

2019 HCCA Philadelphia Regional Conference

Privacy and Info Security: Beyond the Rules to Program Effectiveness

Terrie B. Estes, FACHE, CHC, CHPC
VP, Corporate Compliance & CCO
Office of Privacy and Corporate Compliance
May 30, 2019

Privacy and Security: Beyond the Rules to Program Effectiveness

- About Yale New Haven Health*
- The Rules We Know*
- Best practice in communication (Don't tell me what not to do; tell me what to do)*
- Effective monitoring and response*

Note: 3:10 – 4:10 pm on Friday, May 31st at the DoubleTree by Hilton Philadelphia – Center City.

VISION, MISSION AND VALUES



YaleNewHaven**Health**

About Yale New Haven Health

5 Hospitals and a physician foundation

- **Employees:** 25,199
- **Medical Staff:** 8,287
- **Total Licensed Beds:** 2,563
- **Inpatient Discharges:** 129,100
- **Outpatient Encounters:** 2 million
- **Physician Practices:** 130
- **300+ Ambulatory Sites**
- **Total Revenue:** \$4.3B
- **Specialty Networks**
 - Heart and Vascular Center
 - Cancer Hospital Network
 - Children's Pediatric Network
 - TeleStroke Network
- **Visiting Nurse Association**
- **Rehabilitation Center (SNF)**
- **Psychiatric Hospital**

Getting to know you...

- 77% of Healthcare compliance officers now have responsibility for Health Insurance Portability and Accountability Act (HIPAA) privacy, with about 40% for risk management.
- Compliance offices remain lean, # of full-time dedicated or departmental/decentralized?
- Only 1 out of 5 organizations reported using tools to automate key compliance processes, such as document management, measuring compliance program effectiveness, audit management software, and critical incident management. Your tools?
- Only 29% of recipients have their compliance program independently measured for effectiveness. Frequency?
- 18% of respondents indicated high confidence in their preparation for an Office of Civil Rights (OCR) audit, declining slightly from the 20% reported last year and 30% in 2017.
- Nearly two-thirds of the respondents reported having made disclosure to OCR of breaches of privacy under HIPAA.
- 64% of respondents state they have not used surveys to measure compliance program effectiveness in the past year. Have you?

Training

“When your Values are clear to you,
making decisions becomes easier.”

- Roy E. Disney

Our Values and Privacy & Information Security

PATIENT-CENTERED

Putting patients and families first



Patient health information belongs to the patient. Accessing this information for treatment, payment and operations (TPO) allows us to provide high-value, patient-centered care.

RESPECT

Valuing all people



We protect others' privacy and dignity when we protect their health information.

COMPASSION

Being empathetic



We communicate with courtesy and respect with patients and one another.

INTEGRITY

Doing the right thing



We access and disclose PHI for TPO, obtaining authorization when needed.

ACCOUNTABILITY

Being responsible and taking action



We protect patients' privacy and information. We speak up so review and investigation can be conducted. We acknowledge when we're wrong, apologize and take appropriate, corrective action.



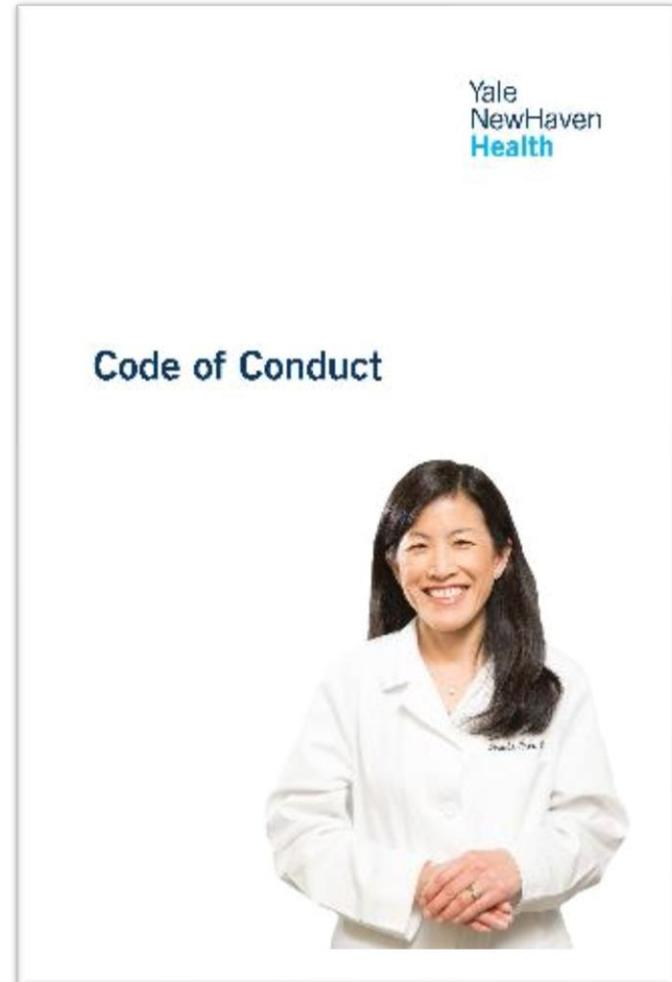
Center for Plain Language

————— Make it clear. —————

- **Step 1: Identify and describe the target audience**
- **Step 2: Structure the content**
 - Flows logically, short sections that reflect natural stopping points
- **Step 3: Write the content in plain language**
 - Keep it short and to the point
 - Present important information first
 - Include the details that help the reader complete the task
 - Leave out details that may distract readers
 - Use a conversational, rather than legal or bureaucratic tone
 - Pick the right words, Use strong verbs in the active voice
 - Use words the audience knows, selective acronyms
 - Make titles or list elements parallel (for example, start each with a verb)
- **Step 4: Use information design to help readers see and understand**
 - Use headers, sub-headers, and fonts to organize the information
 - Use whitespace to organize the information
 - Use images to make content easier to understand
- **Step 5: Work with the target user groups to test the design and content**
 - Were audience needs met?

YNHH Code of Conduct

- Discusses responsibility for doing the right thing, highlights standards of behavior, the role of management and the non-retaliation policy.
- Establishes a zero tolerance for fraud and abuse.
- Promotes and provides guidance for all employees to take personal accountability by asking questions, seeking guidance and raising concerns.
- All employees are required to attest adhere.



Gifts and Gratuities

- YNHHS Policy does not allow Employees to accept cash or cash equivalents as gifts from patients, physicians or vendors.
- If a family of a patient brings perishable food items to the unit on the day that the patient is being discharged from the hospital. Such a token of appreciation is acceptable, provided it is shared with the unit.
- When patients, relatives, or friends express a desire to make a gift to YNHHS, they should be referred to the Hospital's Development Office or Foundation Office



Policies & Procedures

The screenshot shows the Yale New Haven Health System intranet navigation menu. The top navigation bar is dark blue and contains links for Home, Corp. Compliance/Privacy (highlighted with a green box), Training, Emergency Preparedness (CHS), Epic, Jobs, MD Referral, Directory/Paging, and Password Reset (EPIC/Outlook/Network). Below this is a secondary navigation bar with links for Bridgeport, Greenwich, Grimes Center, L+M, Health Services Corp., NEMG, VNASC, Westerly, Yale New Haven, and YNHHS. A search box is located to the right of the YNHHS link. Below the secondary navigation bar is a light blue bar with the text 'Yale New Haven Health System' and a list of application categories: Applications (highlighted with a green box), Dashboard, Departments, Documents, Policies (highlighted with a green box), Projects, References, and Report a Safety Event. Below this is a breadcrumb trail: Home > YNHHS > Yale New Haven Health System > Applications. A list of application categories is shown below the breadcrumb trail, including Benefits Enrollment, BusinessObjects Reporting, and CRISA Web Entry.

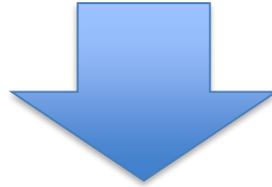
All Policies can be accessed through the intranet.

Click on 'Policies'

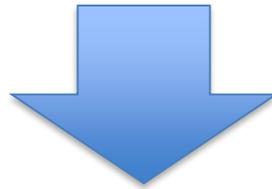
OR

Click on 'Corp. Compliance & Privacy'

To ask questions, express concerns, or report suspected violations related to:



*Bribes and Kickbacks, Theft and Fraud; Gifts and Entertainment;
Medicare/Medicaid Fraud and Abuse; Conflicts of interest;
Confidentiality of Company information; Privacy of Employee and
Patient Records; Potential Criminal Violations or Other Violations of
Company Policies*



Report through your Chain of Command

Contact Corporate Compliance at 203.688.8416 or compliance@ynhh.org

YNHHS Compliance Hotline - 1-888-688-7744

To ask **questions**, express **concerns**, or to **report** suspected violations

Report through your
Chain of Command

1. Direct supervisor
2. Higher level of management.
3. Human Resources
4. Compliance office:
203-688-8416 or
compliance@ynhh.org
5. To make an anonymous report,
call the Compliance Hotline at
[1-888-688-7744](tel:1-888-688-7744)

Potential Violations

- Bribes and Kickbacks
- Theft and Fraud
- Gifts and Entertainment
- Conflicts of Interest
- Inappropriate Disclosure
- Compromise of Patient Information
- Criminal acts
- Violations of Policies

What is PHI?

- *Protected Health information* means any information, whether oral or recorded in any form or medium, that–
 - (A) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
 - The relationship with health information is fundamental but identifiers such as personal names, residential addresses, or phone numbers, are PHI when obtained from clinical systems or care providers. For example, a patient list on YNHH letterhead is PHI.
 - (B) relates to the past, present, or future physical or mental health or condition of any individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

Treatment, Payment, Operations (TPO)

You can access records for purposes of:



Threats to Privacy of PHI

– Paper Disclosures



– Verbal Disclosures



– **Inappropriate Access**

Did you see this?

WARNING:

Access to Clinical Systems is RESTRICTED. Users may only access the patients with whom they have direct care responsibilities. Access to patient data is subject to audit. Unauthorized access or disclosure of sign-on codes will lead to disciplinary action up to and including termination of employment or your medical staff appointment.

The Health Insurance Portability and Accountability Act (HIPAA)

HIPAA is a federal law that gives patients important rights with regard to their protected health information.

THREE KEY RULES:

PRIVACY RULE

- Privacy Rule went into effect **April 14, 2003**.
- Privacy refers to protection of an individual's health care data.
- Defines how patient information used and disclosed.
- Gives patients privacy rights and more control over their own health information.
- Outlines ways to safeguard Protected Health Information (PHI).

SECURITY RULE

Security means controlling:

- **Confidentiality** of electronic protected health information (ePHI).
- **Integrity** of electronic protected health information (ePHI)
- **Availability** of electronic protected health information (ePHI)

BREACH NOTIFICATION RULE

Definition of Breach (45 C.F.R. 164.402)

Impermissible use or disclosure of (unsecured) PHI is assumed to be a breach unless the covered entity or business associate, demonstrates a low probability that the PHI has been compromised based on a risk assessment.

Patient Authorization to access for non-business reasons....

- You accompany your spouse to all of their pre-natal appointments, you are not part of their treatment team BUT your spouse gives you permission to access all of their encounters in epic
 - *Are you allowed to view their medical record?*
- Your mom calls, her doctor is not returning her calls to provide her test results, you are not part of the treatment team BUT mom gives you permission to access the results for her
 - *Are you allowed to view the results and disclose them to your mom (the patient)?*

Access to your information

- Are you allowed to access your child's information via Epic?
 - MyChart?
- Are you allowed to access your parent's information via Epic?
 - MyChart?
- Are you allowed to access your information via Epic?
 - MyChart?

- What is Proxy access in MyChart?
 - How do you obtain proxy access?

Threats to Privacy of PHI

– Paper **Disclosures**



– Verbal **Disclosures**



– Inappropriate Access

Minimum Necessary

- When disclosing PHI for reasons other than treatment, always disclose the “minimum necessary”,
 - The least that is required for the purpose of disclosure.
 - Always err on the side of non-disclosure, but use common sense when patient safety is at stake.
 - Disclose limited information when leaving messages for a patient when they are not available to personally take the call or information

Threats to Privacy of PHI

– Paper **Disclosures**



– Verbal **Disclosures**



– Social **Disclosures**

– Inappropriate Access

STAYING HIPAA COMPLIANT

when using social media

What can healthcare providers do to help ensure HIPAA privacy and security rules are adhered to when posting online?

Here are five tips to avoid disclosing PHI when using social media.



NEVER POST ABOUT PATIENTS

It's extremely difficult to anonymize patients - even the subtlest identifier could land you and your practice in a lot of trouble.



ONLY USE SECURE MESSAGING

Only discuss or exchange patient information using HIPAA-secure messaging platforms.



EDUCATE YOURSELF AND OTHERS

Staff should always be trained and kept up to date with HIPAA compliance best practices and company social media policies.



DON'T MIX WORK AND PERSONAL LIFE

Healthcare professionals should keep their personal and professional lives separate. Interacting with a patient online could result in PHI inadvertently being exchanged in the public domain.



WHEN IN DOUBT, DON'T POST

People can make mistakes in the heat of the moment. Always take a minute, read the post back to yourself, and consider the potential consequences before hitting the 'post' button

Social Media

Do Not Post patient pictures or protected health information on Social Media



Safeguarding PHI

- Log Out!
- Use only your own access
- Discretion when Discussing
- Don't leave PHI unattended
- Dispose of PHI properly
- Discuss with Management
- Keep PHI out of public view
- Leaving Privacy Screens in place
- Identity Verification:** Every effort should be made to verify the identity of the person requesting information.

Mobile Devices and Cell Phones:



- Corporate device preferred
- Photos with PHI - allowed ONLY if using Haiku, Canto (with MaaS360) or Mobile Heartbeat
- Storage of photos on device is strictly prohibited!
- Texting of PHI - ONLY allowed using Mobile Heartbeat
- Texting of Patient Care Orders is strictly prohibited!
- **Never** post photos, video or any PHI/PII to social media sites.
- ❖ Corporate program to discard personal computers from home

MOBILE DEVICES – KEY POINTS



MOBILE DEVICES MUST BE:

- Encrypted – includes all personal devices if utilized for work – contact the ITS Service Desk to obtain a YNHH approved, encrypted USB drive.
- Keep your personal mobile device secure, not unattended in plain view.
- If device is lost or stolen please contact the service desk as soon as possible.

INFORMATION SECURITY KEY TAKE AWAYS

- **PASSWORDS** Change it every 60 days
 - **NEVER SHARE WITH ANYONE**
 - Make them 8 alpha numeric characters, special characters, mixed case
 - No pet, children, spouse names and **NEVER** use “password123”
- Only use your own user credentials
- Never save Patient or Sensitive Information (PHI or PII) to your c:/ or hard drive. Always use network drives.
- All personal devices used to access/store PHI must be approved & encrypted – contact ITS Service Desk
- Log off or lock workstation

Email Phishing Attacks – BE AWARE.....

- Emails **appear to be sent from a legitimate organization or known individual.**
- Messages **entice users to click on a link** to a fraudulent website or to respond.
- Messages **may request personal information** such as account usernames, passwords, first/last name, date of birth and credit card numbers.
- Links provided often install **malicious software** on the user's device.



Response to Threats to Privacy of PHI

– Paper Disclosures



– Verbal Disclosures



– Inappropriate Access

Sanctions Policy

- 3 Levels: Disclosure, Repeated Disclosure, Access
- Non-compliance with Privacy, Information Security and ePrivacy policies **may** lead to disciplinary action
- Federal HIPAA Regulations and Sanctions Policy govern all “Workforce Members”
 - ❖ Opportunities:
 - Medical Staff
 - Phishing

Protected Health Information (PHI)

- *Health information* means any information, whether oral or recorded in any form or medium, that—
 - (A) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
 - (B) relates to the past, present, or future physical or mental health or condition of any individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.
- The relationship with health information is fundamental. Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI.

Treatment, Payment, Operations (TPO)

Workforce can access, use or disclose records for purposes of:



Otherwise Patient authorization is required

Minimum Necessary

- When disclosing PHI for reasons other than treatment, always disclose the “minimum necessary”,
 - The least that is required for the purpose of disclosure.
 - Always err on the side of non-disclosure, but use common sense when patient safety is at stake.
 - Disclose limited information when leaving messages for a patient when they are not available to personally take the call or information

Threats to Privacy of PHI

– Paper Disclosures



– Verbal Disclosures



– Inappropriate Access

Access to your information

- Are you allowed to access your child's information via Epic?
 - MyChart?
- Are you allowed to access your parent's information via Epic?
 - MyChart?
- Are you allowed to access your information via Epic?
 - MyChart?

- What is Proxy access in MyChart?
 - How do you obtain proxy access?

E-Mail and Messaging Security



- If you need to **send a file** with ePHI/PII:
 - You should use email encryption
 - Enter “**Encrypt**” and space in the beginning of the subject line of your email
- **Do Not...**
 - setup your email account to **auto-forward** your business email to a non-Yale / New Haven Health System email account (e.g. Veterans Affairs, Gmail, Hotmail, Yahoo, AOL, etc.).
 - forward any individual email with ePHI/PII from secure business addresses to **non-secure accounts** (e.g. Gmail, Hotmail, AOL).
 - use individual names, medical record numbers or account numbers in **subject line** of email messages.
- Use caution when sending **text messages or instant messaging** as a means to communicate with providers and/or patients. These types of communications are not secure. (Exception – Mobile Heartbeat)
- **Texting of Patient Care Orders is strictly prohibited!**

Social Media

Do NOT post patient pictures or protected health information on Social Media



Safeguarding PHI

- Log Out!
- Use only your own access
- Discretion when Discussing
- Don't leave PHI unattended
- Dispose of PHI properly
- Discuss with Management
- Keep PHI out of public view
- Identity Verification:** Every effort should be made to verify the identity of the person requesting information.



Privacy & Infor Sec Committee: Cyber Security



Top 10 Cyber Security Risks

Risk Area	Risk Description	Metrics for monitoring of Mitigation Plan	Status update	Risk Trend
Data Flows	Tracking and approval for transfers of ePHI	<ul style="list-style-type: none"> Data Flow project Number of 'validated' flows. 	<ul style="list-style-type: none"> New process is operational. Still many legacy dataflows. 	
Medical Device Security	Increased media attention, loss of functionality or availability of medical devices.	<ul style="list-style-type: none"> Creation of small virtual team. Create risk assessment Prioritize and remediate risks. 	<ul style="list-style-type: none"> Management responsibility assigned. Project underway 	 Prev 
Cyber Security	Resource constrained, security aware culture to be built.	<ul style="list-style-type: none"> Remediation Project Plan 	<ul style="list-style-type: none"> Decommissioned a number of older legacy systems/applications. 	 Prev 
Email 'Phishing'	Provides access to YNHHS systems to hackers.	<ul style="list-style-type: none"> Proactive Phishing Campaign Metrics. Incident response reports. Security Logging 	<ul style="list-style-type: none"> FY18 campaign completed FY19 campaign planned 	
Virus/ Malware	Infections provide remote access, data exfiltration or render critical systems inoperable.	<ul style="list-style-type: none"> 24x7 Alert Monitoring Metrics GeoFencing Project Milestones 	<ul style="list-style-type: none"> Implemented Monitoring. 	

Top 10 Cyber Security Risks

Risk Area	Risk Description	Metrics for monitoring of Mitigation Plan	Status update	Risk Trend
Staffing	High industry demand for cybersecurity professionals.	<ul style="list-style-type: none"> Employee Engagement Survey Market Analysis Monitoring Open Positions 	<ul style="list-style-type: none"> Departures coupled with excessive market salaries for some skillsets. 	 Prev 
Hacking / IT System Vulnerabilities	Systems are constantly 'tested'	<ul style="list-style-type: none"> System Vulnerability metrics 24x7 Monitoring statistics 	<ul style="list-style-type: none"> Continued reduction, monitoring as operational process. 	
Legacy Systems	Acquired sites with legacy systems	<ul style="list-style-type: none"> Site Assessments. Creation of Remediation plan and progress against milestones. 	<ul style="list-style-type: none"> Remediation continuing. 	
Encryption	Lack of Encryption increases HIPAA fine risks and loss of regulated data.	<ul style="list-style-type: none"> Landesk reporting. Annual Risk Reviews for other equipment. E.g. Servers. 	<ul style="list-style-type: none"> No Change 100% of ITS Owned Laptops Encrypted, 99.25% ITS Owned Desktops. 	
Network Access	Broad network presents data risk.	<ul style="list-style-type: none"> Review 3rd Party and affiliated access Implement additional Internet restrictions. 	<ul style="list-style-type: none"> Network Segmentation progressing 	

Questions?