Dear Colleague:

The Health Insurance Portability and Accountability Act (HIPAA) went into effect on April 14, 2003.

As a member of the YNHH Medical Staff, it is important for you to understand the policies and operational requirements that the Hospital must implement to be in compliance with HIPAA regulations.

An *Executive Summary* of the new policies and *Highlights of HIPAA at YNHHS* containing important information relative to your activity as a member of the YNHH Medical Staff follow this page.

Please read this information, complete, sign and date the brief Post-Test and return it with your application.

Satisfaction of the above will serve as our record that you have familiarized yourself with YNHH HIPAA policies and understand the importance of adhering to these policies and good practice to satisfy the requirements of HIPAA.

Thank you in advance for your attention to this important matter.

Sincerely,

Peter N. Herbert, M.D.
Chief of Staff

Enclosures

Note: For reference, the full YNHHS HIPAA policies can be temporarily accessed from any YNHHS computer at: http://intranet.mis.ynhh.com/ynhhs/resources/hipaa/index.html. Under HIPAA Resources select "Task Force Meetings," then "Privacy/Med Records" or "Security," then "Policies & Procedures."

Highlights of HIPAA at YNHH

The Notice of Privacy Practices. At first entry to our hospital, patients will be given the Notice to sign as an acknowledgment that they understand how we will use their Protected Health Information (PHI) for the purposes of treatment, payment, and certain operations to improve our clinical effectiveness. They will also learn of their rights under HIPAA to access their medical record, request an amendment to their record, request an accounting of disclosures of their PHI outside of treatment, payment, and operations (TPO), request a restriction or confidential communication, file a complaint, and opt out of our facility directory. We will flag in our systems that the patient has received our Notice.

Research. In order to access patient information for any research-related purpose, including pre-research reviews, a **Request for Access to PHI for a Research Purpose** form will need to be completed. For individuals who are not full-time faculty members or YNHHS attending physicians, appropriate signatures will also need to be obtained to access records for reviews preparatory to research or research on decedents. Requests to access records for research approved by the IRB will need to be accompanied by a copy of the Research Authorization or waiver.

Marketing Authorizations. You are allowed to discuss with a patient health related products and services provided by YNHHS facilities, as well as for treatment of the individual, case management/care coordination, or to recommend alternative treatments, therapies, healthcare providers or settings of care. A patient's authorization will need to be completed in order to provide the patient's PHI to an outside company for the purposes of marketing the outside company's products or services.

E-Mail and Electronic Messaging. Use of commercial e-mail services such as Hotmail and AOL to transmit PHI is not permitted given that the information can be easily intercepted. E-mailing and messaging is allowed within the firewalls of our facilities across the Health System and Yale University. MDLink, a secure web portal, is also an acceptable option.

Faxing. Transmitting PHI via fax is allowed, as long as care is taken to confirm the receiver's fax number, and any fax sent from a YNHHS facility includes the following confidentiality disclaimer:
"This message originates from Yale New Haven Health System. The information contained in this message may be privileged and confidential. If you are the intended recipient, you must maintain this message in a secure and confidential manner. If you are not the intended recipient, please notify the sender immediately and destroy this message. Thank you."

Verification. If the patient (or the patient's legal personal representative) has not provided consent, we need to be careful about to whom we disclose patient information. In regard to unknown callers/individuals who claim to be family members, please first verify that the patient has not opted-out of the facility directory (688-4242), or has placed restrictions on his/her PHI (e.g., an alias). The unknown individuals should then be asked to verify a few patient identifiers such as address, date-of-birth, or social security number before information is disclosed. It is a good rule of thumb in these instances to share general information about the patient's condition only, unless it is evident from the conversation that the individual already knows more than this. Use common sense. In addition, before discussing a patient's condition and treatment in the company of visitors, politely ask the visitors to leave. The choice is then left up to the patient to voice whether the visitors should stay.

Patient's Right to Their Record. Patients may request access to their PHI by submitting a completed **Authorization for Access/Release of Information** form to the Medical Records or Billing Department. For requests from inpatients, you may be asked to review the record with them or to identify a clinician designee to do so, similar to current practice.

Patient's Right to Request an Amendment of Their Record. Patients will need to complete and submit a **Request for Amendment to Protected Health Information Retained in Designated Record Sets** form to the Medical Records or Billing Department. You will receive a copy of the patient's request with a cover letter explaining that you may deny the request for amendment, accept the request, or accept the request as an alternative opinion. The patient would then be notified of your decision.

Patient's Right to an Accounting of Disclosures. If you disclose PHI outside of normal TPO, which the patient has not authorized, such as for reviews preparatory to research; to the state for public health reporting; to coroners, medical examiners, funeral directors, and for cadaveric organ donation purposes; in response to valid subpoenas or court orders; for health oversight or law enforcement requests, for worker's compensation reporting, etc., please be aware that these disclosures must be documented and tracked. Please contact Jean Pawlich (jean.pawlich@ynhh.org) and Jean Ahn (jean.ahn@ynhh.org) via email or at 688-8605. Patients may request an accounting of disclosures of their PHI by completing the **Request for Accounting of Disclosures** form.

State Laws. A state law preemption is in effect, which means that if state law is more stringent it would supersede the HIPAA regulations. HIPAA also contains an exception for any reporting specifically required for state law (e.g., abuse and neglect reporting).

Privacy Officer. HIPAA questions and complaints regarding Yale-New Haven Hospital or System facilities should be referred to the Office of Privacy and Compliance at 688-8416.

Portable Electronic Devices/Working Offsite. Any device containing or storing PHI (e.g., laptops, PDAs) must be password protected and secured when not in use. In addition, any PHI used or accessed should be safeguarded at all times, regardless of device used or location.

Presenting at Conferences. All identifying information needs to be masked or removed from slides, photographs, overhead transparencies, other media used, and handouts in order to keep the patient's identity confidential. In addition, please pick up any remaining copies following meetings and make sure that they are disposed of appropriately.

Disposal of PHI. Locked confidential bins are now located on each unit at the hospital. The contents will be shredded. Use these bins to destroy written PHI. Please see full policy for other types of media.

Good Faith Efforts. Not all of our areas of the hospital allow for confidential communications with patients or the secure storage of PHI. What is asked for are good faith efforts and reasonable measures. For example, turn charts over at the nursing station, pull curtains, talk in hushed tones if possible, use empty conference rooms where available, and avoid conversations in public areas such as elevators, hallways, and cafeterias. When you know it is unavoidable that others will hear your attempts at private conversation, let the patient know that you value keeping their information private and ask if they'd prefer another method to collect or discuss their PHI, particularly if it concerns HIV, drug and alcohol, or mental health information.

Executive Summaries of YNHHS HIPAA Policies

PRIVACY SUMMARIES:

Patient's Right to Access Protected Health Information (PHI)

The **Right to Access** policy outlines how patients may access, inspect, or obtain a copy of their protected health information.

Key Points

- All patients who would like access to their PHI (both inpatients and outpatients) should submit a completed **Authorization for Access/Release of Information** form, which will be forwarded to the relevant Health Information Management/Medical Records Department.
- Inpatients may request to inspect a copy of their medical records in the presence of their physician or the physician's designee.
- A copy of requested records shall be provided within 30 days after the record is completed.
- Documentation of actions taken should be noted in the electronic record and/or on the Authorization for Access/Release of Information form and a copy placed in the patient's record.

Accounting of Disclosures

The **Accounting of Disclosures** policy provides guidelines regarding the patient's right to request an accounting of disclosures. An accounting of disclosures is a listing of where a patient's PHI has been sent, to whom, and for what purpose. The accounting does not need to include those recipients to whom the patient has authorized information be sent, or those that the HIPAA regulations specifically exclude, such as for treatment, payment, and some operations.

Key Points

- Patients may request an accounting of disclosures by submitting a completed **Request for Accounting of Disclosures** form to the Health Information Management/Medical Records or Billing Departments.
- In general, a patient must receive an accounting within 60 days, or within that same time frame, receive notification that an additional 30-day extension will be necessary.
- Examples of disclosures which must be included in the accounting are disclosures made in response to a subpoena, for public health activities, for abuse and neglect reporting, for health oversight activities or law enforcement purposes, for workers' compensation, for reviews preparatory to research, and to coroners, medical examiners, funeral directors, and for cadaveric organ donation purposes. A complete list can be found in the policy.
- The affected departments must provide the disclosure information as requested to the Medical Records/Health Information Management (HIM) Department.

Amendment to PHI in Medical and Billing Records (Patient's Right to Request)

As its title indicates, the **Patient's Right to Request Amendment to PHI in Medical and Billing Records** policy outlines how patients may request an amendment to the protected health information in their medical and billing records. Guidelines are provided for clinicians who will review the request and decide whether the request for amendment will be accepted as a necessary correction to the record, accepted as an alternative viewpoint, or denied.

Key Points

- To request an amendment, patients must complete the **Form to Request Amendment to Protected Health Information Retained in Designated Record Sets** and must provide verification of identity.
- One exception is that routine requests for billing amendments may be received via telephone, given that the caller verifies certain patient identifiers. For non-routine requests, patients will be sent the **Form to Request Amendment to Protected Health Information Retained in Designated Record Sets.**
- A patient must receive a response within 60 days, or, within that same time frame, receive notification that an additional 30-day extension will be necessary.
- In the case of medical records, the patient's request for amendment as well as an explanatory cover letter will be sent to the clinician who authored the portion of the patient record in question for review and response (e.g., accept as necessary, accept as alternative viewpoint, or deny) within the allotted time.
- The original copy of the request form, with the clinician/author's decision noted at the bottom, will be placed or scanned into the patient's record, and a copy sent to the patient.
- As appropriate, reference to accepted amendments and/or actions taken will be noted at the appropriate site in the record by HIM or Billing staff.

De-identification

For uses and disclosures of PHI that are not authorized or permitted by the HIPAA regulations or YNHHS policies and procedures (e.g., as defined in the **Release of Protected Health Information** policy), de-identification of the PHI will be required.

Key Points

- De-identification of PHI requires the removal of a complete list of specific identifiers to render the health information no longer identifiable (e.g., names, dates, addresses, account numbers, etc.).
- De-identification of PHI may be performed by a statistician or other person with appropriate knowledge and experience with statistical and scientific principles and methods for rendering the information not individually identifiable.
- If the individual who will perform the de-identification is not a member of the workforce, a business associate agreement will be required.

Designated Record Sets of Medical and Billing Records

The **Designated Record Set** policy identifies those components of the medical and billing records to which patients or their personal representatives may request access or amendment. Billing records must be maintained for at least seven years. Medical records must be maintained for the minimum period required by state law (e.g., 25 years for most hospital departments, and 7 years for physician offices).

Facsimile (Fax) Transmittal

Protected health information (PHI) and confidential information must be safeguarded when faxed.

Key Points

- Confirm that the receiver's fax number is accurate.
- When possible, pre-program regularly used fax numbers to avoid mis-dialing.
- Use the facility's standard fax cover sheet that includes a disclaimer for all faxes that are sent.
- Report faxes with PHI that are sent to the wrong location to the Office of Privacy and Compliance at 688-8416.
- Make sure fax machines as well as faxes sent or received are located in controlled/properly staffed or non-viewable areas.

Uses and Disclosures of PHI for Fundraising

The **Fundraising** policy provides guidelines for using and disclosing protected health information (PHI) for fundraising purposes.

Key Points

- Only limited PHI may be used for fundraising without a patient's authorization. Permitted PHI include dates of service information and patient demographic information.
- Fundraising materials must include opt-out language.
- YNHHS must make all reasonable efforts to honor patient opt-out requests.

Uses and Disclosures of PHI for Marketing

The **Marketing** policy document outlines both the marketing uses and disclosures of PHI for which an authorization needs to be obtained. It also outlines the exceptions.

Key Points

- Permitted communications that are **not** considered marketing under the HIPAA regulations include communications made by the YNHHS facilities regarding their own health-related products or services; communications regarding treatment of a patient; and communications to a patient regarding case management, care coordination, or recommendation of alternative treatments, therapies, health care providers, or settings of care.
- A patient's authorization must be obtained for any use or disclosure of PHI for marketing purposes unless it occurs during a face-to-face communication with the patient or only involves a promotional gift of nominal value.

Minimum Necessary

The **Minimum Necessary** policy states that YNHHS facilities will limit the protected health information (PHI) used, disclosed, or requested to the minimum amount necessary to carry out workforce members' job duties, or to fulfill the purpose of the disclosures or requests.

Key Points

- Healthcare professionals may access the PHI of any patient for whom they are assigned care; other staff will be granted access based on their roles and job functions. Information access controls will be implemented as necessary.

- Inappropriate or unauthorized access will result in disciplinary action up to and including termination of employment or removal from the Medical Staff.
- Both when disclosing PHI to other entities or requesting PHI from other entities, only the minimum necessary amount of PHI should be disclosed or requested. **Appendix B** of the policy provides general guidance regarding what is minimally necessary disclosures for routine or recurring requests.
- Criteria for determining what is minimally necessary for non-routine disclosures are also outlined in the policy.

Notice of Privacy Practices

The **Notice of Privacy Practices** outlines for patients or their personal representatives how their protected health information (PHI) may be used and disclosed. It also outlines patients' rights in regard to their protected health information (e.g., concerning access, amendments, accounting of disclosures, restrictions, confidential communications, and complaints).

Key Points

- The Notice must be provided to the patient on their first visit, and good faith efforts must be made to obtain the patients' written acknowledgement of receipt of the Notice.
- Either a copy of the patient's signed acknowledgement or documentation of good faith effort to obtain the acknowledgement must be maintained in the medical record and/or noted electronically.
- The most current Notice must be prominently posted within the System facilities and on facility Websites.

Personal Representatives and Communication with Patient Families

The **Personal Representatives and Communication with Patient Families** policy defines who is a legal personal representative acting on behalf of the patient as well as discusses communication with designated family spokespersons who are not legal personal representatives. Both categories of individuals may receive protected health information (PHI) as needed to act on the patient's behalf. Good-faith efforts should be made to identify individuals requesting PHI before sharing the information.

Key Points

- A personal representative is a person legally appointed to act on the patient's behalf, such as a conservator, guardian, or durable power of attorney.
- Before sharing PHI with an unknown individual claiming to be a family member, confirm that the patient has not opted out of the facility directory or placed restrictions on the release of his/her information. The individual should be asked to verify a few patient identifiers such as the patient's address, date-of-birth, social security number, or hospital account number. Restrict the information released to the minimum necessary.
- Regarding communication with patient families, patients may be requested to designate a family spokesperson with whom YNHHS staff can regularly communicate PHI about the patients.

Privacy Complaints

A suspected privacy violation or privacy complaint may be reported by any individual regarding inappropriate use, access, or disclosure of protected health information (PHI).

Key Points

- Patient privacy complaints should be directed to the Patient Relations Department, who will log the information and inform the Office of Privacy and Compliance.
- Privacy complaints occurring at non-hospital YNHHS facilities should be reported to the facility administrator immediately.
- Complaints will be investigated and disciplinary measures will be taken when wrongdoing has been determined.

Release of Protected Health Information

The **Release of Protected Health Information** policy provides guidelines on appropriately releasing/disclosing patients' protected health information (PHI), including for research purposes, to insurance companies, to government agencies, to physicians and other health care facilities, pursuant to subpoenas, to the media, for the facility directory, and to clergy.

Key Points

- A patient's written authorization, valid subpoena, court order, or other authorized documentation will generally be required for most releases and disclosures made for non-TPO (treatment, payment, and health care operations) purposes. Exceptions are outlined in the policy. For example, only certain limited PHI may be disclosed to law enforcement for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person.
- Unless necessary to perform job duties, workforce members must not use or disclose patients' medical or billing PHI either internally within the facility, or externally outside of the facility.

- Inappropriate use or disclosure will be subject to disciplinary action up to and including termination of employment or removal from the Medical Staff.

Research Authorizations

The **Research Authorizations** policy identifies the necessary elements for a valid patient authorization for the use and disclosure of protected health information (PHI) for research purposes.

Key Points

- All required elements listed in the policy must be included in the research authorization in order for the authorization to be valid.
- In most cases, the authorization will be a stand-alone document appended to the back of the informed consent.
- The specifics of privacy guarantees and security procedures relating to PHI should be delineated in the research protocols.

Request for Access to Protected Health Information for a Research Purpose Form (Researcher Representation form)

The **Request for Access to Protected Health Information for a Research Purpose** form provides a means of assurance that a request presented by a researcher to access YNHHS facility records for research purposes, including reviews preparatory to research and research on decedents, is valid.

Key Points

- Researchers must present a copy of the completed **Request for Access to PHI for a Research Purpose** form, with appropriate signatures, in order to obtain PHI for any research purpose.
- If the researcher is not a full-time Yale University faculty member or YNHHS attending physician, s/he will need to obtain the signature of a YNHHS Clinical Department Chair or Section Chief, YSM/YSN full-time Faculty Member, YNHHS Attending Physician, or YNHHS Nurse Manager.

Right to Request Restrictions or Confidential Communications on the Use and/or Disclosure of PHI

The **Right to Restrictions or Confidential Communications** policy states that YNHHS facilities will consider reasonable requests from patients for (1) confidential communications via alternative means or alternative locations and (2) restrictions on the use and/or disclosure of patients' PHI.

Key Points

- A patient will be asked to submit the request in writing on the **Form to Request Restrictions/Confidential Communications on the Use and Disclosure of Protected Health Information**. The form will be filed or flagged in the medical or financial record as applicable.
- The main criterion that will be used in reviewing patients' requests for restrictions on their PHI is whether their health or life is in danger.
- Prior to disclosing PHI, staff must be aware if there is a restriction or confidential communication in place regarding patients' PHI, in order to prevent unnecessary breaches.

Tracking YNHHS Contracts and Agreements

The **Tracking YNHHS Contracts and Agreements** policy provides guidelines on the appropriate tracking of all YNHHS contracts and agreements.

Key Points

- All contracts and agreements with business associates must include the YNHHS-approved business associate language. A Business Associate is a person or entity, who on behalf of YNHHS or a YNHHS facility, performs or assists in the performance of a function or activity involving the use or disclosure of protected health information (PHI), including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing.

HIPAA Security Education at YNHHS

Key Learning Points

I. Computing devices other than those provided by the hospital may not be connected to the hospital network without prior clearance, in writing, from MIS. This is to protect the hospital environment from possible viruses and other malicious code.

II. Any electronic protected health information (PHI) stored on a portable computing device or removable storage device must be protected with encryption, to ensure against disclosure in the event of loss or theft.

III. User ID's and their corresponding passwords must be kept confidential and cannot be shared with anyone else. Using someone else's ID and password may result in termination or loss of privileges.

IV. If you observe any type of security incident (use of another's ID, unauthorized access of PHI, malicious use of computing resources, etc) or experience the loss or theft of PHI or devices containing PHI, you must report the incident. Incidents should be reported to the MIS Help Desk (8-HELP) or to the hospital's Compliance Officer or Security Officer immediately.

V. The health system has policies in place which address both privacy and security. If you have any questions regarding our HIPAA policies please contact our System Privacy Officer & HIPAA Project Director at 688-8605.

Executive Summaries of YNHHS HIPAA Policies

SECURITY SUMMARIES:

Appropriate Use of Electronic Resources

YNHHS workforce members are required to use YNHHS' electronic resources in a professional, lawful and ethical manner, and to prevent the unauthorized use or disclosure of protected health information or any other confidential information. Use of electronic resources will be subject to managerial review and based on job requirements.

Key Points

1. YNHHS can monitor the use of the resources with available technologies, with or without the knowledge of the member of the workforce, with the exception of phone conversations.
2. Electronic Resources include, but are not limited to: Personal Computers, E-mail, Voicemail, Telephones, Fax Machines, Pagers, Laptops, Cell Phones, Copiers, and PDAs.
3. Some examples of inappropriate behavior that should be reported to the Information Security Officer and/or the Office of Privacy and Compliance and that warrant disciplinary actions up to and including termination are:

- Using someone else's password or login ID.
- Unauthorized viewing or use of PHI or confidential information.
- Unauthorized access to system, data or hard copy information.
- Unauthorized transmission of protected health information (PHI) or confidential data over the Internet (for example, unencrypted transmission of a patient's medications)
- Breach of external networks (for example, firewalls, web servers and VPNs)
- Actions that cause unexpected alert by intrusion detection systems.
- Unauthorized entry into the Data Center.

Audit Controls

YNHHS facilities reserve the right to record and review audit trails of computer applications containing PHI and the operating systems they run on to ensure that data is only accessed and/or disclosed for treatment, payment and operations. Incidents of inappropriate access will be addressed by the Office of Privacy and Compliance and/or Information Security Officer.

Computer Virus Protection

YNHHS facilities will ensure that current computer virus protection software is used on all electronic computing devices to protect PHI.

Key Points

1. Remote users or users of standalone devices must take reasonable steps to ensure adequate computer virus protection.
2. No member of the YNHHS workforce may intentionally remove or disable virus protection software installed on YNHHS-provided electronic computing devices.
3. If the current virus protection software reports the unsuccessful handling of a virus, or if users suspect the existence of a computer virus, they should immediately contact the Information Services' Help Desk.

Disposal and Control of Documents and Media Containing PHI

YNHHS workforce members must ensure the protection of PHI by controlling the use, storage, and disposal of documents and other media containing PHI.

Key Points

1. Types of media with PHI include, but are not limited to: Paper, Disks (including hard disks, floppy disks and compact disks), Microfiche, Overhead Transparencies, Photographs, Slides, Patient Identification Bands, I.V. Bags, Embosser Plates, Prescription Bottles.
2. When individuals have completed using PHI, media that contains PHI must be stored in a secure location, returned to the authorized owner, or the PHI or the media it is stored upon must be disposed of appropriately. Each type of media/document may require a specific disposal method for example, shredding confidential information.

Information Security Incidents

YNHHS workforce members are required to report all information security incidents to the Information Security Officer or the MIS Help Desk (8-4357). All reported incidents will be investigated and the results reported to YNHHS management.

Key Points- Incident Examples

1. Using someone else's ID or password.
2. Unauthorized transmission of protected health information (PHI) or confidential data over the Internet (for example, unencrypted transmission of a patient's medications)
3. Introduction of a virus or worm into the computing system or network.
4. Unauthorized use of computing equipment by workforce or non-workforce members.

Portable Electronic Devices

All members of the YNHHS workforce using portable electronic devices [e.g. laptops, mobile carts or PDAs], regardless of ownership, that store protected health information (PHI) must follow strict security standards since PHI can be inappropriately disclosed if the devices are stolen or accidentally lost.

Key Points

1. All portable electronic devices need to be **password protected** or use some other form of **user authentication**, if they are used to store or transmit PHI.
2. Portable electronic devices need to be physically stored in a secure location when not in use.
3. If the information on a portable electronic device does not exist elsewhere, it needs to be backed up periodically to a secured location.
4. If the device is lost or stolen, it needs to be reported immediately to one's manager.

Safeguarding PHI and Confidential Information while Working Offsite

YNHHS policies and procedures regarding confidentiality are to be followed at all times when working offsite with PHI or other confidential information.

User Authentication to Computer Systems

YNHHS workforce members are provided with access to various computing systems which are needed in the performance of their jobs. Each user is authenticated by the use of an ID and password or other security mechanism.

Key Points

1. You may not share your password with anyone, for any reason.
2. Passwords are not to be stored on your computer or anywhere where they may be found by others.
3. Passwords should be at least 5 alphabetic and numeric characters in length.
4. You must report any unauthorized use of your password immediately.