

Compliance For Train The Trainer

Karen Trujillo, RN, MSN

Director of Regulatory Affairs
Northwell Hospice Care Network



Northwell
HealthSM

Our commitment to compliance

The Code of Ethical Conduct

The Code of Ethical Conduct provides guidance for how we can carry out the mission and vision of Northwell Health. The Code reflects Northwell Health's core values.

Our Code provides guidance for you so that you can respond properly when compliance-related issues arise. It is designed to assist you in the performance of your job within appropriate moral, ethical and legal standards. The Code is not intended to cover every situation. Rather, it can help you to make the right decisions or ask the right questions.

The Code and the associated Northwell Health policies and procedures apply to everyone who has a relationship with our organization, including but not limited to:

- Board members
- Officers
- Employed and non-employed staff
- Vendors
- Volunteers
- Consultants and contractors

We also expect all individuals and organizations working on behalf of Northwell Health to adhere to the ethical standards set out in the Code.

We are committed to having an ethical environment at Northwell Health founded on these principles of conduct:

- Treat patients, members, staff and the public with dignity and respect
- Abide by applicable laws, rules, guidelines and procedures
- Behave honestly and fairly and be truthful and accurate in all communications
- Use good judgment and high ethical standards in all business dealings
- Safeguard confidential patient, member, employee health and other private information
- Protect trade secrets, competitive and other business information
- Maintain accurate and timely records
- Strive for mutual respect and trust in work relationships
- Ensure a safe and healthy work environment
- Avoid conflicts of interest
- Guard against theft and misuse of Northwell Health property and other assets
- When in doubt about a situation, ask before acting



Vital signs

We expect and require everyone affiliated with Northwell Health to perform their job duties and responsibilities in a law-abiding, honest and trustworthy manner.

Everyone at Northwell Health is responsible for maintaining an ethical environment. Your actions in the workplace must demonstrate your commitment to honesty, integrity and accountability every day. Your job performance will be evaluated, in part, based on your compliance with the Code and with Northwell Health's compliance-related policies and procedures.

Certain Northwell Health compliance policies are referenced in this Code. Other compliance policies can be reviewed and downloaded from myIntranet, Northwell Health's intranet site, on the Office of Corporate Compliance web page or obtained from a supervisor in hard copy form.

Please contact the Office of Corporate Compliance whenever you have questions about any compliance-related issue. Northwell Health's Human Resources staff also can provide guidance on workplace issues arising from the Code of Ethical Conduct and/or Northwell Health's policies and procedures.



Vital signs

You have a duty to know, understand and comply with the requirements of all Northwell Health policies, regardless of whether they are referenced in this Code.

Northwell Health's Code of Conduct

“... demonstrates that we are committed to honesty, integrity and ethical behavior in all aspects of our work.”

~ Michael J. Dowling,
President and Chief Executive Officer

Our Values Shape the Code

WE ARE:

Truly *Compassionate*

- Every moment matters

Truly *Innovative*

- We never settle

Truly *Ambitious*

- Our ambitious spark changes lives

Truly *Together*

- We rely on each other

Truly *Ourselves*

- We are all unique

Compliance's Role and Responsibilities

Develop policies, procedures, and programs that detect and prevent fraud, abuse, and inappropriate conduct

Develop and implement compliance awareness training and educational programs

Analyze, communicate and respond to changing needs and changes in laws and regulations

Manage compliance reviews and audit programs

Compliance's Role and Responsibilities

Develop avenues to report suspected fraud and other improprieties without fear of retaliation

Ensure the screening of individuals pre and post employment

Independently investigate and act on matters related to compliance and take corrective action where necessary

Report to the Health System's governing body, and key executive committees on program effectiveness

Compliance's Additional Role and Responsibility



Ensuring Northwell Health is compliant with the Health Insurance Portability and Accountability Act (HIPAA)

What HIPAA is not...



Who must abide by the HIPAA Privacy and Security Rules?

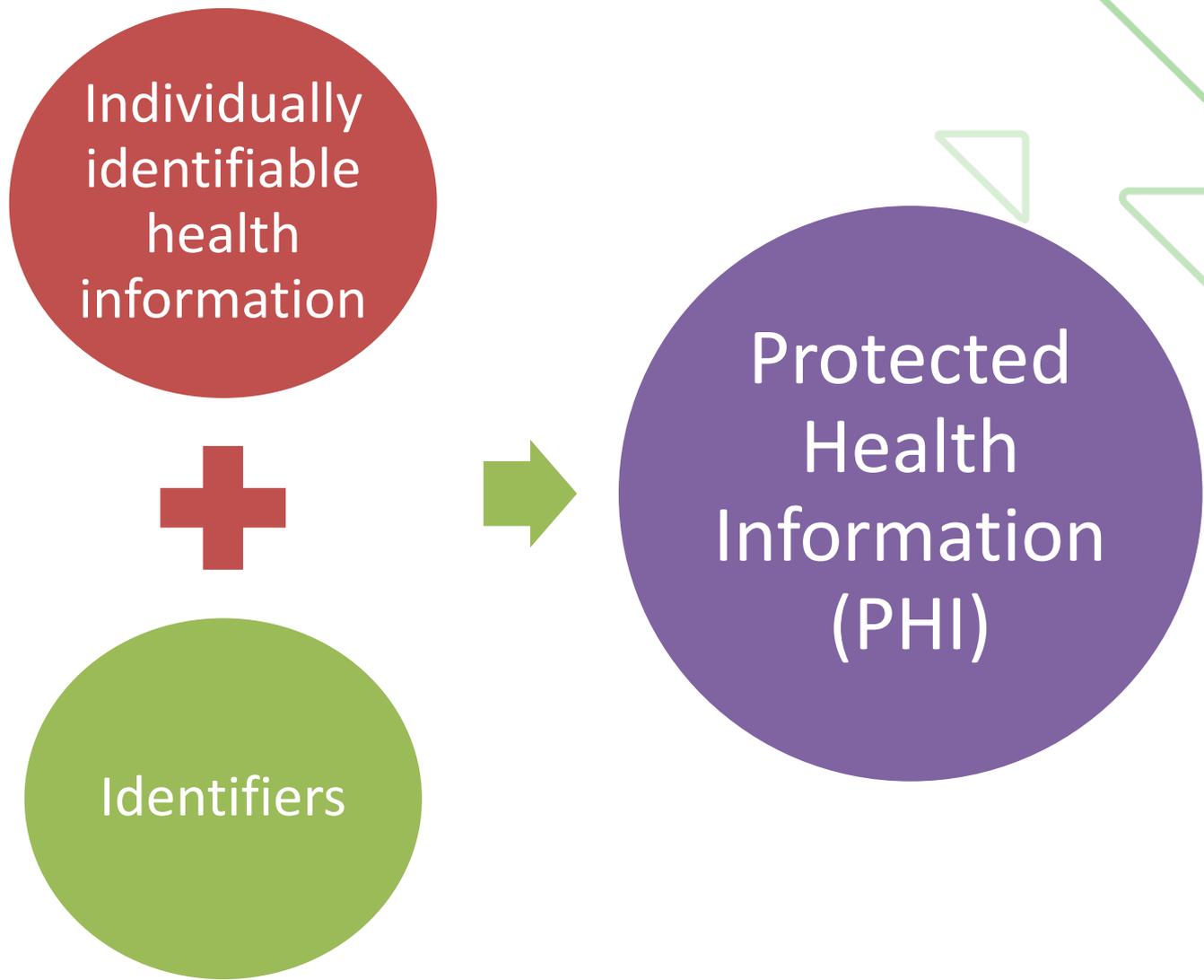
- **Covered Entities**

- Including healthcare providers who transmit healthcare information

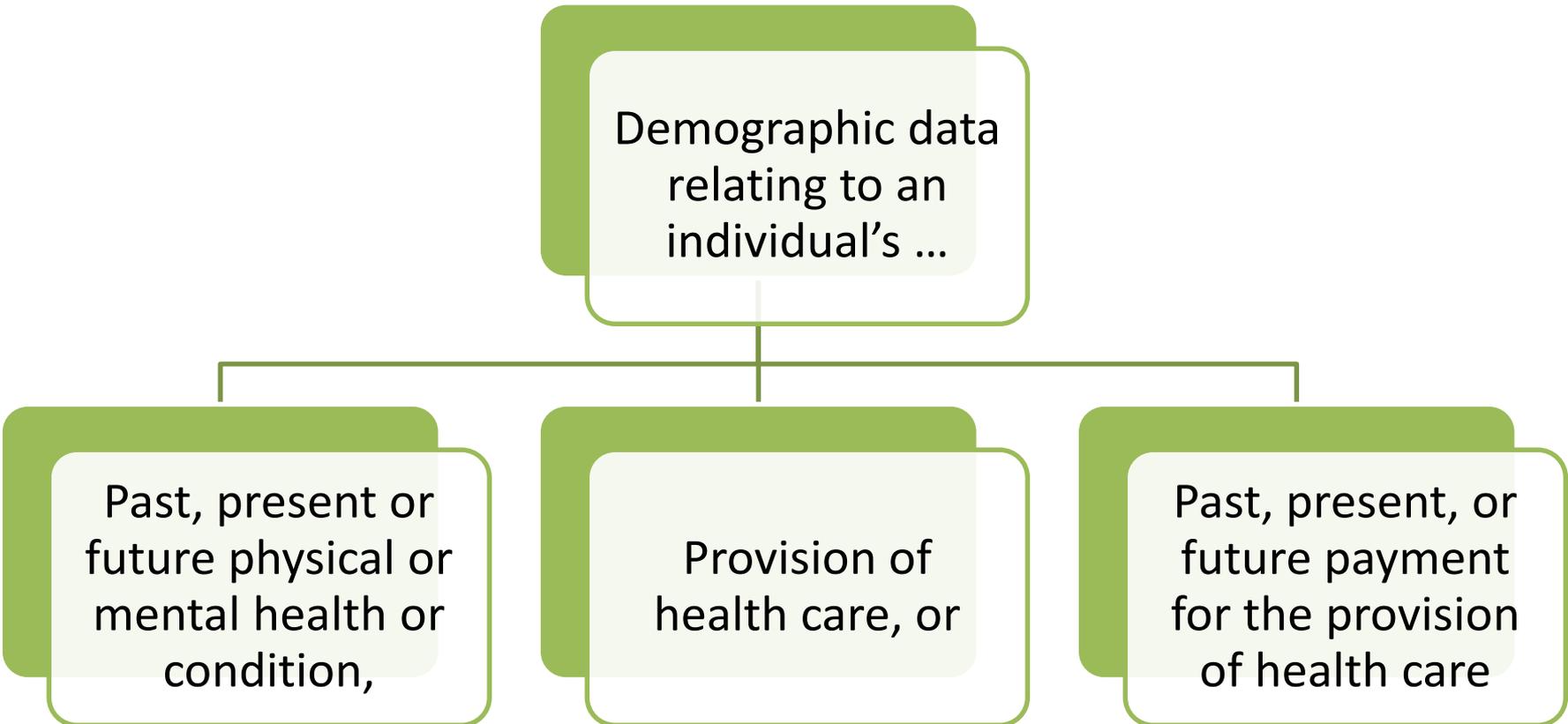
- **Business Associates (“BA”)**

- Any person/entity who/that provides services to or on behalf of a Covered Entity that involves **Individually Identifiable Health Information (“IIHI”)**.
 - A workforce member is not a BA
 - A Covered Entity may also be a BA

HIPAA Protects PHI



Individually Identifiable Health Information ...



Identifying the PHI...

Counting the ways with 18 Identifiers

1. Name
2. All geographic information smaller than state
3. Elements of dates (except year)
4. Telephone #
5. Fax #
6. Email Address
7. Social Security #
8. Medical Record #
9. Health Plan Beneficiary #
10. Account #
11. Certificate/license #
12. VIN, serial #, license plate #
13. Device identifiers/serial #
14. Web URLs
15. IP Address
16. Biometric Identifiers
17. Full face or comparable images
18. Any other unique identifying number, characteristic or code

What is “**Use**” and “**Disclosure**” of PHI

USE = sharing PHI inside the organization

- This may include hospitals within the network, co-workers who also need information to treat the patient

DISCLOSURE = sharing PHI outside of the organization

- Non-organization care services, providers or facilities (insurance companies, attorneys, hospitals outside of the network, etc.)

When do we disclose PHI?

- We may Disclose(Share) PHI when:
- The purpose is for **Treatment, Payment, Operations** (“TPO”);
- We have an “Authorization For Release of Protected Health Information Pursuant to HIPAA” form executed by the patient
- There is a Special Situation requiring disclosure:
 - Legal proceeding
 - Law enforcement
 - Avoid a serious threat to health or safety
 - Public health risk

Incidental Disclosures

Disclosures of PHI which cannot
be avoided.

BUT ...

The risk of an incidental disclosure
must be minimized.

What constitutes a breach?

Any impermissible use, access, acquisition or disclosure under the Privacy Rule that compromises the security or privacy of the PHI is *presumed* to be a breach



Examples of Impermissible Uses and Disclosures



Improper Disposal of PHI





PROTECT ePHI and Electronic Medical Records

- ✓ Let your passwords be your secret (Do not share!)
- ✓ Use email to send PHI, do not text!
- ✓ Always log off of computers before leaving it by typing the following together on your keyboard:



OR



Sending PHI to incorrect recipient(s) (via mail, email or fax)



"HELLO, IS THIS THE DOCTOR'S OFFICE?... THANK YOU FOR SENDING ME ALL THAT INFORMATION, BUT MY NAME ISN'T AMBER AND I'M PRETTY SURE I'M NOT PREGNANT!"

Safeguard PHI in Mailings, Faxes & Emails

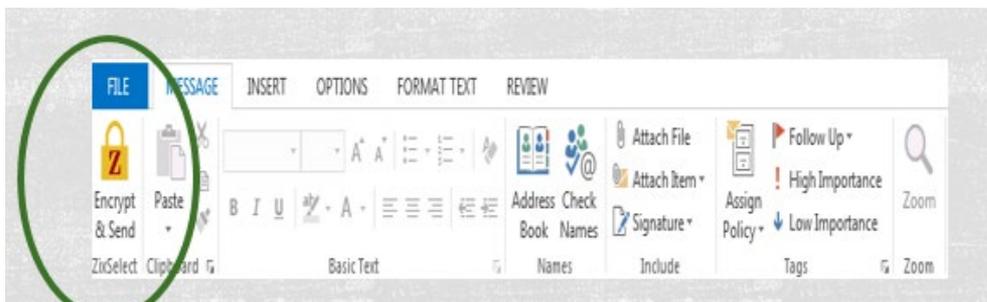
Reasonable safeguards to protect information from impermissible disclosure:

- ✓ Right recipient
- ✓ Right content
- ✓ Right fax number/email/address

EMAIL REMINDERS

Encrypt email with PHI when using your Northwell email address by either:

- (1) Including the words “PHI” or “SECURE” in the subject line of the e-mail; OR
- (2) Using the “Encrypt & Send” button, instead of the usual “SEND” button.



**Northwell Health Policy # 800.02
(Releasing PHI)**

**Northwell Health Policy # 900.11
(Emailing PHI)**

Not safeguarding paper PHI

- ***Office for Civil Rights v. Lincare:***
- **The estranged husband –**
- A home care nurse supervisor kept PHI in her car and home. When she and her husband parted ways, she left behind PHI. He contacted her job and the OCR and told them that she failed to secure PHI
- Outcome → \$239,800 fine levied on the employer



- ***Lessons for employees –***
 - Safeguard spoken and written PHI
 - Limit conversations and documents concerning patients to the work environment

Reminder to Safeguard PHI - Discussions

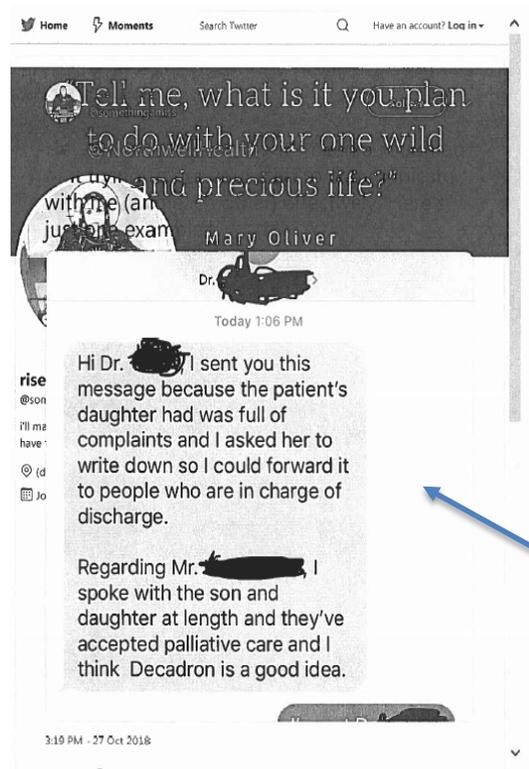
- **Discussions between health care professionals and patients and/or patients' family should include the following safeguards:**
- Only disclose the *minimal* amount of *information* necessary for an effective conversation;
- ***Confirm who can be included*** in the conversation –
 - Confirm that information can be shared in the presence of family members/friends/escorts;
 - Never ask a patient about their medical/mental health history in front of other people, only general questions can be asked in order to determine the severity of the patient's symptoms

Reminder to Safeguard PHI – Telephone Messages

- When you have to leave a message for the patient to contact you, only disclose that you are calling from Northwell Health and leave your name and a call back number;
 - Leave minimum necessary information on voicemail system, answering machines, or with a person who answers the phone.
 - It is never appropriate to leave PHI over the phone, unless authorized to do so.
 - Always verify how the patient prefers to receive information, or if it acceptable to leave messages.

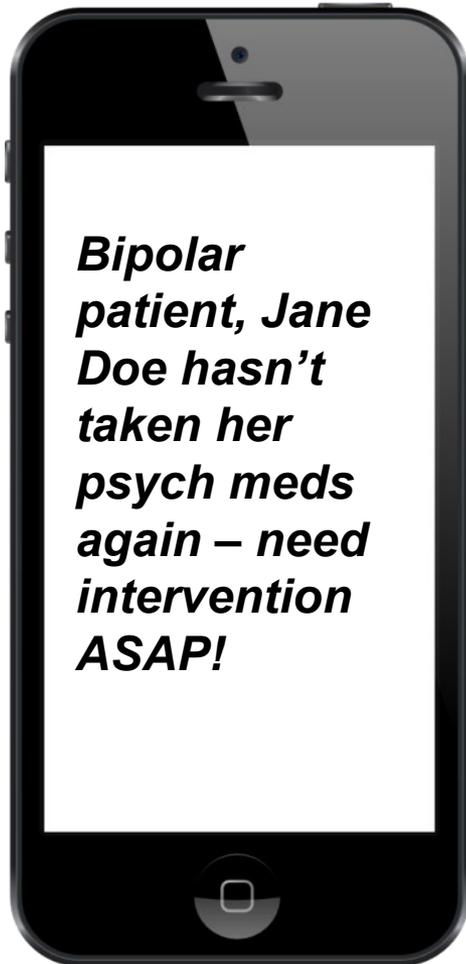
Improper Texting

- Would you be happy if you saw your text on Twitter?



The texting doctor thought he was texting another doctor, but instead texted the daughter who had the complaints...

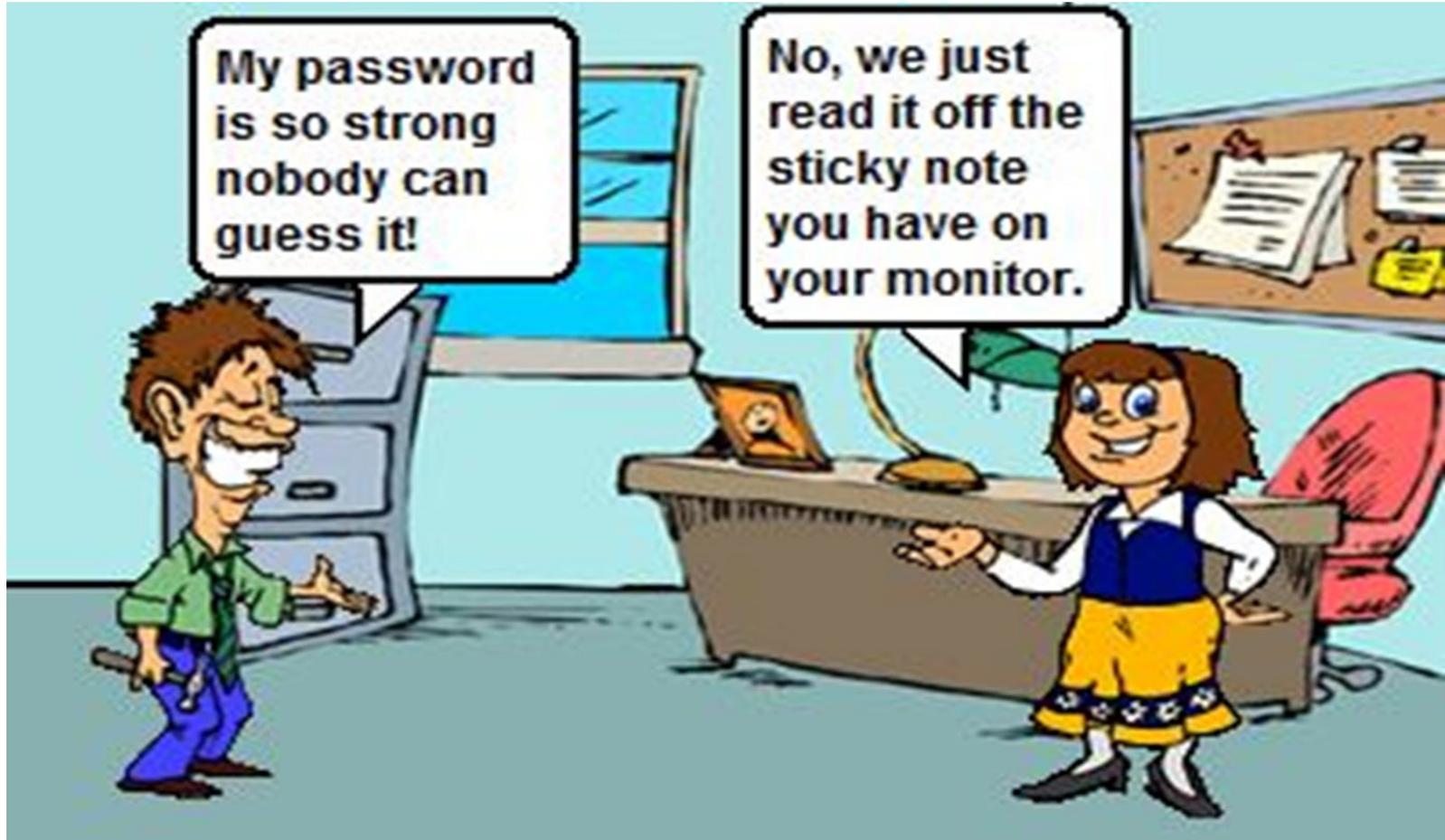
Which text is acceptable?



- ✓ Never include a patient's name , address or other identifier in a text – email this information using secured email
- ✓ Call to provide PHI instead of placing it in a text
- ✓ Never take pictures or video using your phone.



Failing to safeguard PHI/ePHI by sharing or posting passwords



SNOOPING & SHARING



Accessing
medical records
or
sharing
information



Information
learned at work
to someone for
an unrelated
work purpose



***HIPAA
VIOLATION***

Failing to Resist Natural Curiosity

Hospital Security

Northwestern Memorial Fires 60 Employees for Accessing Celebrity's Records

The former employees say they were fired for inappropriately accessing 'Empire' actor Jussie Smollett's medical records, which many are denying.

- “HIPAA has a requirement that people only have access to the minimum necessary information to do their jobs, so if they're not involved in treating [Smollett], they shouldn't have access to even his name,” said attorney Erin Jackson. “The consequences are grave. We're talking about huge fines, potentially criminal liability.”

• <https://www.campussafetymagazine.com/hospital/northwestern-memorial-fires-employees/>

How does Compliance respond to a HIPAA violation?



* Notification is based on classification – possibly patient and/or Office for Civil Rights)



- Compliance investigates a potential violation using a number of tools, including, but not limited to:
 - ✓ Interviews (employees, supervisors, patients, etc.)
 - ✓ Documentation review (including electronic and paper records – health, financial, time records, etc.)
 - ✓ Research
 - ✓ Technological software
- ✓ Compliance needs your help to investigate.
- ✓ Reports are kept confidential.
- ✓ Northwell prohibits retaliation or intimidation for reporting a concern in good faith.



Therefore, REPORT any experience of retaliation or intimidation AFTER you reported a concern in good faith OR are COOPERATING with an investigation.

**Northwell Health Policy # 800.01
(Non-Retaliation)**

Why is this important?



Reputational Risks



Legal Risks

Financial Risks

See something... Speak something

Report a potential violation to Compliance when you first suspect one!



Not sure...

Have doubts

Just report!

Reporting a Compliance/Privacy Concern

- Contact your supervisor/manager
- Online link through the Office of Corporate
- Compliance's website found on the Intranet
- Contact the Health System's SVP and Chief Corporate Compliance Officer or a Compliance Director **516-465-8097**
- Office of Corporate Compliance's Help Line: **800-894-3226**
- Or you can Contact Karen Trujillo RN MSN at HCN:
516- 224-6498
- **ALL REPORTS ARE HELD IN THE STRICTEST OF CONFIDENCE AND MAY BE MADE ANONYMOUSLY.**

Improper Use of passwords...

Accessing the healthcare data of patients without authorization is prohibited under HIPAA legislation, and disclosing it to a third party is a criminal matter. The offense carries a jail term of up to 10 years in addition to a maximum fine of \$500,000 if the disclosure is made for personal gain.

A South Carolina government employee was sentenced to three years' probation and community service for emailing the records of 228,000 Medicare and Medicaid recipients to his personal email address.

Texas healthcare worker gets 18 months in prison for accessing PHI at work with the intention of selling it for personal gain.

Industry Developments: Social Media Reminders

Social Media Posts Can Be Expensive

For example, if a patient posts an unfavorable review of a practice or cites a disagreement with a practice, the practice and its employees cannot subsequently confront the patient on social media.

In October 2019, OCR reached a \$10,000 settlement with Elite Dental, a Dallas, Texas dental practice, for potential HIPAA violations after the practice had responded to social media reviews by disclosing patient names and other PHI. OCR's investigation found that Elite had impermissibly disclosed the PHI of multiple patients in response to patient reviews on the Elite Yelp! review page.

