Yale New Haven Health System (YNHHS)
Privacy & Security Requirements for Medical & Affiliated Medical Staff

Release and Disclosure of Protected Health Information - A patient's written authorization, valid subpoena, court order, or other authorized documentation will generally be required for any releases, access and/or disclosures of Protected Health Information (PHI) or ePHI (electronic PHI) for non-TPO (treatment, payment, and health care operations) purposes. Additional information and exceptions are outlined in relevant YNHHS policies.

- Visitors should politely be asked to leave before discussing a patient's condition and/or treatment. The choice is then left up to the patient to voice whether the visitors should stay.
- Before sharing PHI with an unknown individual claiming to be a family member, confirm that the patient has not placed restrictions on the release of his/her information. Good faith efforts should be made to verify the identity of the requestor. Information released regarding the patient is required to be restricted to the "minimum necessary".

"Minimum Necessary" - The YNHHS policy is that the disclosure, access and use of protected health information (PHI) will be kept to the minimum amount necessary to carry out duties.

- 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.
- Only the minimum necessary amount of PHI should be disclosed or requested when disclosing PHI to other entities or requesting PHI from other entities.

E-Mail and Electronic Messaging - Given that the electronic information can be easily intercepted if not appropriately secured, transmission and/or storage of PHI AND OTHER SENSITIVE INFORMATION is NOT PERMITTED using email or messaging solutions that do not meet the Security Rule requirements.

- Email between YNHHS and its affiliated organizations and Yale University is permitted when using an email application approved by YNHHS/University ITS for use with ePHI and other confidential data, such as YU Exchange/Outlook email.
- Do not put PHI in the "Subject" field of an email message.
- YNHHS employees should only use ITS secured devices to exchange email via smartphones, iPads or other portable electronic devices. For the University, email containing PHI may only be sent with a device that has been secured in compliance with Yale University's security policies and procedures.
- Encrypted YNHHS Exchange/Outlook email containing PHI and other sensitive information *may* be sent to approved external email addresses only with the approval of the sender's Vice President for YNHHS employees, and it must be manually encrypted by typing the word '**encrypt**' in the subject field (there must be a space between the word encrypt and any other characters in the subject). See more detailed instructions in the YNHHS Electronic Mail and Electronic Messaging Policy. For medical staff not required to use YNHHS or Yale University secured devices and applications, electronic communication of PHI should be strictly limited to the minimum necessary.
- No electronic messaging (i.e., texting) of ePHI and other confidential data is permitted using devices and applications unless approved by YNHHS/Yale University and in compliance with the Security Rule.

Connecting to the YNHHS Network – All devices used to connect to the YNHHS network must comply with security controls as defined in the Security Rule.

- If you are a YNHHS employee, computing devices other than those provided by a YNHHS hospital may not be connected to the hospital network without prior clearance, in writing, from Information Technology Services (ITS) Office of Information Security. Only devices that meet minimum security requirements including, but not limited to, encryption, current anti-virus, and endpoint protection will be considered for approval. This is to protect the hospital environment from data loss, possible viruses, and other malicious code.
- Yale University devices used to connect to the YNHHS network must be secured as per University HIPAA policy.

YNHHS Notice of Privacy Practices - At first entry to any YNHHS facility, patients will be given the Notice so that they understand how we will use their PHI for the purposes of treatment, payment, and certain health care operations to improve our clinical effectiveness or as otherwise permitted by HIPAA. The Notice will also explain their rights under HIPAA to access their medical record, request an amendment to their record, request an accounting of disclosures, request a restriction or confidential communication, file a complaint, or opt out of our facility directory. Patients will be asked to sign the Notice as an acknowledgement of their understanding.

Presenting at Conferences - All personal identifying information about any patient must be removed from all and handouts used 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.

Portable Electronic Devices – All portable computing devices or removable storage devices used to connect to the YNHHS network or store YNHHS ePHI or other confidential data must comply with security controls as defined in the Privacy and Security Rules.

- If you are a YNHHS employee, ePHI that is stored on a portable computing device or removable storage device must be protected with YNHHS ITS-approved encryption, to ensure against disclosure in the event of loss or theft. If you need assistance with encryption please contact the ITS Service Desk (688-HELP) or if a device is lost or stolen, it must be reported immediately to the ITS Service Desk (688-HELP).
- Yale University faculty, staff, trainees, students and members of Yale University'sHIPAA Covered Components must secure any portable computing or removable storage devices as per University policy.

Facsimile (fax) Transmittal - Care must be taken when transmitting PHI via fax. The sender is responsible for verifying the accuracy of the fax number for the intended recipient. Do not rely on fax numbers listed in directories or provided by persons other than the recipient. All faxes must include a cover sheet that includes a confidentiality disclaimer as described in the YNHHS facsimile transmittal policy. The cover sheet for example would include the date/time of transmittal; sender and receiver's name, location, contact information; number of pages; list of transmitted documents; and requested notice to the sender in the event of a transmission error to an unintended recipient and a confidentiality statement.

Appropriate Use of Electronic Resources - Medical & Affiliated Medical Staff members of YNHHS hospitals are required to use 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. All Medical & Affiliated Medical Staff members are subject to the same requirements when using YNHHS electronic resources.

Monitoring - YNHHS reserves the right and the authority to monitor the use of YNHHS electronic resources with the exception of phone conversations. Users should have no expectation of privacy in connection with the use of YNHHS resources, systems, equipment, or with the transmission, use or storage of information, including but not limited to stored e-mails or voicemail messages. YNHHS systems, resources and equipment include, but are not limited to, the following: computing devices, E-mail, Voicemail, Telephones, Fax Machines, Pagers, Laptops, Cell Phones, Copiers, PDAs.

User Authentication to Computer Systems - User IDs and their corresponding passwords must be kept confidential and cannot be shared with anyone else. Passwords are not to be stored on your computer or anywhere where they may be found by others. Using someone else's ID and password may result in termination or loss of Medical Staff privileges and disciplinary action up to and including termination if you are an employee. ***Each time you finish using an electronic resource containing PHI or other sensitive data, even for a short period of time - please be certain to log off of the system you are using to minimize the likelihood that an unauthorized user could access records under your name.***

Safeguarding YNHHS PHI and Confidential Information while Working Offsite - YNHHS policies and procedures regarding confidentiality of transporting, storing or accessing PHI are to be followed at all times when working offsite with PHI or other confidential information. Remote users must take reasonable steps to ensure adequate computer virus protection.

Disposal and Control of Documents and Media Containing PHI - 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.

Storage of PHI and other Sensitive Information – Storage of PHI and other sensitive data must be secured by implementing security controls as set forth in the Security Rule.

- ePHI and other sensitive information obtained in connection with your employment and/or Medical or Affiliated Medical Staff membership may not be saved to the local hard drive on personal computing devices including portable devices. All such data must be saved to the network file server that has been assigned to you by YNHHS ITS.
- Yale University faculty, staff, trainees, students and members of Yale University's HIPAA Covered Components must secure storage of PHI and other sensitive data as per University policy.

Privacy Investigations and Information Security Audit Controls - A suspected privacy violation or privacy complaint regarding inappropriate use, access, or disclosure of protected health information (PHI) will be investigated and appropriate measures taken if any wrong doing is determined. YNHHS facilities reserve the right to record and review audit trails of applications containing PHI, the operating systems and network they run on.

Inappropriate use or disclosure may result in disciplinary action up to and including employment termination and/or removal from the relevant YNHHS hospital Medical Staff or Affiliate Medical Staff.

Privacy Officer - HIPAA related questions and complaints regarding the Hospital or YNHHS facilities should be referred to the Office of Privacy and Corporate Compliance at 688-8416 or privacy@ynhh.org.

HIPAA Security Officer – Please contact the ITS Service Desk (688-HELP) with any HIPAA related security questions or concerns and ask to speak to the Chief Information Security Officer (CISO and HIPAA Security Officer) or one of the Managers from the Office of information Security (OIS).

For more information on privacy and security policies, please see the YNHHS intranet, under the Polices tab, or visit https://ynhh.ellucid.com/manuals/binder/604.

For more information on Yale University privacy and security policies, please visit http://hipaa.yale.edu/.

For more information on privacy and security laws please visit http://www.hhs.gov/ocr/privacy/hipaa/understanding/ Please contact the YNHHS Office of Privacy & Corporate Compliance 203-688-8416 or YNHHS Office of Information Security 203-688-HELP with additional questions.

Reporting Incidents and Violations

You are obligated to report any known or suspected violations of the Privacy or Security Policies as well as the loss or theft of PHI or devices containing PHI. Reports can be made to the Office of Privacy and Corporate Compliance or to the Compliance Hotline.

Compliance Hotline: 888-688-7744 Available 24 hours a day/7 days a week
Office of Privacy and Corporate Compliance: 203-688-8416 or privacy@ynhh.org
Information Security: Contact the ITS Service Desk (203.688-HELP) and ask to speak with the Office of information Security (OIS).

Members of the Medical Staff are responsible for the activity of any of their employees who have been granted access to YNHHS applications & systems (including Epic) and ensuring compliance with the requirements stated in this document.

Privacy and Security Agreement

By signing this document, I certify that I have read and understand the Privacy and Security policies in effect at the Yale New Haven Health System and its affiliated entities' (YNHHS) facilities.

I agree to:

1. Abide by all hospital and YNHHS policies, procedures and guidelines relating to the use, access and protection of Protected Health Information (PHI), as amended from time to time.
2. Hold in strictest confidence all PHI and not to disclose or discuss PHI with any other third party, including friends or family, except as permitted by YNHHS policies, procedures and guidelines and in accordance with state and federal laws *(for additional resources on privacy and security laws please review the attached reference document)*.
3. Use PHI only in connection with the provision of medical care to patients and not remove YNHHS hospital PHI and/or Proprietary Information from any YNHHS premises except as permitted by YNHHS policies, procedures and guidelines and in accordance with state and federal laws.
4. Not discuss PHI where unauthorized persons can overhear the conversation.
5. Report incidents and violations to policies (such as privacy and security concerns witnessed) to the YNHHS Office of Privacy and Corporate Compliance.
6. Ensure that I and any individuals employed by me will abide by Privacy and Security rules and YNHHS policies/procedures.

I understand that:

1. Access to and use of PHI is subject to regular auditing and monitoring.
2. The restrictions described in this Agreement are in force at all times and in all locations.
3. If I fail to comply with the terms of the Agreement, I may be subject to disciplinary action, up to and including termination of my employment (if applicable) and from the Medical Staff.
4. A patient's right to confidentiality of PHI is protected by state and federal laws and YNHHS policies, procedures and guidelines.
5. If I violate this Agreement, I may, as an individual, be subject to civil or criminal legal action for which I will not be provided defense counsel or insurance coverage by YNHHS.
6. My obligations under this Agreement shall survive termination of my employment (if applicable) and Medical Staff membership.
7. Audits are performed and users are responsible for securing and not sharing user names and passwords.

Applicant Full Name (please print):_____

_____ _____

Signature Date