary

end of module 1

- ❖ Beaumont has established a Notice of Privacy Practices. Employees can view this document on the Corporate Compliance Web Page.
- ❖ There is a Corporate structure with HIPAA requirements, including the designation of a Privacy Officer and an Information Security Officer
- ❖ HIPAA Privacy Rules place restrictions on the access, use and disclosure of Protected Health Information, PHI

Patient Confidentiality Training

For ALL Members of Beaumont Hospital's Workforce

Module 2

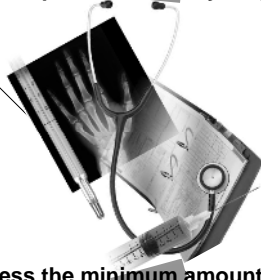
2008

Introduction- in this module you will learn:

- ❖ Appropriate and inappropriate use of a patient's Protected Health Information (PHI) and Electronic Protected Health Information (ePHI)
- ❖ Reporting breaches of a patient's privacy/confidentiality
- ❖ Potential consequences for a breach of a patient's privacy/confidentiality

Access to PHI

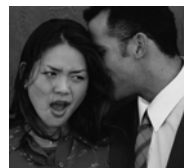
- ❖ Access patient information as it pertains to the performance of your job



- ❖ Access the minimum amount of information needed to complete your job

Breach of Patient Confidentiality

- ❖ The intent of a person who breaches confidentiality does not matter



- ❖ It is **NOT** necessary for a breach to be of a harmful or malicious nature



Some employees, such as licensed health care professionals (doctors, nurses, therapists and so on) may release, in the performance of their job, limited PHI without written authorization. If you are unsure, ask your manager or supervisor.

When can caregivers (nurses, therapists, etc.) disclose PHI without the patient's authorization?

- ❖ For treatment, payment and health care operation such as quality assurance, medical record review and education efforts

All other reasons require the patient's WRITTEN authorization, unless under an exception.

- ❖ If in doubt, complete the **Authorization for Release of Medical Information** form, in the Management Manual, Policy #314
- ❖ Contact your supervisor or manager for guidance

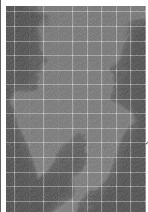
Caregivers can share PHI with the following individuals, unless otherwise directed by the patient:

- ❖ Next of kin

Spouse	Parents
Adult children	Siblings
- ❖ The individual that has durable power of attorney for health care or as the patient advocate
- ❖ Legal Guardian
- ❖ Designated Contact Person

Designated Contact Person

- ❖ The patient will be asked to identify a designated contact person upon admission to the hospital.
- ❖ This person's name will be entered into the admission assessment database for all hospital staff to use when they need to share protected health information (PHI).
- ❖ This person is someone from whom we can obtain and share information related to the patient.

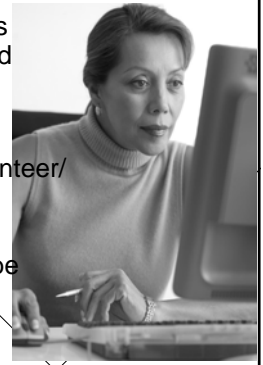


Designated Contact Person

- ❖ This person has no decision-making ability unless the person has the legal authority (with documentation) to do so.
- ❖ Those who do have the decision making authority are:
 - Legal Guardian
 - Durable power of attorney/patient advocate
 - Next of kin

Releasing Patient Room Number Information

- ❖ Due to patient privacy status concerns, it is recommended that all calls from the public for patient room number information be forwarded to the Hospital Operators/Volunteer/Information desk.
- ❖ Only the Information Desk feature on Patient1 should be used to release patient room number information.



There are 5 exceptions to the authorization requirement



1. Medical emergencies



2. Reporting information on communicable diseases to the Health Department

3. Reporting child abuse, spousal abuse or elder adult abuse

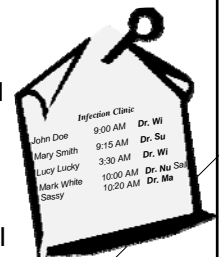


4. Organ donation activities

5. Disclosures required or allowed by law

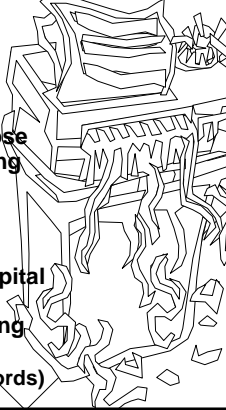
Activities to be avoided . . .

- ❖ Posting private patient information in public areas
- For example:** a schedule listing clinic patients scheduled for that day along with any PHI: the type of Appointment (Infection Clinic, and doctor)
- ❖ Leaving patient charts with PHI unattended - - always attend or secure PHI



Activities to be avoided. . .

- ❖ Leaving patient charts with PHI unattended - - always attend or secure PHI
- ❖ Disposing of paper records in waste baskets – you must dispose of them by shredding or recycling following the guidelines in the confidential recycling policy
- ❖ Removing hospital forms or report sheets with PHI from hospital property -- is not allowed they must be disposed of by shredding or appropriate recycling
(See Policy #111 - Destruction of Records)



Verbal Information

- ❖ Conversations you may have had or overheard need to remain private. These conversations may be with:
 - Patients
 - Family members
 - Physicians
 - Other staff
- ❖ DO NOT discuss patient care in inappropriate public places — such as elevators or a cafeteria



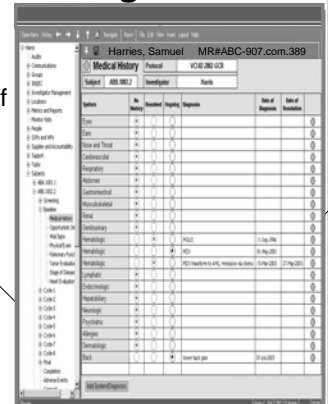
System Access

- ❖ Do not use clinical/business systems to look up phone numbers or addresses of co-workers, friends, family, etc.
- ❖ Do not use the clinical/business system to access information to satisfy curiosity about a patient, coworker, age, birth date, etc.
- ❖ Be especially careful with PHI about other employees. Employees have stated many concerns about the confidentiality of their PHI.



Employees Accessing PHI

- ❖ Employees cannot access medical information on behalf of friends or co-workers even with patient authorization
- ❖ If you notice a co-worker's name on a schedule, medical record or other paperwork, keep that information private



What is breach of confidentiality?

- ❖ Inappropriate access of Protected Health Information (PHI)

and/or

- ❖ Inappropriate disclosure of Protected Health Information (PHI)



To whom do you report suspected breaches in patient confidentiality?

- ❖ Your Supervisor/Manager
- ❖ Your Department Compliance Coordinator
- ❖ The Privacy Officer

248 - 55 - 15006

- ❖ HIPAA Information Security Officer

248 - 59 - 72471

- ❖ Hospital Compliance Line

1 888 495 5100

All reports will be investigated and remain confidential

What are the consequences of a breach of confidentiality?

- ❖ Anyone who inappropriately accesses or discloses PHI would be subject to disciplinary action, including:
 - Dismissal or loss of privileges
 - Civil or criminal penalties and sanctions, including:
 - Monetary fines
 - Imprisonment

Frequently asked questions (FAQ's) about PHI are:

- ❖ Can I have a conversation with a patient that will include such things as their treatment plan, tests scheduled or test results if others are present in the room?

Answer: Yes, if the patient has given you approval. State you are here to discuss their treatment, test or test result, and ask if it is acceptable to have this conversation with those present.

FAQ's, (continued)

- ❖ Can family members access an adult patient's chart without patient approval?

Answer: **Usually No** - There are times when they can. If you are unsure, call your manager or supervisor. Medical Information Services Department (MISD) and Legal Affairs should be consulted.

- ❖ Can the parent or guardian of a minor access that individual's medical record?

Answer: **Usually Yes** - There are times when they can not. Call your supervisor or manager. MISD and Legal Affairs should be consulted. Refer to Policy #314.

FAQ's, (continued)

- ❖ What should I do if I receive a subpoena for PHI?

Answer: Call your manager or supervisor. Medical Information Services Department (MISD) and Legal Affairs should be consulted.

- ❖ Can I send copies of PHI to a law office or court, upon request?

Answer: Yes, if the appropriate authorization is presented. Call your manager or supervisor. MISD and Legal Affairs should be consulted.

FAQ's, (cont.)

- ❖ What should I do if I am asked to do something and I don't know what I should do?

Answer: Call your manager or supervisor, MISD or the Legal Affairs department

- ❖ If I have access to the electronic medical record, can I look at my own Protected Health Information (PHI)?

Answer: Yes. You first **must complete and submit** an authorization form to view your own records, just as any other patient.

- ❖ Remember to treat ALL patient information as you would like to have your own personal information handled

- ❖ Use common sense

Golden Rule

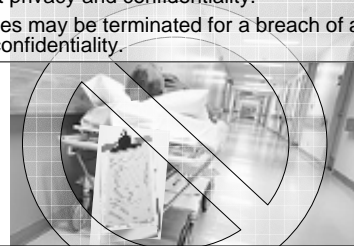
Do to others
What you would want
Them to do to you

Summary

- ❖ Keeping PHI secure is your responsibility.
- ❖ Access PHI only for your patient's benefit and only the minimum amount necessary.
- ❖ Patient PHI can be revealed for treatment, payment and health care operations or with the patient's **written** authorization.
- ❖ **Exceptions to the authorization requirements include: medical emergency, reporting abuse, reporting communicable disease, organ donation and those required or allowed by law.**

Summary

- ❖ Never post PHI in public areas or leave medical records/documents unattended or unsecured.
- ❖ Avoid disposing of all paper records in waste baskets – must dispose by shredding or recycling. Follow guidelines in the confidential recycling policy **Policy #111 - Destruction of Records.**
- ❖ There are penalties or sanctions associated with breaches in patient privacy and confidentiality.
- ❖ Employees may be terminated for a breach of a patient's privacy/confidentiality.



Patient Confidentiality Training

For ALL Members of Beaumont Hospitals' Workforce

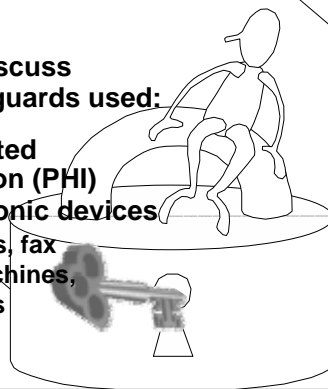
Module 3

2008

Introduction

❖ This module will discuss the Physical Safeguards used:

- Accessing Protected Health Information (PHI) when using electronic devices such as: computers, fax machines, copy machines, answering machines and e-mail



Physical Safeguards and Access Controls

Passwords

To protect against unauthorized access to Beaumont systems and networks, users must identify themselves through an authentication process.

❖ Carefully create and maintain your user passwords

- Passwords must be at least eight characters. Passwords must be letter and number combinations
- Passwords should be difficult to guess. Common words and simple number sequences (12345678), family names, or a special date are not recommended
- System Administrators can only reset a password, they cannot view passwords
- Users may change passwords at anytime. You are required to change your passwords every six months
- Do not write down passwords
- Regardless the circumstance, **passwords must never be shared or revealed to anyone**
- You are responsible for each system access related to your ID, regardless who may use it

Information Security

❖ Beaumont promotes information security awareness through training and education and verifies compliance with the Information Security Policy through internal and external audit



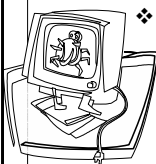
❖ Beaumont has the authority to monitor, audit, log, store, retrieve, destroy or process any electronic information crossing over or accessed from any of its networks. Including, but not limited to e-mail content, voice mail content, network addresses, frequency or occurrence, and identification of specific on-line services

- ❖ The Hospital routinely reviews each person's access into the system. This will show an **"audit trail"** of all the information you have accessed. This audit trail will be reviewed for the appropriateness of each access.



Viruses, worms - Malicious Software

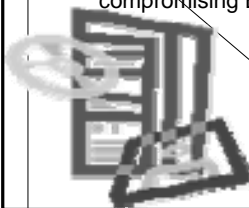
❖ All Beaumont hardware and software installations must be in compliance with the rules of Beaumont's **Information Security Policies, HIPAA Security Requirements**



❖ WBH may report any violation of local, state, federal or international laws to the appropriate authorities. Misuse of external networks in violation of this policy and/or other Beaumont policies may result in disciplinary action up to and including termination of employment or criminal or civil action

❖ Access to the Internet may be made only via authorized firewalls. Beaumont-approved firewalls are designed, operated, monitored, and regularly tested to support the following key technical security controls:

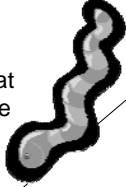
- Only authorized users to access the Internet
- Prevent any unauthorized user/system from compromising Beaumont systems or data



- ❖ Reduce vulnerabilities by visiting only reputable websites
- ❖ Avoid clicking on pop-ups. It's a good idea to close all pop-ups
- ❖ Access provides audit trails of user/system activity

❖ **Viruses** are programs or programming code that replicate by being copied to another program, document or computer boot sector. Viruses can destroy or alter information/applications

❖ A **WORM**, is a self-replicating virus that does not alter files but resides in active memory and duplicates itself. It is common for worms to slow or halt tasks, causing system performance to become slow



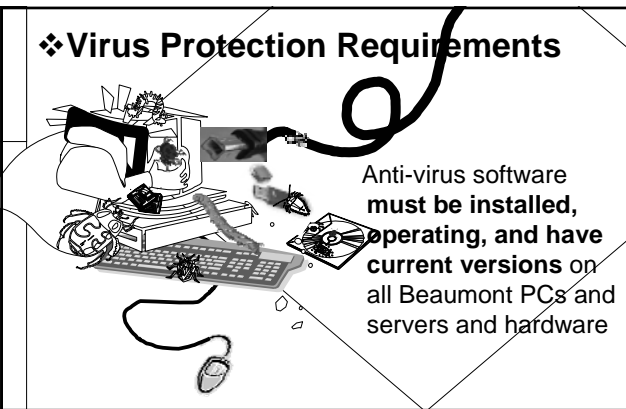
❖ **Spyware** is any technology that aids in gathering information about a person or organization without their knowledge. The collected information is then relayed to advertisers or other interested parties.



❖ Spyware is often installed on a computer as part of a software installation/download process

❖ Virus Protection Requirements

Anti-virus software **must be installed, operating, and have current versions** on all Beaumont PCs and servers and hardware



Safeguards when using computers to access PHI

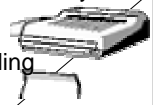
- ❖ PHI should only be accessed when you are actively involved in treatment, payment or healthcare operations
- ❖ Accessing information for personal interest when you are not actively involved in the person's care **is not permitted**
- ❖ Secure all media that contains PHI (such as CD's, diskettes, memory sticks and so on)
- ❖ Do not use media from unknown sources, unless you first check them for viruses (call the Help Desk x72727)



- ❖ **DO NOT** have PHI displayed on your computer screen when you are not using it
- Position your monitor so others cannot easily read it
- Activate the password protection screensaver. Set it to come on after a specific period of no activity
- Consistently log off or lock computer when you leave your workstation. Press Ctrl-Alt-Del simultaneously and then select the **Lock Workstation** button
- A procedure should be in place for backing up data. A secondary copy of files should be stored on a separate device or location

Physical safeguards when faxing PHI

- ❖ Faxed requests for information may not be legitimate
- ❖ Verify that the fax machine to which you are sending information is secure
- ❖ Follow the guidelines in Policy #314, Confidentiality and Disclosure of PHI
- ❖ Dial fax numbers carefully to avoid sending information to the wrong party



- ❖ Use programmable keys for frequently dialed fax numbers - - such as nursing homes or third party payers
- ❖ **Always** use a coversheet with a Confidentiality Notice (available on web page)
- ❖ Facsimile software or systems that automatically dial patient information in fax format must be tested at any new location before patient information is sent out.
- ❖ Each fax system will maintain an audit trail

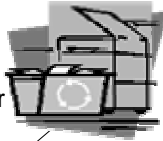
- ❖ Read only those faxes addressed to you

- ❖ If you receive faxed PHI intended for someone else, notify the sender and then destroy the information



Physical safeguards when using copy machines

- ❖ When you are done, be sure to remove all documents from the copier
- ❖ If you find originals in copier, DO NOT read them
- ❖ Dispose of unneeded copies in an appropriate manner, by shredding or recycling following the guidelines in Confidential Recycling, Policy # 111



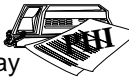
Physical safeguards when using the telephone

- ❖ Employees must be aware that while retrieving voice mail/answering machine messages using a speakerphone the information is at risk of exposure
- ❖ DO NOT read PHI over the telephone. Follow the guidelines in Policy #314, **Confidentiality and Disclosure of PHI**



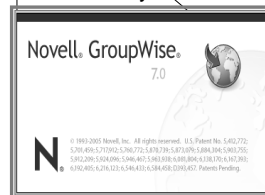
Physical safeguards when using answering machines

- ❖ Listen to phone messages where others will not overhear PHI
- ❖ When you need to use the phone to relay PHI, make sure you are talking to the right person. **DO NOT** leave messages containing medical information on answering machines. The wrong person may access the information



Physical safeguards when using E-Mail

- ❖ E-mail containing PHI should be exchanged only in appropriate circumstances and only with proper security measures
 - ❖ E-mail guidelines are contained in the Security Policy Guidelines, Policy #222

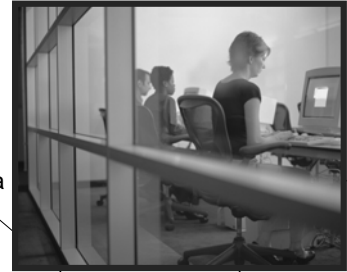


- ❖ Do not e-mail PHI or important information across the Internet and expect it to be secure. A tool, SecureFile, is available to securely communicate data. For more information call the Help Desk at ext. 72727

- ❖ Do not open e-mails or attachments from unknown or untrusted sources, select DELETE to remove
- ❖ E-mail from a Beaumont GroupWise account to a Beaumont GroupWise account **is secure**
- ❖ Accessing private e-mail systems (AOL, Hotmail, Yahoo, Comcast, etc.) using Beaumont network equipment is discouraged – it raises the risk of virus infections



- ❖ Make sure the sender's and receiver's e-mail accounts cannot be accessed by others.
- ❖ Remember, e-mail sent or received on a workplace e-mail system is not private and can be viewed by others.

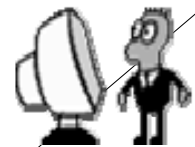


Summary

- ❖ Your password is an example of a physical safeguard that Beaumont requires when accessing PHI on computers
- ❖ When using technology to view or send PHI, follow the guidelines in Policy #314, Confidentiality and Disclosure of PHI
- ❖ All Beaumont hardware and software must be in compliance with the rules of Beaumont's **Information Security Policies, HIPAA Security Requirements.**
- ❖ Dispose of PHI in an appropriate manner, by shredding or recycling following the guidelines in Confidential Recycling, Policy # 111



- ❖ Current anti-virus software must be installed, and operating on all Beaumont PC's and servers
- ❖ Access information about patients **only** when you are actively involved in treatment, payment or healthcare operations
- ❖ Always log off or lock your computer when you leave your workstation exchanged only in appropriate circumstances and only with appropriate security measures
- ❖ Do not e-mail PHI or important information across the Internet, to a non-Beaumont GroupWise user unless you use an encryption tool such as SecureFile



Conclusion

end of module 3

- ❖ Always report security incidents, problems or suspicious behavior regarding electronic PHI (ePHI), software or hardware to the HIPAA Information Security Officer and the Help Line at x72727



- ❖ If you have additional questions about confidentiality policies or wish to make a suggestion on how to improve patient information confidentiality, please contact:

The Privacy Officer

248 - 55 - 15006

The HIPAA Security Officer

248 - 597 - 2800

Hospital Compliance Line

1-888- 495-5100

All reports are investigated and remain confidential

Patient Confidentiality Training

For all All Members of Beaumont's Workforce

Post Test Assessment with Remediation

Question 1:

Who is responsible for maintaining patient confidentiality at Beaumont Hospital?



- Everyone who takes care of patients
- Everyone who is a member of the Beaumont work force
- Everyone who enters the patient's room
- Everyone who talks to the patient

Question 2:

When using computers to access PHI, which of the following must you do?



- Activate the password protection on the Screensaver feature
- Position your monitor so non-employees cannot easily read it.
- Log off or lock your computer when you leave your workstation (Ctrl-Alt-Del)
- All of the above

Question 3:

Protected Health Information (PHI) is any health information that also includes any personal identifiers, such as name, date of birth, admission/discharge date, health plan numbers and others.



- True
- False

Question 4:

A patient has a right to place restrictions on who has access to their medical information?



- True
- False

Question 5:

When can you release information without the patient's authorization?



- During medical emergencies
- When reporting suspected child abuse, spousal abuse or elderly adult abuse
- When reporting information on communicable diseases to the Health Department
- During organ donation activities
- All of the above

Question 6:

If, upon investigation, it is determined that your ID was used to inappropriately access PHI, you will be held responsible?



- True
- False

Question 7:

The Hospital routinely looks at your access into the electronic system. This will show an "*audit trail*" of all the electronic records you have viewed.



- True
- False

Question 8:

What does a **breach of confidentiality** mean?



- Talking to someone involved with the patient's care about Protected Health Information (PHI)
- Not getting authorization each time you access PHI
- Keeping everything to yourself
- Inappropriate access/disclosure of PHI

Question 9:

The intent of/reason a person who breaches confidentiality does not matter.



- True
- False

Question 10:

If you suspect a breach in confidentiality or security you should call:



- Your Supervisor/Manager
- Your Department Compliance Coordinator
- The Privacy Officer
- Information Security Officer
- Hospital Compliance Line
- Any of the above

Question 11:

Maintaining confidentiality is your ethical and legal obligation. Every health care worker is obligated to keep **ALL** information concerning patients and their PHI confidential.



- True
- False

Question 12:

A "designated contact person" is:



- This person is one with whom we can share and obtain information about the patient.
- This person is entered into the admission assessment database upon being admitted to the hospital.
- Has no decision-making ability unless they have the legal authority to do so (next of kin, legal guardian, or durable power of attorney or patient advocate).
- All of the above

Question 13:

It is appropriate to e-mail PHI to someone who is outside the Beaumont organization, outside the GroupWise system and without using a security system such as SecureFile?



- Usually
- Never
- If you are using a security system such as Secure File
- If you know the recipient

Question 14:

Passwords should be changed every six months and should not include common words, simple number sequences, family names or a special date.



- True
- False

Question 15:

Beaumont Hospitals has the authority to monitor, audit, log, store, retrieve, destroy or process any electronic information crossing over or accessed from any of its networks.



- True
- False

Question 16: Confirmed violations of **Information Security Policies** and/or other WBH policies will result in disciplinary action up to and including:



- 1. WBH may report any violation of local, state, federal or international laws to the appropriate authorities
- 2. Automatic Suspension
- 3. Termination of employment, and criminal or civil action
- 4. Automatic warning, with a written counseling
- 1 and 3
- 2 and 4

Question 17: When accessing electronic PHI, how much of the electronic record can you view?



- 1. The entire record
- 2. The progress notes
- 3. the nurses notes
- 4. What is necessary within the scope of your job
- 1 and 3
- 2 and 4

Question 18

Warning! !

Breach of confidentiality is a serious event and all employees confirmed to be involved in inappropriate access or sharing of PHI
WILL BE TERMINATED ! !

Acknowledge the statement below to continue with the test:
"I understand any employee confirmed to be involved in a breach of confidentiality WILL BE TERMINATED."



- I acknowledge my awareness that if I am found to be involved in a breach of confidentiality, I will be terminated from employment with William Beaumont Hospital.

Corporate Compliance



An important subject affecting everyone within the organization



2008

Introduction

This lesson provides information about healthcare compliance and why it is important.

Everyone who works for a health care organization must know and obey the laws, rules and regulations affecting their jobs.

When we comply (follow) the healthcare provider laws, rules and regulations it is called ***compliance***.

Failure to follow the laws, rules and regulations is called ***noncompliance***.

2

Objectives

After reviewing this lesson, you should be able to answer the following questions:

- What does compliance mean?
- Why compliance is important?
- What agencies are responsible for creating compliance laws, rules, regulations and penalties?
- Who, at Beaumont, is responsible for Compliance?
- What are the 7 Elements of Beaumont's Corporate Compliance Plan?
- How you can communicate compliance concerns?

3

What does ***compliance*** mean?

Compliance means:




- Conducting business in a legal and ethical manner
- Following healthcare laws and regulations while doing your job
- Following Beaumont's Code of Business Conduct
- Each employee committing to do their *job the right way*



4





What is the “Right Way?”

Doing your job the right way means you:

-  Know
-  Understand and
-  Follow the laws, rules and regulations that apply to your job



5

Why compliance is important?

-  It protects patients' rights and their privacy
-  It guards the safety of patients and employees
-  It protects employees and the community at large
-  It prevents possible errors, waste and fraud that can result in penalties or sanctions enforced upon Beaumont Hospitals and/or employees

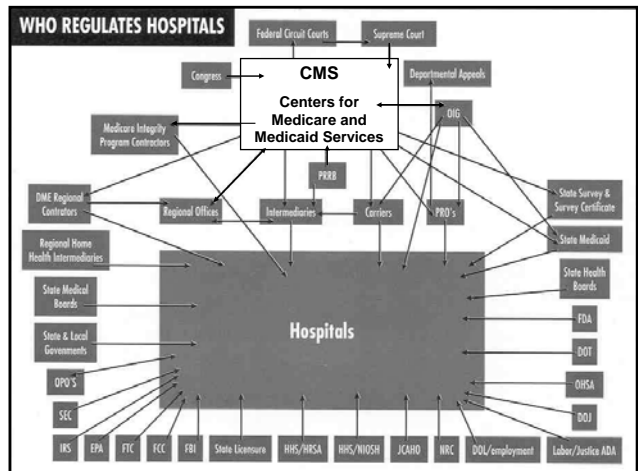
6

Who regulates hospitals and healthcare providers?

-  Congress passes healthcare laws. These laws are managed through the Department of Health and Human Services (HHS).
-  The Centers for Medicare and Medicaid Services (CMS), a division of HHS, sets the rules and regulations to follow in order to receive proper payment from Medicare or Medicaid.



7



Reasons to Comply

- 🔨 **Criminal and Civil Penalties**
 - Imprisonment or loss of License
- 🔨 **Monetary penalties**
- 🔨 **Corporate Integrity Agreement**
 - Government's Compliance Program
- 🔨 **Excluded from participation in Government programs**
- 🔨 **Loss of Public Trust**



9

Who is responsible for Compliance?

ALL Beaumont employees, physicians, students, volunteers, etc!

Every member of Beaumont's Health Care Team is responsible



When we follow the laws, rules and regulations that apply to our jobs, we are in *Compliance*.

10

What you need to know about Compliance

- 🔨 Know and follow the content of the Code of Business Conduct, Corporate Compliance Policy #350.
- 🔨 Attend compliance education and training sessions.
- 🔨 Know the laws, rules and regulations that apply to your job.
- 🔨 Ask questions when you are not sure.
- 🔨 Report potential compliance concerns.



11

Beaumont's Corporate Compliance Plan

- 🔨 Has 7 key elements
- 🔨 Was approved by the Board of Directors
- 🔨 **We are all responsible to follow it**

12

7 Elements of the Corporate Compliance Plan

1. Written Policies and Procedures

- ✎ Management Policies
- ✎ Department Policies

2. Official Personnel

- ✎ Corporate Compliance Officer
- ✎ Business Ethics & Corporate Compliance Committee



Ed Grima,
Corporate Compliance Officer

Dr. Mark Kolins,
Business Ethics & Corporate
Compliance Committee

7 Elements of the Plan (cont.)

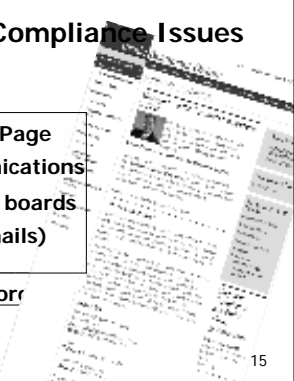
3. Compliance Education and Training for all employees

- ✎ The Corporate Compliance Office provides education on the Corporate Compliance Plan
- ✎ Individual departments provide training on specific policies, rules, laws and regulations that apply to that department
- ✎ Annual compliance education via Pathlore

7 Elements of the Plan (cont.)

4. Communication of Compliance Issues

- ✎ Corporate Compliance Web Page
- ✎ Beaumont Specific Communications
- ✎ Brochures, Posters, Bulletin boards
- ✎ Phone calls, GroupWise (emails)
- ✎ Meetings, inservices
- ✎ Department Compliance Coor



15

7 Elements of the Plan (cont.)

4. Communication (cont.)

Who can you call?

- ❖ Your Supervisor or Manager
- ❖ Your Department Compliance Coordinator
- ❖ Corporate Compliance Officer
 - Ed Grima
Ext.-15004
- ❖ Privacy Officer
 - Doug Clarkston
Ext. -15006
- ❖ Information Security Officer
 - Larry Randolph
Ext. 72471
- ❖ The Compliance Line
 - 1- 888-495-5100
(24 hours)

All reports remain confidential and will be investigated

1

16

7 Elements of the Plan (cont.)

5. **Enforce** compliance standards through investigation, education and communication and, if necessary, disciplinary actions.
6. **Monitors and Audits** allow the Department Compliance Coordinator *and* Compliance Team to **Support** the Corporate Compliance Plan and the Department Compliance Plans.
7. **Respond** in a timely manner to all reports or suspicions of potential non-compliance.

17

Beaumont Hospitals has a Decentralized Approach to Compliance

- Each department compliance plan also has 7 elements
- Each department has identified the department specific risk areas (areas where regulations apply)
- Each department has a Department Compliance Coordinator who is responsible for:
 - Department specific education and communication
 - Reviewing and updating the plan, annually at minimum
 - Keeping employees informed and up to date

Who is your Department Compliance Coordinator?

(If you don't know, ask your supervisor or check the Corporate Compliance website)

Conflict of Interest/Disclosure of Remuneration Policy #351

What is Conflict of Interest (COI)?

COI = When an employee or family member has a financial interest, or any interest in another organization that has business relationships with Beaumont **and/or** when the employee might be able to influence business decisions with Beaumont may be a COI and therefore must be disclosed for evaluation and determination

Who can COI impact?

All employees – especially those who represent Beaumont in business relationships, or who make recommendations regarding the position of Beaumont in those relationships

19

COI, Policy #351 (cont.)

What is Your responsibility

Self-disclose and report any known potential or actual conflict of interest to the Corporate Compliance Officer

Do Not participate in any kind of financial or personal obligation or interest, which affects your judgment in internal or external business matters for Beaumont

Ask the Corporate Compliance Officer, if not sure whether a situation or circumstance may be a COI.

20

COI, Policy #351 (cont.)

Remuneration

Compensation for services, for any reason, to or from any individual/entity that has any past, present, or prospective future business dealings with Beaumont if the compensation might be construed as preventing the employee from acting in the best interest of Beaumont or in any way competes with Beaumont

Examples:

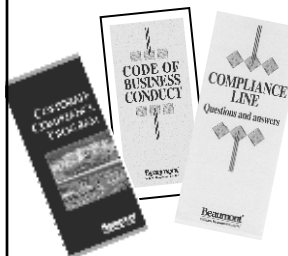
Borrowing Money
Gifts, Gratuities & Tips
Honoraria

Acceptance of Entertainment
Travel Expenses
And more ..



Tools of Beaumont's Compliance Program

- Tools provide the information you need to maintain compliance with federal and state rules/regulations and internal guidelines which guide healthcare delivery



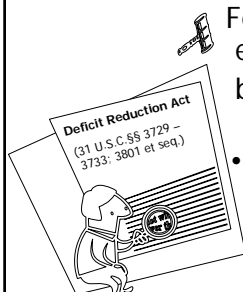
22

False Claims Acts

Education

Federally mandated: employee education beginning January 1, 2007

- The result of the *Deficit Reduction Act*



23

False Claims Acts

- What are they?

🔑 Federal Law

(31 U.S.C. §§ 3729 – 3733; 3801 et seq.) All types of federal claims (a federal act establishing the rules and regulations; applicable to most situations where federal dollars are involved)

- Statute dates back to the Civil War
 - Amended in 1986 to combat **all** forms of government procurement and contracting fraud, including Medicare/Medicaid fraud
 - Imposes civil liability on any individual or entity that knowingly submits, conspires to submit, a false claim to the federal government

24

False Claims Acts *(cont.)*

- 🔑 **Michigan Laws**
 - (M.C.L.A. 400.607 (Medicaid))
 - (M.C.L.A. 752.1003 (All non-government health claims))
 - Prohibit a person from making or presenting or causing to be made or presented a claim for payment of health care services knowing the claim to be false

25

Examples of False Claims

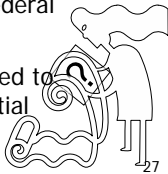
Claims that are:

- 🔑 Based on services that were not actually rendered or costs that were not actually incurred
- 🔑 Contain information that is not accurate or is misleading about the quality or type of services or products supplied
- 🔑 Payments made, which, by law, the claimant was not allowed to receive
- 🔑 Contain false or misleading pricing information

26

How Does This Affect You?

- 🔑 All employees should report compliance concerns internally via the Compliance Line, which can be done anonymously if preferred.
- 🔑 You have the right, under the law, to report any potential issues of non-compliance at Beaumont Hospitals to state and federal administrative agencies.
- 🔑 By law, organizations are not allowed to penalize callers for reporting potential compliance issues.



27

How Beaumont Prevents and Detects Fraud, Waste and Abuse

- 🔑 Developed an internal Corporate Compliance Program approved by the Board of Directors
- 🔑 Appointed a Compliance Officer and Business Ethics and Corporate Compliance Committee with responsibility to oversee the Corporate Compliance Plan
- 🔑 Publishes and makes readily available compliance brochures/programs to all employees
 - Corporate Compliance Program
 - Code of Business Conduct
 - Compliance Line

28

How Beaumont Prevents and Detects Fraud, Waste and Abuse, cont.

- 🔑 Promotes and conducts training programs for all employees to ensure awareness of ethical and legal standards
- 🔑 Promotes reporting of potential concerns internally
- 🔑 Investigates and resolves **all** reports of potential non-compliance

29

Corporate Compliance Office Roles and Responsibilities

- 🔑 Oversight of the Compliance Program and related activities
- 🔑 Effectively implement and manage the Corporate Compliance Plan
- 🔑 Provide administrative, education, compliance audit and communication activities

30

Corporate Compliance Office Activities

Administrative

- 🔑 Shared governance with the Business Ethics and Corporate Compliance Committee
- 🔑 Ensures compliance with ethical and professional standards of conduct, as well as with all of the laws and regulations affecting WBH health care operations, business practices, and revenue cycle
- 🔑 Assures corporate business integrity with regulatory areas via the Code of Business Conduct, and other Beaumont compliance policies
- 🔑 Facilitate interactive communication

31

Corporate Compliance Office Activities, cont.

Education

- 🔑 Provide compliance education in a variety of venues to assist staff in performing their jobs the right way, the first time, and in accordance with rules and regulations
- 🔑 Develop and implement education as identified via audit outcomes

Audit

- 🔑 Proactively conduct reviews and analyze outcomes to identify:
 - ❖ Compliance with regulatory risks
 - ❖ Areas for opportunity and education

32

Corporate Compliance Office Activities, cont.



Communication

- ✎ Effectively communicate the content and purpose of the Corporate Compliance Plan
- ✎ Provide a mechanism (Corporate Compliance website) to provide up to date compliance information

33

In Summary

- Compliance is doing business in a legal and ethical manner
- There may be penalties (sanctions) for non-compliance
- Being "Compliant" allows Beaumont Hospitals to receive proper payment for services provided
- Each of us is responsible for Compliance
- The **Right Way** is: knowing, understanding and following the laws, rules and regulations that apply to your job
- Three brochures that provide compliance information are: Corporate Compliance Program, The Code of Business Conduct and The Compliance Line
- Compliance polices are located on "*Inside Beaumont*"



You
Are the
Key

Doing the Right Thing
The Right Way
The First Time

35

Name: _____

Date _____

Compliance Annual Training

1. What does **compliance** mean?
 - a. Conducting business in a legal and ethical manner
 - b. Following healthcare laws and regulations while doing your job
 - c. Following Beaumont's Code of Business Conduct
 - d. Each employee committing to do their job as quickly as possible
 - e. All of the above
 - f. a, b, and c
 - g. None of the above

2. Doing your job the right way means you know, understand and follow the laws, rules and regulations that apply to your job.

 True False

3. Compliance does not affect our patients.

 True False

4. There are just a few regulatory and enforcement agencies that manage the laws, rules and regulations.

 True False

4. Which of the following is a penalty or sanction to the employee or hospital for **noncompliance**?
 - a. Probation or imprisonment
 - b. Monetary fine
 - c. Not allowed to participate in government programs
 - d. All of the above
 - e. A and B

5. **DO NOT** do which of the following?
 - a. Know and follow the content of the Code of Business Conduct, Corporate Compliance Policy #350.
 - b. Attend compliance education/training sessions.

11. Compliance means:

- a. Never making a mistake
- b. Never talking about PHI
- c. Doing the right thing, the first time
- d. Doing what is ethical and legal

- 1. A and B
- 2. C and D
- 3. None of the above
- 4. All of the above

13. Confidentiality is not part of BeaumontHospitals' Compliance Program

_____ True ____ False

14. Which of the following is NOT an example of remuneration and isn't COI?

- a. Gifts, gratuities and tips
- b. Accepting entertainment
- c. Hourly salary
- d. Borrowing money
- e. Travel expenses

15. Of the following, which is the BEST answer to the question: Who is responsible for compliance at WBH?

- a. Administrators
- b. Hourly employees
- c. Professional staff
- d. We are all responsible
- e. Department leaders
- f. Department Compliance Coordinator

16. Passwords should be changed every six months and should not include common words, simple number sequences, family names or a special date.

_____ True ____ False

Acknowledgment Of
Code Of Business Conduct, Compliance Line and Corporate Compliance Plan

I acknowledge that I have completed the Compliance module and have reviewed the Beaumont Code of Business Conduct, Beaumont Compliance Line and Corporate Compliance Program informational brochures.

I have a clear understanding of the business ethics standards of William Beaumont Hospital. I fully understand that, I have an obligation to exercise good judgment and be committed to upholding Beaumont's standards of integrity and ethics.

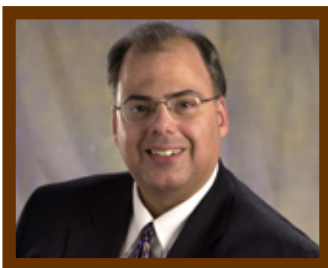
When I have a question or concern about a possible violation of Hospital Policy or a potential compliance issue, I will promptly report the concern to either my:

- Department Compliance Coordinator
- Department Manager
- Department Medical Chief
- Contact the Compliance Line
- Corporate Compliance Officer

in accordance with the Corporate Compliance Program.



I acknowledge awareness of the three brochures and agree to uphold Beaumont's standards of integrity and ethics.



Edward Grima,
Corporate Compliance Officer



Confidentiality & Systems Usage Agreement

I. Confidentiality

There are moral, ethical, and legal responsibilities to maintain the confidentiality of patients' personal and medical information, whether that information is verbal, written, printed, or electronic. There are similar responsibilities regarding confidential information of William Beaumont Hospital (WBH) itself. Confidential information is defined as patient care or WBH business information which is not for the public domain. Confidential information is sensitive and valuable and is protected by law and by strict WBH policies.

I understand that any access or disclosure of confidential information, except for approved job-related uses, is strictly prohibited. If involved in clinical care, I will retrieve or attempt to retrieve from WBH medical records or computer systems data for only those individuals with whom I have a patient care relationship, or for approved educational, administrative, or research purposes.

I understand that I have no right or ownership interest in any confidential information referred to in this Agreement. WBH may at any time revoke my access to confidential information.

I will discuss confidential information only as required by my work, and only with authorized persons who have a work-related need to know such information. I understand that confidential information is not an appropriate topic in casual conversation. I will avoid discussing confidential information in public places such as elevators or cafeterias, and will take care to avoid being inadvertently overheard while communicating or dictating such information.

I will exercise appropriate care when storing, transporting, photocopying, disposing of, or faxing confidential information. I will take precautions to avoid having computer monitors, printers, fax machines, or paper records in view of unauthorized onlookers while such data is displayed.

I understand that I am responsible for all data, information, and orders which are entered into any WBH system using my ID. I will not reveal, release, or make accessible any WBH system user ID/key/password I may have to others. I will not allow anyone else to access, enter, or alter information in a WBH system under my identity. I will not use the ID/key/password of anyone else in order to access any WBH system.

I understand that WBH may maintain electronic logs of user access to any WBH information system, and may audit these logs at any time to detect inappropriate use. I will report any improper use, access, or disclosure of confidential information that I observe.

II. Systems Usage

As part of my employment, service, association, or privileges with WBH, I may have need to access various WBH computer systems. I understand that use of this information infrastructure is a privilege, and that inappropriate use may result in denial of access to these systems.

I will not seek personal benefit or permit others to benefit personally by any confidential information or use of equipment available through my association with WBH. I will not install or operate any non-licensed software on any computer provided by WBH. I will not make unauthorized copies of WBH software for use by myself or others.

Confidentiality & Systems Usage Agreement (continued)

I understand that WBH-provided Intranet/Internet access and applications, including electronic mail and web browsers, are intended for job-related activities only. My use of the Intranet/Internet may be electronically logged and reviewed by the appropriate WBH administrative bodies.

I understand that WBH reserves the right to retrieve and read any data, documents, or communications composed, sent, received, or stored in its computer systems. All such information is considered to be part of the official records of WBH and, as such, may be subject to disclosure under the law or to third parties. Consequently, I will ensure that information I communicate in any WBH system is accurate, appropriate, ethical, and lawful.

III. General

I understand that my obligations regarding confidentiality under this Agreement will continue even after termination of my employment, service, association, or privileges with WBH. I understand that if I breach the terms of this Agreement, WBH may institute disciplinary action up to and including termination of my employment, service, association, or privileges with WBH, as well as possible legal action under state or federal law.

I understand that any relevant WBH policies, rules, or regulations remain applicable, in addition to the standards described above. By signing this document, I agree to abide by and uphold the above standards.

Signature

Name (Printed)

/ /
Date

Employee/Physician ID (if applicable)

Department/Office/Facility/Agency

Work Telephone

February 14, 2005

Dear Schools of Allied Health Visitor:

It is **mandatory** that all visitors to the Schools of Allied Health who are visiting areas of possible exposure to blood or other body fluids participate in an **infection control program**.

This requirement can be met by:

Reading the enclosed Infection Control Review.

Completing the enclosed test.

Signing the Acknowledgement Form stating that you have received this information and understand the necessary precautions you should take while visiting the department.

Bring the completed test and signed Acknowledgment form with you when you visit.

Should you have any questions regarding this information please call the Schools of Allied Health at 248-898-8047.

Thank you,

Ann F. Sosnowski
Manager
Beaumont Schools of Allied Health

Infection Control Review for Schools of Allied Health Visitors

Any person may have a disease found in the blood or other body fluids. Standard Precautions (formerly Universal Precautions) are designed to reduce the risk of transmission of microorganisms from both recognized and unrecognized sources of infection in hospitals.

The following **STANDARD PRECAUTIONS** are used for all patients, regardless of their diagnosis:

- **Handwashing:** Handwashing is frequently called the single most important measure to reduce the risk of transmitting infection. Hands must be washed:
 - After touching blood, body fluids, or contaminated items, whether or not gloves are worn.
 - Wash hands immediately after gloves are removed, as well as before, and after touching a patient.
 - Hands must also be washed before touching our eyes, nose or mouth, as well as before touching food, and after using the restroom.
- **Gloves:**
 - Gloves must be worn before touching blood or other body fluids.
 - Gloves are also worn if we touch a patient's eyes, nose or mouth, or to touch the patient if he or she has non-intact skin (including a rash).
 - Remove gloves promptly after use, (and wash hands) before touching clean items and environmental surfaces.
- **Gown:** Wear a cover gown to protect skin and to prevent soiling of clothing during procedures and patient care activities that are likely to generate splashes or sprays of blood or body fluids.
- **Patient Care Equipment:** Handle used patient-care equipment soiled with blood or body fluid in a manner that prevents skin and mucous membrane exposures, contamination of clothing, and transfer of microorganisms to other patients. Ensure that reusable equipment is not used for the care of another patient until it has been cleaned or reprocessed appropriately.
- **Linen and Laundry:** Soiled linen should be handled as little as possible and with minimum agitation to prevent gross microbial contamination of the air and of persons handling the linen. Soiled linen is placed in an impervious laundry bag.
- **Dishes, Glasses, Cups and Eating Utensils:** No special precautions are needed for dishes, glasses, cups, or eating utensils. The combination of hot water and detergents used in the hospital dishwashers is sufficient to decontaminate dishes, glasses, cups and eating utensils.

Additional Transmission-Based Precautions are used for patients documented or suspected to be infected or colonized with highly transmissible or epidemiologically important organisms for which additional precautions beyond Standard Precautions are needed to interrupt transmission.

Schools of Allied Health Visitors are not to enter any patient rooms with Isolation or Transmission Precautions signs on the door. The types of isolation or additional precautions in use at Royal Oak Hospital include:

Airborne Transmission Precautions (yellow sign)

Droplet Transmission Precautions (lime green sign)

Contact Transmission Precautions (orange sign)

Additional Contact Transmission Precaution for VRE (hot pink sign)

Immuno/myelo-suppression Precautions (turquoise sign)

Hepatitis B and C, HIV and other Bloodborne Pathogens:

Schools of Allied Health Visitors, may be exposed to bloodborne pathogens by a sharp object contaminated with blood or other potentially infectious material, if it punctures or cuts the skin (percutaneous); splash or spray of blood or other potentially infectious material into the eyes, mouth or nose (perimucosal); or contact with blood or other potentially infectious material with non-intact skin i.e., cuts, scraps, abrasions etc. (non-intact skin). If you are exposed to blood or potentially infectious body fluid, you must:

- Report to the supervisor, and or the manager of the unit where you were exposed. He/She will:
- Help you fill out an Accident and Incident Report, form 553, and send you to:
- Employee Health Services or the Emergency Department for post-exposure care
- It is very important that you follow-up with *your personal physician* after your post-exposure care

Tuberculosis:

Schools of Allied Health Visitors may potentially be exposed to patients with unrecognized respiratory tuberculosis, who are not on effective anti-tuberculosis therapy, and who have not been placed in Airborne isolation. Persons with respiratory TB can generate tiny particles (droplet nuclei) when they cough, sneeze, sing, or even talk. These particles stay suspended in the air, and can spread throughout a room or building. Although TB is airborne, meaning that people can be infected simply by breathing air contaminated with infectious particles, it is not especially infectious. In fact, only 32% of household contacts of persons with TB become infected.

A PPD skin test is used to identify persons who have been infected with tuberculosis. A positive skin test tells us that a person has breathed in a TB organism at some time during their life, and that their body has reacted to it. Infection with tuberculosis does not mean that one has active TB disease. In fact, only 5 to 10% of all persons with a positive skin test ever develop active disease. All employees, volunteers, and students at WBH must be skin tested for TB annually. This tells us (and you) if you have been exposed to TB during the past year. Once a person has a true positive skin test (a raised, hardened area, if it is only red, it is not positive) they should not be skin tested again. A chest x-ray will be taken at the time of the positive skin test, and one year later. Further x-rays are not indicated. The following group of symptoms in a person with a positive skin test may indicate active TB infection, and should be reported to your physician:

- Rapid, unexplained weight loss
- Night sweats,
- Cough that continues for more than 2 weeks
- Fatigue, loss of appetite, generally feeling “blah”

We make all efforts to rapidly identify any patients with symptoms suggestive of tuberculosis, and place them into Airborne Isolation. Special airborne isolation rooms are designed to prevent any infectious particles from leaving the room. These rooms have negative pressure, and all potentially infected air is exhausted directly outside, where UV light from the sun kills it. All persons entering the room must wear special N-95 masks. Schools of Allied Health Visitors should **NOT** enter these rooms, when there is an airborne isolation sign on the door.

In addition to protecting our visitors from exposure to infection at work, we also protect our patients from possibly infectious healthcare workers/volunteers/students. All visitors should be immune to measles, German measles, (rubella, rubeola), and chickenpox. Persons with symptoms of infectious disease should not come to work. Remember to take the flu shot annually, to protect yourself, and our patients.

Please call the Department of Epidemiology at 248-551-4040 if you have any questions about Infection Control.

INFECTION CONTROL REVIEW QUESTIONS

1. Standard precautions are used for all patients, regardless of their diagnosis. The most important of these are handwashing and the use of gloves.

True False

2. Soiled linen should be handled as little as possible and with minimum agitation.

True False

3. Dishes, glasses, cups and eating utensils, need no special precautions as the combination of hot water and detergents used in the hospital is sufficient to decontaminate the dishes, glasses, cups, utensils.

True False

4. Additional precautions are sometimes needed for patients and there will be signs on the patient's doors to alert you. Volunteers are not to enter these patients' rooms.

True False

5. Volunteers may be exposed to bloodborne pathogens by a sharp object contaminated with blood or other potentially infectious material. If you are exposed to blood or any potentially infectious body fluid, you must report this to your supervisor immediately.

True False

6. TB tests are done annually for all volunteers, this would tell us if you have been exposed to TB during the past year. Although TB is airborne, meaning that people can be infected by breathing air contaminated with infectious TB particles; it is not especially infectious. In fact, only 32% of household contacts of persons with TB become infected.

True False

7. Volunteers that work in areas designated as "at risk" of blood/body fluid exposure are eligible and encouraged to receive free Hepatitis B vaccine through Employee Health Service.

True False

8. Individuals who are infected with Human immunodeficiency virus (causative agent of Aids) can look healthy (asymptomatic), yet be infectious to other people.

True False

ACKNOWLEDGEMENT OF
INFECTION CONTROL REVIEW FOR SCHOOLS OF ALLIED HEALTH VISITORS

I acknowledge that I have read the Infection Control Review for Schools of Allied Health Visitors and have a clear understanding of the Standard Precautions I should be using while visiting the department.

I have completed the test.

Date

Signature

Printed Name

School of Allied Health Visiting

