



# Everything You Always Wanted to Know About HIPAA

## A Self Study Packet for the JHH Department of Nursing

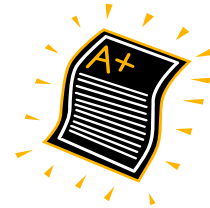
Updated April 2005



### Introduction

This self-study packet is designed to help you understand the HIPAA regulations and how they affect you. It contains key concepts related to:

- A. General privacy issues
- B. Electronic protected health information
- C. Tracking and accounting for disclosures of health information
- D. Release of patient information



After reading the information, you will take a posttest.

### Objectives

After completing this packet, you will be able to:

1. Identify HIPAA, why it became a law, how it is enforced, and its requirements.
2. Define PHI, guiding principles, use, and disclosure.
3. Identify the rights given to patients under HIPAA.
4. Identify what types of disclosures must be accounted for and tracked.
5. List what information must be provided for each accounting of a disclosure.
6. Identify the type of PHI that can be released under various circumstances.



## A. General Privacy Issues



### What Is HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) is a federal law that governs the use, transfer, and disclosure of identifiable health information.



### Why Was the New Law Passed?

It was clear that patient information was being used in ways that violated the privacy rights of individuals. The government reacted by passing a federal law to protect the privacy and confidentiality of identifiable health information.

## HIPAA Privacy Regulations include new:

- Rights for patients
- Privacy requirements for healthcare providers.

**These new rights and requirements went into effect April 14, 2003, and apply to apply to ALL Johns Hopkins staff, students, and faculty.**



## What is Identifiable Health Information?

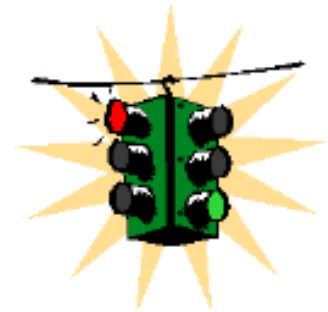
HIPAA protects individuals' **identifiable** health information. Identifiable information is any information about **living or deceased** persons':

- Health conditions – diagnosis, test results
- Demographic information – name, address, gender
- Clinical data – vital signs, lab results, etc.
- Treatments & procedures
- Department where the patient was seen or the name of the physician if this information could reveal the diagnosis or condition of the patient
- Billing and payment information

The HIPAA Privacy Regulations protect identifiable health information in any form – on paper, electronic (computer), recorded, or spoken. When Hopkins creates or receives this information, this information is called "protected health information" (PHI).

## Examples of HIPAA Violations Include:

- Accessing health information of coworkers, family members, or celebrities.
- Throwing PHI into the trash.
- Sharing patient information with those who do not have a need to know.
- Telling friends or relatives about patients in the hospital.
- Sending PHI in emails.
- Discussing PHI in public areas, including elevators, the cafeteria, hospital lobbies.
- Discussing PHI on the phone in public areas.
- Leaving PHI unattended in public areas.
- Failing to log off computer systems containing patient information.



## Non-compliance with HIPAA regulations can result in:

- Fines for institutions of up to \$100 for each violation and up to \$25,000 for all violations of the same type during the calendar year
- Individual criminal penalties up to \$250,000 and imprisonment of up to 10 years for intentional use of patient identifiable information for "commercial advantage or malicious harm."



The federal Office of Civil Rights is charged with enforcing HIPAA regulations. If an employee sees another staff member or student misusing PHI, the incident may be reported to the JH Compliance Hotline 1-877-WE COMPLY or 1-877-932-6675 (toll free).

## How to Dispose of PHI



Documents containing PHI should be disposed of in a secure way. They should be shredded or put in secured bins for later shredding or incineration. PHI should not be placed in trashcans or recycling bins or left accessible to people who do not require access to the PHI.

## Important Principles & Definitions:

The HIPAA Privacy Regulations are governed by two main principles:

1. Need-to-Know
2. Minimum Necessary



### 1. "Need to Know" – What information do you need to know to do your job?

- **Example 1:** A nurse needs access to PHI to provide care for patients on his/her unit. However, the nurse does not need to have access to PHI for those patients who are not on his/her unit.
- **Example 2:** A security guard needs access to the name and location of patients to guide visitors if necessary. However, the guard does not need access to other PHI such as diagnosis, the treatment plan, etc.
- **Example 3:** A worker wants to send a birthday card to a coworker but he/she is not sure of the exact date. The worker knows the coworker was a patient at Hopkins and wants to look up the coworker's birth date in the Electronic Patient Record (EPR). The worker does not have an official or professional need to know the birth date of the worker's friend and may not get the birth date from EPR.

### 2. "Minimum Necessary" - Are you using or disclosing the smallest amount of PHI necessary to complete the job?

In most instances, you should use your professional judgment to determine what amount of PHI is necessary to complete the given task.

- **Example 1:** To submit a claim for reimbursement, a billing person needs to view the patient's current visit information but does not need the entire patient history. Therefore, the patient's current visit information would be the minimum necessary amount of PHI the billing person would need to complete the task.
- **Example 2:** A nurse is putting together a case study for teaching purposes. The nurse has a need to know patient information but does not need to use the patient's name, social security number, or other identifying numbers to teach the class. The nurse should block these items when making copies for the class.



## The Difference between "Use" and "Disclosure"



- **“Use” = sharing of PHI within the Hopkins family**, which includes JHH, Bayview, Howard County General Hospital, JH Home Health Services, JH Pediatrics at Home, JH Pharmaquip, JH Community Physicians, Priority Partners Managed Care Organization, JH Ophthalmology Associates, JHU School of Medicine, JHU School of Nursing, and parts of the Bloomberg School of Public Health, the Whiting School of Engineering, and the School of Arts and Sciences, Kennedy Krieger Institute.
- **“Disclosure” = sharing of PHI with any person or entity not within the Hopkins family**, such as consultants, outside counsel, or sponsors of research.

## Patient Rights Under HIPAA

HIPAA creates new rights for patients with respect to their own health information, including the right to:

1. Receive a Notice of Privacy Practices about how Hopkins will use and disclose their PHI
2. See their PHI and to get a copy of their PHI
3. Request that their PHI be amended if they believe Hopkins has recorded their PHI incorrectly
4. Request an accounting of disclosures of PHI
5. Request restrictions on the use of PHI
6. Ask for confidential communications



For each of these rights, JH must have a policy.

### Right #1 - Right to Receive the Privacy Notice

- Patients have a right to a clear and complete notice of Hopkins' privacy practices, which includes the uses and disclosures that Hopkins may make of their PHI. All patients will be given the “Notice of Privacy Practices” and will be asked to sign an acknowledgment that they got the notice.
- If the patient or the patient's representative refuses to sign the acknowledgement of receipt, the Hopkins representative must document the refusal. In this case, Johns Hopkins may still provide care to the patient and continue to use and disclose the patient's PHI according to the notice of privacy practices.
- Each patient only needs to receive one Notice of Privacy Practices. However, until JH develops a system to keep an accurate record of which individuals have received the Notice, it will be necessary to determine whether the individual has received the Notice at each encounter. If the individual has not, the Notice must be given and the good faith effort to obtain their acknowledgment must be made.



## Right #2 - Right to Access PHI

- Individuals generally have the right to see and get copies of their medical treatment and billing records. However, there are some exceptions to this right. For example, patients do not have a right to see or get copies of their psychotherapy notes or information put together for use in a legal proceeding.
- If an individual asks you to see his/her medical record or to copy it, he/she should be referred to the Medical Records Department or the HIPAA Office.
- Family members, close friends, or other designated persons may only access an individual's PHI if the provider reasonably believes from all the circumstances that the individual is involved with the patient's care or billing and the patient does not object. You may allow a person to act on behalf of a patient to pick up a filled prescription, medical supplies, x-rays, or other similar forms of PHI.

## Right #3 - Right to Request an Amendment to PHI

- Individuals have a right to request an amendment to their medical treatment and billing records.
- Hopkins does not have to make the change if Hopkins did not create the PHI and the doctor who created the record is still available.
- If Hopkins finds that the PHI is, in fact, accurate and complete, Hopkins does not have to agree to make the amendment.
- If an individual asks to amend their medical or billing record, you should refer him or her to the Medical Records Department. JH must respond to the request within 60 days.

## Right #4 - Right to Request an Accounting of Disclosures of PHI

- This will be covered in depth later in this packet.

## Right #5 - Right to Request Restrictions on the Use of PHI



- Individuals may ask Hopkins not to use their PHI in certain ways. For example, an individual may ask that a false name be used if he/she is famous or do not want friends or family to know that he/she is a patient. Hopkins does not have to agree to the request, but when Hopkins does agree, Hopkins must implement adequate controls to ensure that the request is followed.
- Hopkins currently allows the masking of VIP names from the Hopkins inpatient directory and paper medical charts. Hopkins intends to continue this process.

## Right #6 - Right to Request Confidential Communications

Individuals may ask Hopkins to use a different way of getting in touch with them. For example, they may not want any regular mail and may only want communication by email. They also may ask that Hopkins use a different address to protect the person's confidentiality. If you are asked to do this, you should comply with the request so long as it is reasonable to do so. However, Hopkins may use the non-confidential address or number if the other methods of contact are unsuccessful.



## Privacy Authorizations

**A “Privacy Authorization” must be obtained from the patient if the provider wishes to use or disclose PHI for a purpose other than treatment, payment, or healthcare operations.**

The following are examples of activities that use PHI and require a Privacy Authorization:

- Fundraising (other than use of demographic data)
- Marketing\*
- Research
- Photographing or filming or including patient information in publications

\*JH may market it’s own products & services to patients without obtaining a Privacy Authorization. However, providing patient names and demographic information to outside companies is considered marketing.

Patients may cancel their authorizations at any time.

If you participate in any of the activities mentioned above, you are required to complete a HIPAA course on that topic(s). See <http://www.insidehopkinsmedicine.org/hipaa/> for more information.

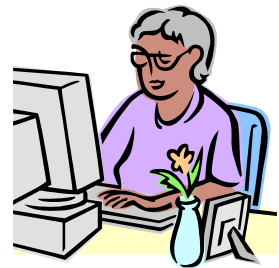
---

## B. Electronic PHI

**HIPAA Security requires security and confidentiality of protected health information in electronic form (E-PHI), which is often maintained on computers and portable devices or transmitted electronically.** (These new HIPAA Security regulations become effective and enforceable as of April 20, 2005.)

How you use your computer/public workstations can impact the security and privacy of patient information. To protect E-PHI, follow these steps:

- Keep your user IDs and passwords to yourself.
- Make your passwords hard to guess and change it frequently.
- Use only the computer systems, programs, and files you are authorized and required to access to perform your job.
- Avoid sending PHI in emails over the internet.
- Save PHI only to a secure network, not to your local PC drive or portable device.
- Beware of downloading or opening software, documents, or email attachments from unknown, untrustworthy sources.
- Log off or lock your computer when not in use.
- Seek approval from your system administrator before installing computer programs.
- Use and update antivirus software regularly.
- Report all security incidents to the HELP Desk or your LAN administrator.



## Reporting security incidents:

Even with good security habits, there will be incidents from time to time that need reporting. Such an incident could be:

- Belief that someone is using your account when you were not using it
- Unauthorized access to steal or alter data
- Unauthorized access to gain the ability to monitor computer activity
- Tampering with or destroying a computer, handheld device, or server
- A computer virus

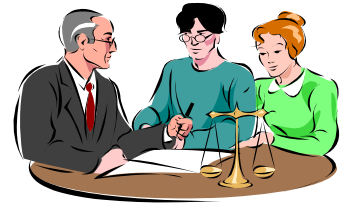
---

## C. Tracking & Accounting for Disclosures of PHI

---

### Disclosures of Health Information

- As previously mentioned, a "disclosure" of PHI occurs when PHI is shared outside of a covered entity for any purpose. Disclosures include sharing of PHI with non-Hopkins care providers, other parts of The Johns Hopkins University not covered by HIPAA, contractors, consultants, outside counsel, research sponsors, government agencies, payers, or an individual's family members.
- The HIPAA Privacy Regulations require covered entities to account for certain disclosures of PHI. This means that Hopkins must keep track of to whom a disclosure was made, what PHI was disclosed, when the disclosure occurred, and why. The purpose of this requirement is so that patients may know how their PHI is being shared.
- All Hopkins personnel should continue to comply with the Maryland requirements for tracking disclosures of patients' medical records.



### Disclosures that Do NOT Need To Be Accounted For

Some disclosures do not need to be accounted for. They include:

1. Those made in the course of treatment
2. Those made in connection with payment.
3. Those made in carrying out health care operations.
4. Those made to the patient him/herself.
5. Those authorized by the individual patient.
6. Those made to persons involved in the individual's care.
7. Those made in a covered entity's facility directory.
8. Those made for disaster notification purposes.
9. Those made for national security purposes as permitted by HIPAA.
10. Those for law enforcement purposes relating to correctional facilities.
11. Those that are incidental to uses or disclosures otherwise permitted by HIPAA (Example: A physician, speaking quietly to a patient about her health condition, is nevertheless overheard by the patient in the next bed.)
12. Those that are made as part of a "limited data set."



## Disclosures That DO Need To Be Accounted For Include:



1. Disclosures used in certain research activities
2. Disclosures required by law, such as:
  - **Court** ordered subpoenas
  - Requests from the government for information to investigate JH compliance with HIPAA
  - Information provided to Medicare/Medicaid
3. Disclosures for public health activities, including:
  - Reporting of diseases, injury, births and deaths, etc.
  - Information given to government agencies for their oversight of healthcare and government benefit programs
4. Disclosures about victims of abuse, neglect or domestic violence
5. Disclosures for health oversight activities, including:
  - Reports to the FDA and the manufacturer if a medical device causes or contributes to the death or serious injury of one of our patients
  - Notification of person who may be at risk of contracting or spreading an infectious disease or condition
  - Information to an employer to evaluate work-related illnesses and injuries so the employer may comply with Occupational Safety and Health Administration (OSHA) rules.
6. Disclosures for law enforcement purposes, including:
  - Reporting gunshot wounds to law enforcement authorities.
  - Information provided upon request of a law enforcement official for the purpose of locating a suspect or fugitive. (Note: There are significant restrictions on these types of disclosures. Contact Hopkins' Privacy Officer prior to making these types of disclosures.)
7. Disclosures to coroners and funeral directors, including:
  - Disclosures to coroners and medical examiners to identify a person or determine cause of death.
  - Disclosures to a funeral directors
8. Disclosures for organ & tissue donation purposes
9. Disclosures for cadaveric organ, eye, or tissue donation purposes.
10. Disclosures to avert a serious threat to health or safety (Example: If a patient threatens to harm someone else and the threat is serious and imminent, we may, under certain circumstances consistent with our ethical obligation to warn an intended victim, disclose the patient's PHI to someone in a position to reduce the threat.)
11. Disclosures for certain specialized government functions (Example: If we treat a patient the government believes may be a threat to the President, we may disclose PHI to a government agency, such as the FBI or Secret Service.)
12. Disclosures for workers' compensation

## How to Account for Disclosures

For each of the disclosures described above, the accounting must include:

- The date of the disclosure
- The name of the entity or person who received the PHI
- The address of the entity or person, if known
- A brief description of the PHI disclosed
- A brief statement of the purpose of the disclosure that simply informs the individual why the disclosure was made

Until Hopkins develops a database to record, store, and access these reports, you should fill out the reporting form for each disclosure and put it in the person's medical record.

## D. Release of Patient Information

The HIPAA Privacy Regulations require that the patient must be told about the use of the information and must be given the opportunity to object to or restrict the use or release of the information. However, Maryland law is stricter and therefore Hopkins must follow Maryland law, which:

- Allows a facility directory to contain the patient's full name, location in the health care facility, and the patient's condition, as described in general terms that do not communicate specific information about the individual.
- Only allows a directory to be retained for inpatients, not outpatients.
- Restricts the types of patients who may be added to the directory without objection. For example, psychiatric patients must opt-in to the directory.



### Inpatient Directory



The JHH will continue to maintain an inpatient directory. When a patient is admitted to the hospital, emergency department, or outpatient surgery units, the Admitting Office or intake department must tell the patient about the facility directory.

If the patient objects to being included in the directory, the patient must sign the Request for Non-Disclosure of Facility Directory Information Form, which will be placed in the patient's medical record.

The inpatient facility directory may not contain the following types of inpatients:

- Patients in a psychiatric unit (unless they opt-in by written consent)
- Patients who are involved in an alcohol or drug-treatment program

Disclosure to confirm or deny the presence of psychiatry patients will be permitted in accordance with state and federal laws. We may confirm or deny the presence of a psychiatry patient:

- To a parent, guardian or next of kin
- To any individual who has a significant interest in the status of the patient if they have filed a missing persons report regarding the patient
- To respond to a court order
- As required by law



Patients who are involved in an alcohol or drug-treatment program are entitled to complete confidentiality, including whether they are in fact participating in the program or not. We may confirm or deny the presence of a drug and/or alcohol abuse patient in a program only as required by law.

Generally, the release of any information concerning the HIV/AIDS status of a patient is prohibited under state law. Additionally, we must be cautious about releasing information about any patient associated with the commission of a crime or where the safety and security of both patients and hospital personnel may be jeopardized.

## Outpatients

Johns Hopkins will not maintain a directory of outpatients. At registration, patients will be notified that they will be unable to be contacted or located while they are in our facility.

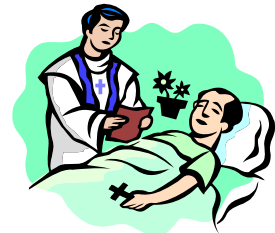


## Minors

Minor children (under the age of 18) may have information released with the consent of a parent or legal guardian, in accordance with the guidelines listed above. Minors under age 18 who are authorized to consent generally (e.g., married) are authorized to consent to specific medical procedures under state law retain control over the use and disclosure of their health information.

## Clergy

Members of the clergy frequently request access to names and locations of patients in our facilities to determine if members of their congregations have been admitted. Clergy may have access to the patient's location (i.e., building and room) as long as the patient agrees to be in the facility directory.



## Emergency Circumstances

In an emergency treatment circumstance Johns Hopkins may use or disclose an individual's information if the use or disclosure is:

- Consistent with a prior expressed preference of the individual, if any, that is known to Johns Hopkins; **and**
- In the individual's best interest as determined by the patient's physician, in the exercise of professional judgment

Once the patient is no longer incapacitated, JH must tell him/her about the facility directory and his/her right to be excluded. At that point, we need to honor the patient's agreement or objection to being included in the facility directory.

## Emergency Medical Services (EMS)

EMS units or ambulance services that provide health care services to patients are considered covered entities under HIPAA and are subject to the same restrictions on use and disclosure of a patient's information as Hopkins.



## Disasters

Johns Hopkins may disclose information regarding a patient's health to a public or private entity authorized by law to assist in disaster relief efforts. Information also may be released to these types of organizations for the purpose of contacting a family member, personal representative, or person directly responsible for a patient's care.

## Deaths

Johns Hopkins must report patient deaths to authorities as required by law. Typically, public information about a death will be disclosed after efforts have been made to notify the next-of-kin. Information about the cause of death must come from the patient's physician, and a legal representative of the deceased must approve its release. This means that hospitals cannot share information with the media on the specifics about sudden, violent, or accidental deaths, or deaths from natural causes, without the permission of the decedent's next-of-kin or other legal representative.



Although hospitals have traditionally released information about patient deaths to the media upon request, HIPAA allows the disclosure of such information only in response to certain law enforcement inquiries; to coroners, medical examiners, and funeral directors, to allow them to do their jobs; and to family, a personal representative, or another person directly responsible for the patient's care. Reports to public health authorities in their role of collecting vital statistics also are an exception. If a patient is deceased, no matter if the body is still present in our facility or not, we will not inform the requestor that the patient is deceased, unless authorized by law or the patient's personal representative. No other details about the circumstances, time, cause, etc., may be released without written authorization from the patient's representative.

## Media Access to Patients

Public Affairs should be contacted whenever the media wants to interview or photograph a patient.

- Public Affairs must obtain the patient's authorization before releasing the patient's PHI (i.e., even his/her name and contact information) to the media.
  - A personal representative may also sign the authorization on behalf of the patient (e.g., the parent or legal guardian may sign for the minor).
  - If the patient is under arrest, permission also must be obtained from the law enforcement officer in charge of the patient's custody.



- An authorization to photograph or interview patients remains in effect for one year, unless a patient cancels the authorization.
- Media representatives who are interviewing patients should be accompanied by Public Affairs or other appropriate staff at all times while in our facilities.

The HIPAA Privacy Regulations limit the information about patients that members of the media may have access to. The following are some questions that may help clarify the types of PHI that media will be able to access.

- **Question:** If a reporter is covering a traffic accident and calls the hospital asking for information about the condition of a vehicle's occupants, citing the location of the accident but not the victims' names, may the hospital provide a condition report?  
**Answer:** Information in the directory (e.g., patient location) may be released *only* if the media or the public asks for the patient by full name and only if the patient has not objected to or restricted the release of such information. If a patient is unable to communicate for the purpose of objecting to or restricting the use of directory information, this information may be released only if any past preferences are known and disclosure is in the best interests of the patient, in the professional judgment of the medical services provider.
- **Question:** What if the reporter asks about the accident victim by name?  
**Answer:** If an individual, including a representative of the media, asks for information about the patient by name, only location and condition may be released, and only if the patient has not objected to or restricted the release of that information.
- **Question:** What if a reporter calls with information that is already part of the public record, such as name or condition of the patient obtained from police reports?  
**Answer:** If the reporter has the patient's name, he/she may access the patient directory. However, if the reporter tries to gain additional information about the patient on the basis that the name and condition are already part of the public record, this request should be denied. Members of the media often obtain police reports and other information about hospital patients. The claim is frequently made that once information about a patient is in the public domain, the media is entitled to any and all information about that individual. This is not true. Johns Hopkins must observe the general prohibitions against releasing patient information found in the HIPAA Privacy Regulations, state statutes or regulations and the common law, regardless of what information is in the hands of public agencies or the public in general. Requests for a patient's health information from the media on the grounds that a public agency, such as law enforcement, is involved in the matter should be denied.

---

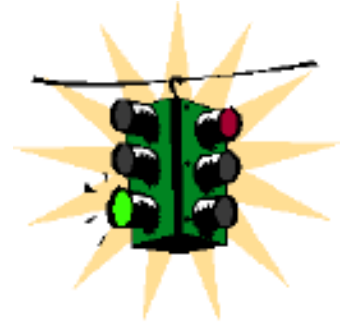
## Conclusion

---

Good work! You finally made it through the summary of the complex HIPAA Privacy Regulations.

In conclusion, to comply with HIPAA regulations:

- Treat all patient information with the utmost concern for confidentiality and privacy.
- Access only the information you need to do your job.
- Refer patient information questions to the appropriate department.
- Account for disclosures of health information as required.
- Release patient information in accordance with HIPAA regulations.
- Dispose of documents containing health information appropriately.



If you would like more information, login to take the complete HIPAA Office online courses at <https://secure.lwservers.net/>.

If you have any questions, contact the HIPAA Office via email at [hipaa@jhmi.edu](mailto:hipaa@jhmi.edu) or see <http://www.insidehopkinsmedicine.org/hipaa/>

Please take the test now. You may do this in one of two ways:

1. Take the paper/pencil test on the next page. Submit it to your nurse manager or nurse educator. Your manager/educator will correct your test and submit your completion record to the HIPAA Office.
2. Go to the online General Privacy Issues course at <https://secure.lwservers.net/>. Login to the course. Click through the course content pages until you get to the posttest. Take the test online. The test will be scored automatically and a record maintained in the HIPAA Office automated system.

You must get a score of 75% to pass the test. Go for it! You can do it! Thanks for taking your time to complete this training.

## JHH Department of Nursing - HIPAA Posttest

Name \_\_\_\_\_ ID badge # \_\_\_\_\_ Date \_\_\_\_\_

Job title \_\_\_\_\_ Nursing unit \_\_\_\_\_ Dept. \_\_\_\_\_

TRUE	FALSE	
_____	_____	1. The HIPAA Privacy Regulations go into effect April 14, 2003.
_____	_____	2. The new law was passed because some people were misusing patients' identifiable information.
_____	_____	3. If Maryland law re: privacy is stricter than HIPAA, we must follow the Maryland law.
_____	_____	4. Only staff who provide direct patient care must follow the HIPAA Privacy Regulations.
_____	_____	5. Violations of HIPAA regulations may lead to fines or criminal penalties.
_____	_____	6. Throwing PHI in a non-secure trashcan without shredding it is an acceptable way of disposing of PHI.
_____	_____	7. HIPAA Privacy Regulations only apply to a patient while he/she is alive.
_____	_____	8. Identifiable information includes a patient's name, address, gender, diagnosis, and test results.
_____	_____	9. To protect E-PHI, you should keep your user IDs and passwords to yourself and log off your computer/public workstation when not in use.
_____	_____	10. Under HIPAA, all patients have a right to receive a Notice of Privacy Practices.
_____	_____	11. HIPAA requires Hopkins to get a patient authorization if Hopkins wants to use the patient's health information for other than treatment, payment, or healthcare operations.
_____	_____	12. If PHI is shared between JHH and JH Pediatrics at Home, this is considered "use."
_____	_____	13. "Disclosure" is considered sharing of PHI with any person/entity NOT within the Hopkins family.
_____	_____	14. The "Need to Know" principle asks if you need to know patient information to do your job.
_____	_____	15. The "Minimum Necessary" principle asks if you are giving the patient at least the minimum amount of information for him/her to do self-care post discharge.
_____	_____	16. Patients do not have a right to see or get copies of psychotherapy notes or information for a legal proceeding.
_____	_____	17. Staff, students, and faculty whose responsibilities include research, fund raising, or marketing need to complete the online HIPAA course on these topics.
_____	_____	18. Reporting of diseases to public health agencies as required by law, births, deaths, and suspected cases of abuse do NOT need to be tracked as disclosures.
_____	_____	19. If a member of the clergy calls to see if a member of his/her congregation has been admitted, the patient's name and location may be given if the patient is in the hospital directory.
_____	_____	20. Public Affairs should be contacted whenever the media want to interview or photograph a patient.

4/8/2005