Stony Brook
Medicine

Objectives

Text – Acceptable texting practices & legal challenges (TCPA)

eMail – Acceptable/unacceptable messages, risks, safe communications

Social Media – advantages & disadvantages

Networking/Outreach – communicating with other providers

Texting with each other

1) Consider mobile device security (encryption, password protection, loss/theft, malware, Network/Wi-Fi, vendor selection)
2) Consider mobile device privacy (use in public places, over-the-shoulder snooping, device sharing)
3) Personal vs. Business devices (security settings on the devices, permissible apps, cookies/autofill, time-out/lock-out, password protection, jail-breaking, right to examine for compliance/investigations, etc.)

Policies

- Text messages containing PHI must be sent in a secure (encrypted) manner
- Text messages containing PHI must be sent from only approved devices
- Approved personal cellphones must be submitted to IT to be properly sanitized upon separation of service/termination
- The mobile device used to text PHI must be password protected at all times
- The mobile device used to text PHI must be configured to lock automatically after a period of inactivity not to exceed five (5) minutes
- All text messages containing PHI/ePHI must be limited to the minimum amount of information necessary and caution when using multiple identifiers (full patient name, date of birth, MRN, SSN & condition)
- Safety first – no abbreviations/shorthand messages, no patient orders, confirm delivery/receipt of the message, messages used for clinical decision making are documented in the MR
- Report all texts in violation of this policy to the Privacy Officer for breach risk determination

Texting with a patient

Patients are not held to HIPAA

But, HCPs are held to HIPAA

Patient can text you anything they want

You cannot reply back with a message that contains PHI – keep your response simple

What if you initiate the contact?

The content of your response MUST not include “personal identifiers” and the patient has to agree to receiving text messages in compliance w/ the Healthcare Message Exemption under the Telephone Consumer Protection Act/TCPA:

Permitted artificial/prerecorded calls and/or text messages to cellphones w/o consent:

Appointment and exams

Confirmations and reminders

Wellness checkups

Pre-registration instructions

Lab results

Post-Discharge follow-up intended to prevent readmission

Prescription notifications

Home healthcare instructions

Remember…

The call must be free to the end user

The customer must provide the wireless phone number to the caller

The message must contain certain disclosures - name & HCP contact info

The message MUST not contain any telemarketing, cross-marketing, solicitation, debt collection or advertising content.

The message must be short—one minute or less for calls and 160 characters or less for texts.

There must be an easy opt-out mechanism and an immediate honoring of opt-out requests.

There can be no more than one message per day, three messages per week, per sender.

eMail

Still widely used/Still inherently not secure

Unless…

Your service provider is willing to sign a Business Associate Agreement (BAA)

Your service provider offers encryption both in transit and at rest

You have policies and procedures in place to address HIPAA compliance

Similar requirements to those for texting - password protected, encrypted, auto-lock for inactivity no more than 5 min., use of secure Wi-Fi/network connection, minimum necessary information contained in the message, no PHI in message unless encrypted, simple responses to patients (call for an appointment, prescription refill sent in to your pharmacy, lab results are in, make an appointment/call the office for your results, address safety considerations, address retention period, messages used for clinical decision making included in the MR, retention policy and misdirected emails received by an incorrect recipient must be reported to Privacy Officer for breach risk determination.

Keep communications with patients simple and when replying do not reply with all the confidential information the patient may have sent – delete it/reply w/o history, etc.

Patient Portals provide easy access for the patient to their health information & include secure a mechanism for communications

Did you know the patient has the right to direct their HCP to send their PHI to another recipient?

Did you know the patient has the right to direct their HCP to send their PHI to another recipient?

Including to a friend/family?

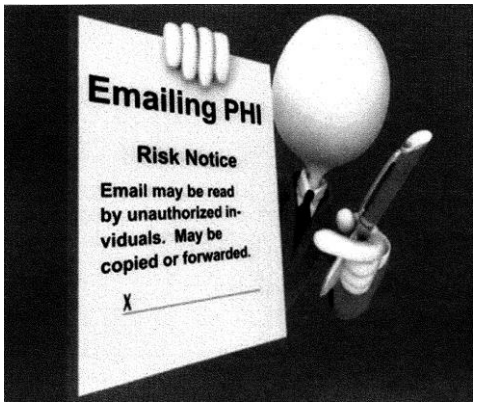
Did you know the patient has the right to direct their HCP to send their PHI to another recipient?

Including to a friend/family?

Via email?

What should I do to respond to such a request?

1. Request must be in writing
2. Must be signed by the patient/legally authorized representative
3. Must clearly identify the designated recipient
4. Must clearly identify where to send the specified PHI
5. If an unsecure method of transmission is requested (e-mail), the patient must indicate they are aware that the requested method is not secure and they want it sent anyway.



Watch out for…

Phishing

Spear phishing

Spoofing

Malware/Viruses

If you use the same device to connect to your EMR/other business systems

You may have invited a nefarious outsider into your systems/EMR

Don't use your work email for personal use:

1) it increases the amount of spam you review
2) your employer has the right to view your email
3) you do not want to be the person who invites in a hacker or virus by clicking on a link or attachment in a personal email b/c that email will have to be shared with the CISO, vendor assisting with forensics exam, organizational leadership, etc.

Social Media

Stating The Obvious

Staff and Providers must never post or share information about patients that could potentially identify a patient

Ok so you avoid using identifiers

Dr. Alexandra Thran, ED physician at Westerly Hospital – Rhode Island

She posted a few cases she had seen in the ED on her Facebook page. She avoided using patient names, ages and other identifiers. Apparently, “unauthorized” third parties were able to determine the identity of one patient from the posted information about the case.

Dr. Thran immediately deleted the post as soon as the controversy ensued but it was too late. She was fired from her job and the RI Board of Medical Licensure found her guilty of “unprofessional conduct” and issued her a reprimand and $500 fine.

So what does “avoid using patient identifiers” really mean?

Don’t post patient information to social media

But, I want my practice to have a Social Media presence

Best Practice Recommendations:

- ✓ Facebook – do not friend patients
- ✓ Restrict the type of information workforce members can share via social media – new programs, new services, new staff introductions, etc. information about the practice not the patients (limit who can post i.e. Office Manager)
- ✓ Prohibit social media use during the work day
- ✓ Keep personal and professional sites separate
- ✓ Develop policies addressing inappropriate use (disparaging/defamatory comments about employer, violation of privacy and that ramifications of a violation may lead to discipline up to and including termination)

Best Practice Recommendations continued:

- ✓ Have a social media plan
- ✓ Limit how many social media platforms you use
- ✓ Don't use excessive hashtags
- ✓ Proofread and then do it again before posting
- ✓ Respond to customer complaint promptly – don't delete as that will only make them angrier

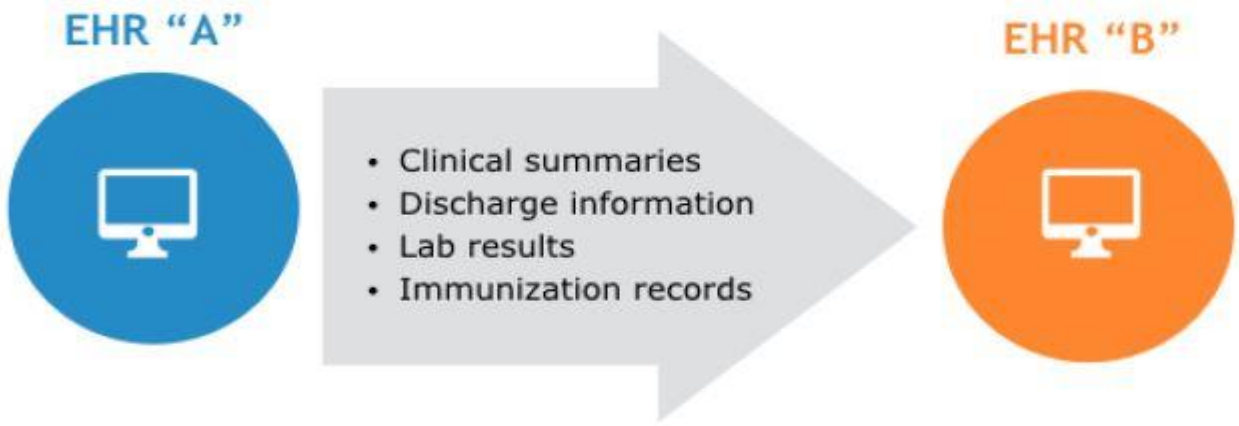
Dr. Farris Timimi, Medical Director Mayo Clinic Center for Social Media offers his 12 word social media guide

Don't Lie, Don't Pry, Don't Cheat, Don't Delete, Don't Steal, Don't Reveal

Networking/Outreach

Mechanisms to communicate with other Providers/Receive Patient Information

1) RHIO
2) Public HIE vs. Private HIE
3) Direct Messaging
4) DPC pilot program


EHR "A"
EHR "B"
• Clinical summaries
• Discharge information
• Lab results
• Immunization records

How do I implement Direct?

You need to obtain a Direct address, i.e. stephanie.musso@direct.stonybrookmedicine.edu

Health Internet Service Providers (HISPs) issue Direct addresses and provide the software you need to use them

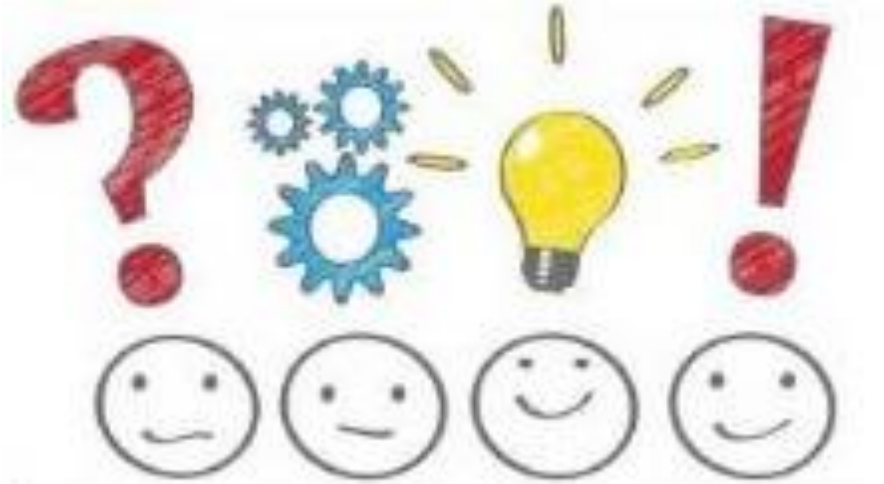
HISPs Include:

- ONC certified EHR vendors offer Direct addresses
- Companies that specialize in stand-alone Direct services through cloud-based applications
- HIE networks (independently or state sponsored) via a web-based application

Fees: monthly or pay-per-message charges

Provider Directory: In development – DirectTrust and long overdue

Thank you!



hipaa@stonybrookmedicine.edu

(631) 444-5796