Texting and Emailing Patients, Providers and Others: HIPAA, CMS, and Suggestions



Bo Ferger Rhinogram, Inc.

Kim C. Stanger Holland & Hart LLP

(2-18)



Preliminaries

This presentation is similar to any other legal education materials designed to provide general information on pertinent legal topics. The statements made as part of the presentation are provided for educational purposes only. They do not constitute legal advice nor do they necessarily reflect the views of Holland & Hart LLP or any of its attorneys other than the speaker. This presentation is not intended to create an attorney-client relationship between you and Holland & Hart LLP. If you have specific questions as to the application of law to your activities, you should seek the advice of your legal counsel.



Overview

Kim Stanger

- Relevant rules that apply to texts or e-mails:
 - To patients.
 - To other providers.
 - To others
- Texting orders
- Risk management issues

Bo Ferger

- Technical issues
- What to look for in a compliant solution



Preliminaries

- Submit questions via chat feature or directly to <u>kcstanger@hollandhart.com</u>.
- The session will be recorded and available for download at <u>http://www.hhhealthlawblog.com/webinar-</u>

recordings-and-presentations.



Written Materials

- H&H Client Alert, *HIPAA, E-mails and Texts*
- HHS, Individual's Right Under HIPAA to Access Their Protected Health Information (6/16)
- HHS, Omnibus Rule Commentary, 78 FR 5634 (1/25/13)
- Joint Commission, "Use of Secure Text Messaging for Patient Care Orders Is Not Acceptable," *The Joint Commission Perspectives* (12/16)
- CMS S&C Letter 18-10-ALL (12/28/17)
- AMA Guidelines for Patient-Physician E-Mail and Text Messaging



Preliminaries

- We will focus on HIPAA and CMS rules.
- Other rules may apply depending on your circumstances.
 - Federal laws or regulations
 - State laws or regulations
 - Contract requirements
 - Accreditation requirements
- Additional risk management issues should be considered.



To Text or Not to Text

Pros

- Common means of communication
- Available anywhere (so long as sender has a smartphone)
- Instantaneous
- Avoids phone tag
- Likely to reach recipient
- Providers generally want it to make their life easier

Cons

- Subject to errors in text.
- Subject to misinterpretation.
- Not in medical record.
- May be sent to wrong recipient.
- Cannot authenticate recipient.
- May not be able to confirm receipt.
- Receipt may be delayed.
- May be stored on unsecure device.
- May be stored on server.
- Regulatory risks



Health Insurance Portability and Accountability Act ("HIPAA")





Entities Subject to HIPAA

- Covered entities
 - Health care providers who engage in certain electronic transactions.
 - Health plans, including employee group health plans if:
 - 50 or more participants; or
 - Administered by third party (e.g., TPA or insurer).
 - Health care clearinghouses.
- Business associates of covered entities
 - Entities with whom you share PHI to perform services on your behalf.

(45 CFR 160.103)



Protected Health Information

- Protected health info ("PHI") =
 - Individually identifiable health info, i.e., info that could be used to identify individual.
 - Concerns physical or mental health, health care, or payment.
 - Created or received by covered entity in its capacity as a healthcare provider.
 - Maintained in any form or medium, e.g., oral, paper, electronic, images, etc.

(45 CFR 160.103)



Protected Health Info

- To de-identify PHI, must remove certain identifiers, e.g.,
 - Names
 - Physical address
 - Birth date, admission date, discharge date, date of death, etc.
 - Telephone numbers
 - E-mail mail addresses
 - Social security numbers
 - Medical record numbers
 - Account numbers
 - Device identifiers and serial numbers
 - Web Universal Resource Locators (URLs)
 - Internet Protocol (IP) address numbers
 - Full face photographic images and any comparable images
- Any other unique identifying number, characteristic, or code.
 (45 CFR 164.514(b) HOLLAND&

Presumptively PHI
if related to health or health care



HIPAA

- Privacy Rule (45 CFR 164.500 et seq.)
 - Covered entity or business associate may not use or disclose PHI without the patient's authorization unless an exception applies.
 - Covered entity must implement reasonable safeguards to protect PHI.
 - Patients have certain rights concerning their PHI.
- Security Rule (45 CFR 164.300 et seq.)
 - Covered entity and business associate must implement safeguards to protect confidentiality, availability and integrity of e-PHI.
- Breach Notification Rule (45 CFR 164.400 et seq.)
 - Must report breaches if unsecured PHI to individual, HHS, and, in some cases, media.



HIPAA Civil Penalties

(as modified by recent inflation adjustment)

Conduct	Penalty
Did not know and should not have known of violation	 \$112 to \$55,910 per violation Up to \$1,667,299 per type per year No penalty if correct w/in 30 days OCR may waive or reduce penalty
Violation due to reasonable cause	 \$1,118 to \$55,910 per violation Up to \$1,667,299 per type per year No penalty if correct w/in 30 days OCR may waive or reduce penalty
Willful neglect, but correct w/in 30 days	 \$11,182 to \$55,910 per violation Up to \$1,667,299 per type per year Penalty is mandatory
Willful neglect, but do not correct w/in 30 days	 At least \$55,910 per violation Up to \$1,667,299 per type per year Penalty is mandatory
(45 CFR 160.404; see also 74 FR 56127)	I I ULLAND &I IAKI.

OCR Settlements in 2017		
12/17	Cancer center failed to implement safeguards to protect ePHI despite prior warnings that its information had been hacked.	\$2,300,000
5/17	Hospital issued press release containing patient's name after patient used fraudulent identification card.	\$2,400,000
5/17	Health center faxed HIV information to wrong entity.	\$387,000
4/17	Monitoring company's laptop containing 1,390 patients' info stolen from car; insufficient risk analysis and no finalized security policies.	\$2,500,000
4/17	No business associate agreement ("BAA") with record storage company.	\$31,000
4/17	FQHC's info hacked; no risk analysis and insufficient security rule safeguards.	\$400,000
2/17	Hospital allowed unauthorized employees to access and disclose records of 80,000 patients; failed to terminate users' right of access.	\$5,500,000
2/17	Hospital lost unencrypted PDAs containing info of 6,200 persons; failure to take timely action to address known risks.	\$3,200,000
1/17	Insurance company's unencrypted USB containing info of 2,209 persons stolen; no risk analysis, implementation, or encryption.	\$2,200,000
1/17	Failure to timely report breach.	\$475,000

HIPAA Civil Penalties

- "A covered entity's employee lost an unencrypted laptop that contained unsecured protected health information. HHS's investigation reveals the covered entity feared its reputation would be harmed if information about the incident became public and, therefore, decided not to provide notification as required by § 164.400 et seq."
- Failure to report → "willful neglect" → mandatory penalties (\$10,000 to \$50,000 per violation)
 (75 FR 40879)



HIPAA Privacy Rule

- Covered entity and business associate must:
 - Ensure the use or disclosure is for a permissible purpose (e.g., treatment purposes or disclosure to family) or obtain the patient's authorization.
 - Implement reasonable safeguards to protect the PHI.
 - Limit disclosure to the minimum necessary.
 - Verify identity of the recipient.
- Patient has right to receive communications by alternative means or at alternative locations.
 (45 CFR 164.500 et seq.)



HIPAA Security Rule

- Covered entities and business associates must, e.g.,
 - Conduct a risk assessment of ePHI.
 - Implement administrative, physical, technical safeguards, e.g.,
 - Access controls
 - Unique user identification (Required)
 - Automatic logoff (Addressable)
 - Encryption (Addressable)
 - Transmission security
 - Integrity controls (Addressable)
 - Encryption (Addressable)

(45 CFR 164.300 et seq.; 45 CFR 164.312)



HIPAA Security Rule

"When a standard ... includes addressable implementation specifications, a covered entity or business associate must—

"(A) Implement the implementation specification if reasonable and appropriate; or

"(B) If implementing the implementation specification is not reasonable and appropriate—

"(1) Document why it would not be reasonable and appropriate to implement the implementation specification; and

"(2) Implement an equivalent alternative measure if reasonable and appropriate."

(45 CFR 164.306(d)(3))

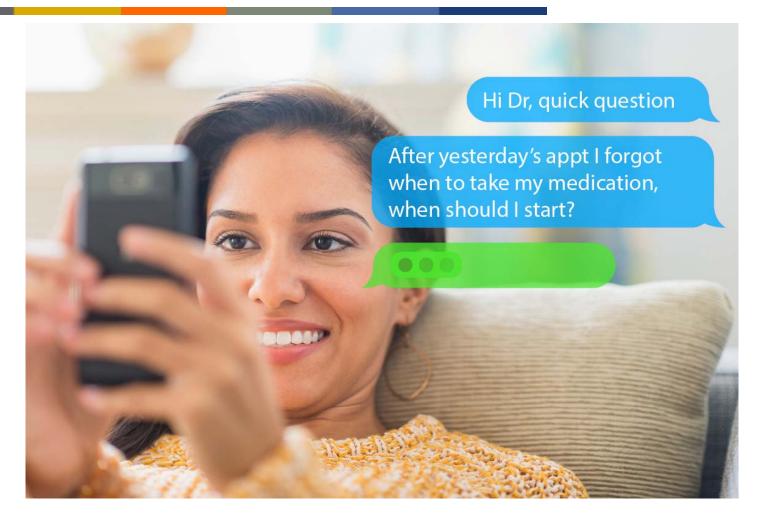


HIPAA Security Rule: Encryption

"Is the use of encryption mandatory in the Security Rule?

"Answer: No. The final Security Rule made the use of encryption an addressable implementation specification.... [It must] be implemented if, after a risk assessment, the entity has determined that the specification is a reasonable and appropriate safeguard in its risk management of the confidentiality, integrity and availability of e-PHI. If the entity decides that the addressable implementation specification is not reasonable and appropriate, it must document that determination and implement an equivalent alternative measure..."

(hhs.gov/hipaa/for-professionals/faq/2001/is-the-use-of-encryption-mandatory-inthe-security-rule/index.html) HOLLAND&HART





Security Rule

 "[A covered entity must] implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network." (45 CFR 164.312(e))

Privacy Rule

"A covered health care provider must permit individuals to request and must accommodate reasonable
requests by individuals to receive communications of protected health information from the covered health care provider by alternative means or at alternative locations." (45 CFR 164.522(b))



Texting and E-mailing Patients: Privacy Rule

"Does the HIPAA Privacy Rule permit health care providers to use e-mail to discuss health issues and treatment with their patients?

"Answer: Yes. The Privacy Rule allows covered health care providers to communicate electronically, such as through e-mail, with their patients, provided they apply reasonable safeguards when doing so.... For example, certain precautions may need to be taken when using e-mail to avoid unintentional disclosures, such as checking the e-mail address for accuracy before sending, or sending an e-mail alert to the patient for address confirmation prior to sending the message. Further, while the Privacy Rule does not prohibit the use of unencrypted e-mail for treatment-related communications between health care providers and patients, other safeguards should be applied to reasonably protect privacy, such as limiting the amount or type of information disclosed through the unencrypted e-mail. In addition, covered entities will want to ensure that any transmission of ePHI is in compliance with the HIPAA Security Rule."

(www.hhs.gov/hipaa/for-professionals/faq/570/does-hipaa-permit-health-care-providers-to-use-email-to-discuss-health-issues-with-patients/index.html)



Texting and E-mailing Patients: Security Rule

"Does the Security Rule allow for sending electronic PHI (e-PHI) in an email or over the Internet? If so, what protections must be applied? "Answer: The Security Rule does not expressly prohibit the use of email for sending e-PHI. However, the standards for access control (45 CFR § 164.312(a)), integrity (45 CFR § 164.312(c)(1)), and transmission security (45 CFR § 164.312(e)(1)) require covered entities to implement policies and procedures to restrict access to, protect the integrity of, and guard against unauthorized access to e-PHI. The standard for

guard against unauthorized access to e-PHI. The standard for transmission security (§ 164.312(e)) also includes addressable specifications for integrity controls and encryption. This means that the covered entity must assess its use of open networks, identify the available and appropriate means to protect e-PHI as it is transmitted, select a solution, and document the decision. The Security Rule allows for e-PHI to be sent over an electronic open network as long as it is adequately protected."

(www.hhs.gov/hipaa/for-professionals/faq/2006/does-the-security-rule-allow-forsending-electronic-phi-in-an-email/index.html) HOLLAND&HART

• "[C]overed entities are permitted to send individuals unencrypted emails if they have advised the individual of the risk, and the individual still prefers the unencrypted email. We disagree that the "duty to warn" individuals of risks associated with unencrypted email would be unduly burdensome on covered entities and believe this is a necessary step in protecting the protected health information. We do not expect covered entities to educate individuals about encryption technology and the information security. Rather, we merely expect the covered entity to notify the individual that there may be some level of risk that the information in the email could be read by a third party. If individuals are notified of the risks and still prefer unencrypted email, the individual has the right to receive protected health information in that way, and covered entities are not responsible for unauthorized access of protected health information while in transmission to the individual based on the individual's request."

(78 FR 5634)



"Do individuals have the right under HIPAA to have copies of their PHI transferred or transmitted to them in the manner they request, even if the requested mode of transfer or transmission is unsecure?

"Yes, as long as the PHI is 'readily producible' in the manner requested, based on the capabilities of the covered entity and transmission or transfer in such a manner would not present an unacceptable level of security risk to the PHI on the covered entity's systems... For example, individuals generally have a right to receive copies of their PHI by mail or e-mail, if they request. It is expected that all covered entities have the capability to transmit PHI by mail or e-mail ..."

(OCR Guidance on Patient Access, available at <u>https://www.hhs.gov/hipaa/for-</u> professionals/privacy/guidance/access/index.html) HOLLAND&HART

"Further, while covered entities are required by the Privacy and Security Rules to implement reasonable safeguards to protect PHI while in transit, individuals have a right to receive a copy of their PHI by unencrypted e-mail if the individual requests access in this manner. In such cases, the covered entity must provide a brief warning to the individual that there is some level of risk that the individual's PHI could be read or otherwise accessed by a third party while in transit, and confirm that the individual still wants to receive her PHI by unencrypted e-mail. If the individual says yes, the covered entity must comply with the request." (OCR Guidance on Patient Access, available at https://www.hhs.gov/hipaa/forprofessionals/privacy/guidance/access/index.html)



- "Is a covered entity responsible if it complies with an individual's access request to receive PHI in an unsecure manner (e.g., unencrypted e-mail) and the information is intercepted while in transit?
- "No. While covered entities are responsible for adopting reasonable safeguards in implementing the individual's request (e.g., correctly entering the e-mail address), covered entities are not responsible for a disclosure of PHI while in transmission to the individual based on the individual's access request to receive the PHI in an unsecure manner (assuming the individual was warned of and accepted the risks associated with the unsecure transmission). This includes breach notification obligations and liability for disclosures that occur in transit. Further, covered entities are not responsible for safeguarding the information once delivered to the individual."
- (OCR Guidance on Patient Access, available at <u>https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html</u>)



Texting and E-mailing Patients: Can You Require Unsecure Messages?

- "A covered entity may not require individuals to waive their rights under [the Privacy or Security Rules] as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits. (45 CFR 164.530(h))
- "A covered entity may not condition the provision to an individual of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of an authorization..." (45 CFR 164.508(b)(4))
- "[A] covered entity is not permitted to require an individual to accept unsecure methods of transmission in order to receive copies of her health information." (OCR Guidance on Patient Access, available at https://www.hhs.gov/hipaa/forprofessionals/privacy/guidance/access/index.html) HOLLAND&HART.

Texting and E-mailing Patients: Must You Make It Available?

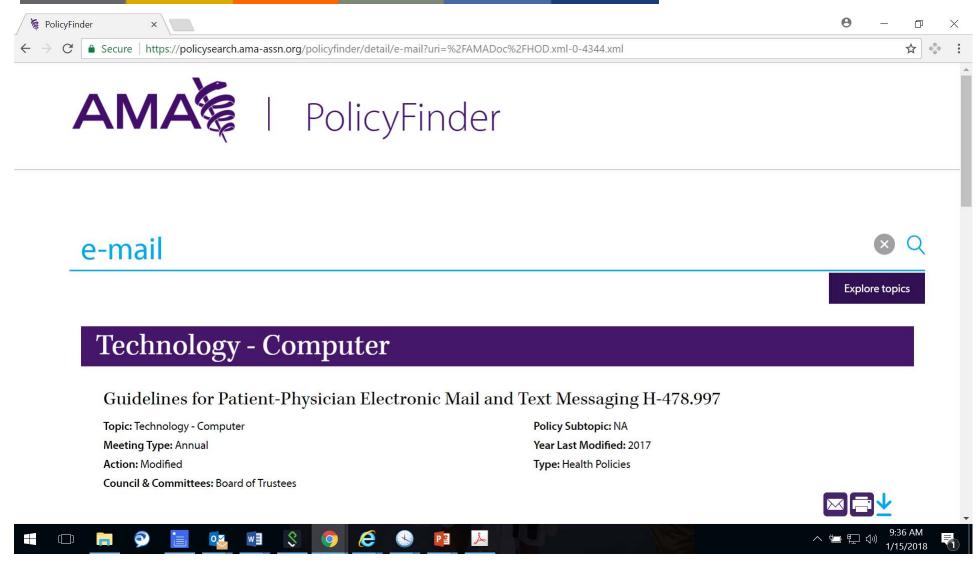
"It is expected that all covered entities have the capability to transmit PHI by mail or e-mail (except in the limited case where e-mail cannot accommodate the file size of requested images), and transmitting PHI in such a manner does not present unacceptable security risks to the systems of covered entities, even though there may be security risks to the PHI while in transit (such as where an individual has requested to receive her PHI by, and accepted the risks associated with, unencrypted e-mail." (OCR Guidance on Patient Access, available at https://www.hhs.gov/hipaa/forprofessionals/privacy/guidance/access/index.html)



Texts and E-mails <u>from</u>Patients

- "The Security Rule ... does not apply to the patient. A patient may send health information to you using email or texting that is not secure. That health information becomes protected by the HIPAA Rules when you receive it." (OCR Guide to Patient Access at p.31).
- "Patients may initiate communications with a provider using e-mail. If this situation occurs, the health care provider can assume (unless the patient has explicitly stated otherwise) that e-mail communications are acceptable to the individual. If the provider feels the patient may not be aware of the possible risks of using unencrypted e-mail, or has concerns about potential liability, the provider can alert the patient of those risks, and let the patient decide whether to continue email communications. (OCR FAQ, available at http://www.hhs.gov/ocr/privacy/hipaa/faq/health_information_technology/570 .html).

AMA Guidelines for Patient-Physician E-Mail and Text Messaging



Texting or E-mailing Providers or Other Persons





Texting or E-mailing Others: Privacy Rule

"Does the HIPAA Privacy Rule permit a covered health care provider to e-mail or otherwise electronically exchange ... PHI with another provider for treatment purposes?

"Yes. The Privacy Rule allows covered health care providers to share PHI electronically (or in any other form) for treatment purposes, as long as they apply reasonable safeguards when doing so. Thus, for example, a physician may consult with another physician by e-mail about a patient's condition, or health care providers may electronically exchange PHI to and through a health information organization (HIO) for patient care."

(OCR FAQ dated 12/15/08)



Texting or E-mailing Others: Security Rule

"Can you use texting to communicate health information, even if it is to another provider or professional?

"Answer: It depends. Text messages are generally not secure because they lack encryption, and the sender does not know with certainty the message is received by the intended recipient. Also, the telecommunication vendor/wireless carrier may store the text messages. However, your organization may approve texting after performing a risk analysis or implementing a thirdparty messaging solution that incorporates measures to establish a secure communication platform that will allow texting on approved mobile devices."

(<u>www.healthit.gov/providers-professionals/faqs/can-you-use-texting-</u> <u>communicate-health-information-even-if-it-another-p</u>)



May Patient Authorize Use of Unsecure Text or E-mail?

Not clear how OCR would respond...

Arguments in Support

- HIPAA is primarily intended to protect patient's privacy interests.
- Patient has the right to determine what happens to their PHI.
- Patient may require transmission of PHI to third party by unsecure means per 45 CFR 164.524.
- Patient should be able to authorize disclosure by unsecure means per 45 CFR 164.508.

Arguments Against

- Providers are generally required to comply with security rule.
- "A covered entity may not require individuals to waive their rights under [the Privacy or Security Rule] as a condition of the provision of treatment...." (45 CFR 164.530(h))
- For an authorization, "PHI must be sent securely." (OCR Guidance on Access).



May Patient Authorize Providers to Text or E-mail Others via Unsecure Network

- "A covered entity is permitted to use or disclose PHI ... pursuant to and in compliance with a valid authorization under §164.508." (45 CFR 164.502(a)(1)(iv))
- "If an individual's request for access directs the covered entity to transmit the copy of PHI directly to another person designated by the individual, the covered entity must provide the copy to the person designated by the individual. The individual's request must be in writing, signed by the individual, and clearly identify the designated person and where to send the copy of PHI." (45 CFR 164.524(c)(3)(ii))



May Patient Authorize Providers to Text or E-mail Others via Unsecure Network

"If requested by an individual, a covered entity must transmit an individual's PHI directly to another person or entity designated by the individual. The individual's request must be in writing, signed by the individual, and clearly identify the designated person or entity and where to send the PHI.... [T]he individual can designate the form and format of the PHI and how the PHI is to be sent to the third party...

"[For example,] a patient requests in writing that the hospital where she recently underwent a surgical procedure use its Certified EHR Technology (CEHRT) to send her discharge summary to her primary care physician...."

(OCR Guidance on Patient's Access, available at <u>https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html</u>)



May Patient Authorize Providers to Text or E-mail Others via Unsecure Network

• "[C]overed entities must safeguard the information in transit, and ... may be liable for impermissible disclosures of PHI that occur in transit. The only exception arises when an individual has requested that the PHI be sent to the third party by unencrypted e-mail or in another unsecure manner, which the individual has a right to request. As long as the individual was warned of and accepted the security risks to the PHI associated with the unsecure transmission, the covered entity is not responsible for breach notification or liable for disclosures that occur in transit.

(OCR Guidance on Patient's Access, available at <u>https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html</u>)



Texting in Facilities





Joint Commission and CMS: Texting Orders

- 2011: Joint Commission prohibits texting orders.
- 5/16: Joint Commission allows texting orders if platform secure, elements of order included, etc.
- 7/16: Joint Commission reinstates prohibition while it obtains clarification.
- 12/16: Joint commission reaffirms prohibition on texting orders.
 - Burden on nurses to manually input order into medical record.
 - Verbal order allows for real-time clarification and confirmation.
 - If CDS recommendation or alert is triggered while entering verbal order, nurse can ask practitioner immediately.
- 12/18: HCCA publishes article recounting recent CMS emails prohibiting all texting re patient care.



CMS: Texting in Facilities

18-10-ALL ×				Θ	—
C Secure https://	/www.cms.gov/Medicare/Prov	ider-Enrollment-and-Certification/Surve	eyCertificationGenInfo/Downloads/Survey-and-Cert-Letter-18-10.pd	lf	Z
-10-ALL		1 / 2	2	¢	Ŧ
	Centers for Med 7500 Security Bo Baltimore, Mary Center for C DATE: TO: FROM: SUBJECT:	OF HEALTH & HUMAN SERVICES icare & Medicaid Services pulevard, Mail Stop C2-21-16 land 21244-1850 Inical Standards and Quality/Surv December 28, 2017 State Survey Agency Directors Director Survey and Certification Group Texting of Patient Information among Memorandum	Ref: S&C 18-10-ALL		
	accom	nplished through a secure platform. ng of patient orders is prohibited reg			
	• Comp	• • • • •	POE) is the preferred method of order entry		
	Background				

CMS: Texting in Facilities

- "Texting patient information among members of the health care team is permissible if accomplished through a secure platform."
- "Texting of patient orders is prohibited regardless of the platform utilized."
- "Computerized Provider Order Entry (CPOE) is the preferred method of order entry by a provider."
 (CMS S&C Letter 18-10-ALL (12/28/17))



CMS: Texting Orders

- Texting orders violates the CoPs and CfCs, e.g.,
 - Hospitals must maintain medical records and protect the security of record entries.
 - Hospitals must maintain records for at least 5 years.
 - Hospitals must protect confidentiality of records. (*See, e.g.,* 42 CFR 489.24)



CMS:

Computerized Provider Order Entry

"Computerized Provider Order Entry (CPOE) is the preferred method of order entry by a provider. CMS has held to the long standing practice that a physician or Licensed Independent Practitioner (LIP) should enter orders into the medical record via a hand written order or via CPOE. An order if entered via CPOE, with an immediate download into the provider's electronic health records (EHR), is permitted as the order would be dated, timed, authenticated, and promptly placed in the medical record." (CMS S&C 18-10-ALL (12/28/17))



Can You Treat Text as "Verbal Order"?

- CPOE rule refers to "hand written order..."
- CMS/Joint Commission concerns about texting orders included:
 - Burden on nurses to manually input order into medical record.
 - Verbal order allows for real-time clarification and confirmation.
 - If CDS recommendation or alert is triggered while entering verbal order, nurse can ask practitioner immediately.
- Those concerns still remain if enter text as verbal order.



Can You Treat Text as "Verbal Order"?

- "(i) If verbal orders are used, they are to be used infrequently."
- "(ii) When verbal orders are used, they must only be accepted by persons who are authorized to do so by hospital policy and procedures consistent with Federal and State law." (42 CFR 482.23; *see also* Joint Commission, "Clarification: Use of Secure Text Messaging for Patient Care Orders Is Not Acceptable," The Joint Commission Perspectives (12/16))

Check your state law.



Can You Treat Text as "Verbal Order"?

 "[T]he possibility of errors associated with verbal orders is an important issue, and that is why we continue to believe that hospitals should make efforts to minimize the use of verbal orders... [I]t is expected that the standard practice would be for the person taking the order to read the order back to the practitioner to ensure that they have correctly understood it." (77 FR 29055)



Can You Treat Text as "Verbal Order"?

- "Verbal orders, if used, must be used infrequently. This means that the use of verbal orders must not be a common practice. Verbal orders pose an increased risk of miscommunication that could contribute to a medication or other error, resulting in a patient adverse event. Verbal orders should be used only to meet the care needs of the patient when it is impossible or impractical for the ordering practitioner to write the order or enter it into an electronic prescribing system without delaying treatment. Verbal orders are not to be used for the convenience of the ordering practitioner."
- "The content of verbal orders must be clearly communicated. CMS expects nationally accepted read-back verification practice to be implemented for every verbal order.... [A]II verbal orders must be promptly documented in the patient's medical record by the individual receiving the order."

(CMS SOM for 42 CFR 482.23(c)(3)(i); see also CMS SOM 42 CFR 485.635(d)(3)).



CMS:

Texting Other Communications

"CMS recognizes that the use of texting as a means of communication with other members of the healthcare team has become an essential and valuable means of communication among the team members. In order to be compliant with the **CoPs or CfCs, all providers must utilize and maintain** systems/platforms that are secure, encrypted, and minimize the risks to patient privacy and confidentiality as per HIPAA regulations and the CoPs or CfCs. It is expected that providers/organizations will implement procedures/processes that routinely assess the security and integrity of the texting systems/platforms that are being utilized, in order to avoid negative outcomes that could compromise the care of patients." (CMS S&C 18-10-ALL, dated 12/28/17)









Insufficient

security

protections

The U.S. Department of Health and Human Services, Office for Civil Rights (OCR), has announced a Health Insurance Portability and Accountability Act of 1996 (HIPAA) settlement based on the impermissible disclosure of unsecured electronic protected health information (ePHI). CardioNet has agreed to settle potential noncompliance with the HIPAA Privacy and Security Rules by paying \$2.5 million and implementing a corrective action plan. This settlement is the first involving a wireless health services provider, as CardioNet provides remote mobile monitoring of and rapid response to patients at risk for cardiac arrhythmias.

In January 2012, CardioNet reported to the HHS Office for Civil Rights (OCR) that a workforce member's laptop was stolen from a parked vehicle outside of the employee's home. The laptop contained the ePHI of 1,391 individuals. OCR's investigation into the impermissible disclosure revealed that CardioNet had an insufficient risk analysis and risk management processes in place at the time of the theft. Additionally, CardioNet's policies and procedures implementing the standards of the HIPAA Security Rule were in draft form and had not been implemented. Further, the Pennsylvania –based organization was unable to produce any final policies or procedures regarding the implementation of

HHS.gov		U.S. Department o	f Health & Human Services
About HHS	Programs & Services	Grants & Contracts	Laws & Regulations
Soarch Nows Poloases	FOR IMMEDIATE RELEASE January 18, 2017	Text Resize AAA	Print 🚔 Share 😭 💟 🕂 Contact: HHS Press Offic 202-690-634
\$2.2 Million		ent demonstrate	•
		ent demonstrate safeguards for el	•
Lost USB;	The U.S. Department of Health	safeguards for el	Vil Rights (OCR), has announced a
Lost USB; insufficient	The U.S. Department of Health Health Insurance Portability and impermissible disclosure of uns	and Human Services, Office for Ci d Accountability Act of 1996 (HIPAA secured electronic protected health	vil Rights (OCR), has announced a A) settlement based on the information (ePHI). MAPFRE Life
Lost USB;	The U.S. Department of Health Health Insurance Portability and impermissible disclosure of uns Insurance Company of Puerto F HIPAA Privacy and Security Ru	and Human Services, Office for Ci d Accountability Act of 1996 (HIPAA secured electronic protected health	vil Rights (OCR), has announced a A) settlement based on the information (ePHI). MAPFRE Life le potential noncompliance with the ementing a corrective action plan.
Lost USB; insufficient	The U.S. Department of Health Health Insurance Portability and impermissible disclosure of uns Insurance Company of Puerto F HIPAA Privacy and Security Ru With this resolution amount, OC provided by MAPFRE with rega	and Human Services, Office for Ci d Accountability Act of 1996 (HIPAA secured electronic protected health Rico (MAPFRE) has agreed to settl iles by paying \$2.2 million and impl CR balanced potential violations of	PHI vil Rights (OCR), has announced a A) settlement based on the information (ePHI). MAPFRE Life le potential noncompliance with the ementing a corrective action plan. the HIPAA Rules with evidence MAPFRE is a subsidiary company

On September 29, 2011, MAPFRE filed a breach report with OCR indicating that a USB data storage device (described as a "pen drive") containing ePHI was stolen from its IT department, where the

Secure https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/catholic-health-care-services/index.html

+

÷

Loss of unsecure mobile device

HIPAA for Professionals

🖑 Business Associate's Failu 🗙

Audit

Reports to Congress

State Attorneys General

Business Associate's Failure to Safeguard Nursing Home Residents' PHI Leads to \$650,000 HIPAA Settlement

Catholic Health Care Services of the Archdiocese of Philadelphia (CHCS) has agreed to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule after the theft of a CHCS mobile device compromised the protected health information (PHI) of hundreds of nursing home residents. CHCS provided management and information technology services as a business associate to six skilled nursing facilities. The total number of individuals affected by the combined breaches was 412. The settlement includes a monetary payment of \$650,000 and a corrective action plan.

Text Resize AAA

Print 📥

Share

"Business associates must implement the protections of the HIPAA Security Rule for the electronic protected health information they create, receive, maintain, or transmit from covered entities," said U.S. Department of Health and Human Services Office for Civil Rights (OCR) Director Jocelyn Samuels. "This includes an enterprise-wide risk analysis and corresponding risk management plan, which are the cornerstones of the HIPAA Security Rule." OCR initiated its investigation on April 17, 2014, after receiving notification that CHCS had experienced a breach of PHI involving the theft of a CHCS-issued employee iPhone. The iPhone was unencrypted and was not password protected. The information on the iPhone was extensive, and included social security numbers, information regarding diagnosis and treatment, medical procedures, names of family members and legal guardians, and medication information. At the time of the incident, CHCS had no policies addressing the removal of mobile devices containing PHI from its facility or what to do in the event of a security incident; OCR also determined that CHCS had no risk analysis or risk management plan.

- "Mobile devices in the health care sector remain particularly vulnerable to theft and loss. Failure to implement mobile device security by Covered Entities and Business Associates puts individuals' sensitive health information at risk. This disregard for security can result in a serious breach, which affects each individual whose information is left unprotected." (Roger Severino, OCR Director, at https://www.hhs.gov/about/news/2017/04/24/2-5million-settlement-shows-not-understanding-hipaa-requirements-createsrisk.html)
- Number of persons affected x \$10,000 to \$50,000 = Penalties



- HIPAA security requirements include:
 - Unique user identification (e.g., passwords)
 - Emergency access
 - Automatic logoff or autolock
 - Encryption

(45 CFR 164.312)



Mobile Device Security

ire https://www.health	it.gov/providers-professionals/	your-mobile-device-and-h	ealth-information-privacy	r-and-security	
	Blog	g Federal Advisory Committe	ees (FACAs) Contact Get	Email Updates <u>ର</u> 📘 불	s 🖬 🕵
				in Partnership with t	he rning C onsortium
Health	.gov				
		Newsroom - FAQs N	Multimedia Implementation Re	esources	Q
Providers & Pi	ofessionals Patie	ents & Families 🕞 📃	Policy Researche	rs & Implementers	

Privacy & Security

Your Mobile Device and Health Information Privacy and Security



Physicians, health care providers and other health care professionals are using smartphones, laptops and tablets in their work. The U.S. Department of Health and Human Services has gathered these tips and information to help you protect and secure health information patients



Additional HIPAA Considerations





Business Associates

- May need business associate agreement ("BAA") with vendor who "creates, receives, maintains, or transmits" PHI on behalf of the provider.
 - Includes cloud service providers and other vendors who host PHI on their servers.
 - May include IT vendors who access PHI to perform their functions.
 - Does not include conduits, i.e., entities that to not store and do not regularly access the PHI.
- BAA must contain required terms.

(45 CFR 164.314 and 164.504(e))



Failure to Implement BAA

aa/for-professionals/compliance-enforcement/agreements/ccdh/index.html

No Business Associate Agreement? \$31K Mistake – April 20, 2017

The Center for Children's Digestive Health (CCDH) has paid the U.S. Department of Health and Human Services (HHS) \$31,000 to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule and agreed to implement a corrective action plan. CCDH is a small, for-profit health care provider with a pediatric subspecialty practice that operates its practice in seven clinic locations in Illinois.

In August 2015, the HHS Office for Civil Rights (OCR) initiated a compliance review of the Center for Children's Digestive Health (CCDH) following an initiation of an investigation of a business associate, FileFax, Inc., which stored records containing protected health information (PHI) for CCDH. While CCDH began disclosing PHI to Filefax in 2003, neither party could produce a signed Business Associate Agreement (BAA) prior to Oct. 12, 2015.

0

Liability for BA Conduct: Failure to Implement BAA



 BA had access to CE's database of 290,000 persons

En

North Memorial Health Care has agreed to settle charges that it potentially violated the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules by failing to implement a business associate agreement with a major contractor and failing to institute an organization-wide risk analysis to address risks and vulnerabilities to its patient information. North Memorial is a comprehensive, not-for-profit health care system in Minnesota that serves the Twin Cities and surrounding communities. The settlement includes a monetary payment of \$1,550,000 and a robust corrective action plan.

Patient Access

• As a general rule, you must allow patients to access PHI in "designated record set", i.e.,

"(i) The medical records and billing records about individuals maintained by or for a covered health care provider; [and]

"(iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals."

(45 CFR 164.501 and .524)

- May apply to texts and e-mails.
- No HIPAA obligation to retain the e-mails for specified period of time, but...
 - Medicare rules may require retention for specific time, e.g., hospitals must maintain records for 5 years.
 - State law may require retention for specific time.



Reporting Breaches of Unsecured PHI

- Business associate must report breach of unsecured PHI to covered entity within 60 days.
 - BAA should require shorter time.
- Covered entity must report breach of unsecured PHI to individuals, HHS and, in some cases, local media.
 - Individuals: ASAP but no more than 60 days after discovery.
 - Beware situations in which knowledge is imputed to CE
 - HHS: depends on number of persons involved-
 - ≥500: immediately
 - < 500: no later than 60 days after end of calendar year
 - Media: No more than 60 days after discovery.

(45 CFR 164.400 et seq.)



Reporting Breaches of Unsecured PHI

The "acquisition, access, use, or disclosure of PHI in a manner not permitted under [the Privacy Rule] is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

"(i) The nature and extent of the [PHI] involved, including the types of identifiers and the likelihood of re-identification;

"(ii) The unauthorized person who used the [PHI] or to whom the disclosure was made;

"(iii) Whether the [PHI] was actually acquired or viewed; and

"(iv) The extent to which the risk to the [PHI] has been mitigated." (45 CFR 164.402(2)) HOLLAND&HART.

Reporting Breaches of Unsecure PHI

"What is a covered entity's obligation under the Breach Notification Rule if it transmits an individual's PHI to a third party designated by the individual in an access request, and the entity discovers the information was breached in transit?

"If a covered entity discovers that the PHI was breached in transit to the designated third party, and the PHI was "unsecured PHI"..., the covered entity generally is obligated to notify the individual and HHS of the breach and otherwise comply with the HIPAA Breach Notification Rule

"However, if the individual requested that the covered entity transmit the PHI in an unsecure manner (e.g., unencrypted), and, after being warned of the security risks to the PHI associated with the unsecure transmission, maintained her preference to have the PHI sent in that manner, the covered entity is not responsible for a disclosure of PHI while in transmission to the designated third party, including any breach notification obligations that would otherwise be required."

(OCR Guidance on Patient's Access, available at <u>https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html</u>)



Reporting Breaches of Unsecured PHI

- Remember: failure to report breach → "willful neglect" → \$10,000 to \$50,000 per person affected.
- For example:

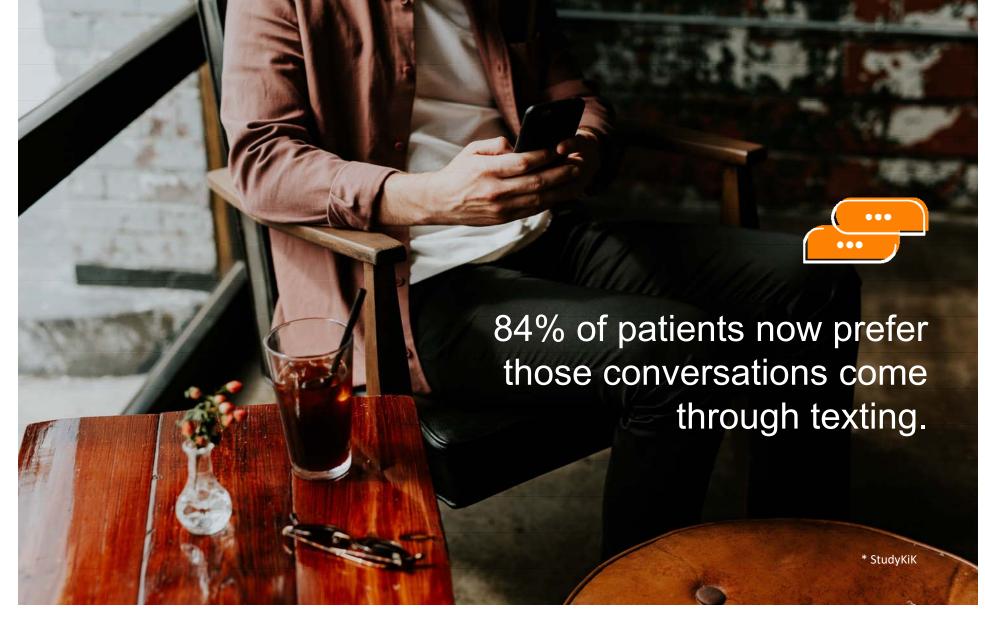
"A covered entity's employee lost an unencrypted laptop that contained unsecured protected health information. HHS's investigation reveals the covered entity feared its reputation would be harmed if information about the incident became public and, therefore, decided not to provide notification as required by § 164.400 et seq." (75 FR 40879)





Texting Technology 101







But... what is texting?



Texting could be....

- SMS
- MMS
- Social Media
 - Facebook
 - Twitter
 - WhatsApp
 - etc.
- In App (portal, etc.)



To explain how to implement texting in HIPAA-compliant manner, let's dive into the two texting categories.

What is secure texting?

What is insecure texting?



To benefit from texting with patients without violating HIPAA, you'll need to find a vendor with a robust HIPAA solution.



Consider these elements:

- Does the vendor meet the HIPAA requirements for business associates?
- Does the vendor solution differentiate between minor and adult patients?
- Does the vendor keep permanent, uneditable records of every text sent and received?



Consider these elements:

- Does the vendor store ePHI in a HIPAA-compliant secure infrastructure? Cloud based?
- Does the vendor provide an end-to-end encrypted channel?
 - Does the vendor provide an unencrypted channel?



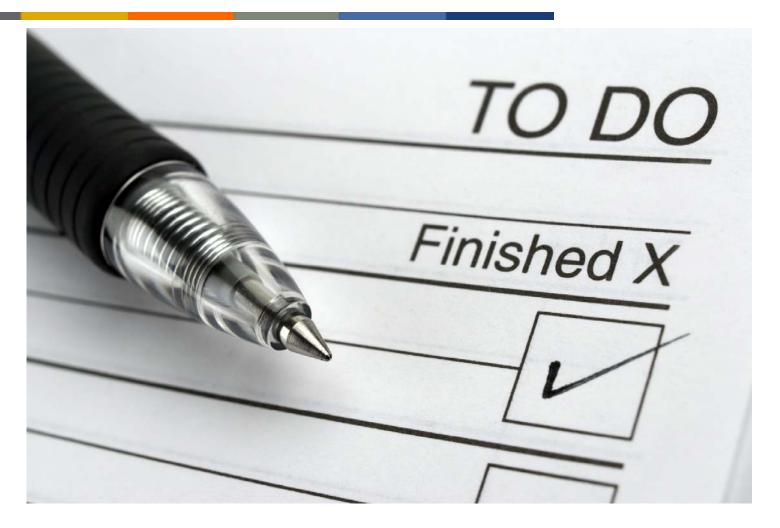
In short, make sure a vendor has built the HIPAA protections into their software.







Action Items





- ✓ Address texting and e-mails in your HIPAA risk assessment.
 - IT platform
 - Mobile devices
 - Others
- ✓ Implement security rule requirements
 - Secure e-mail or messaging apps
 - Encryption
 - Unique user name and password
 - Remote wipes

 Execute business associate agreement ("BAA") with vendor if necessary.



- Review and update policies re texting and e-mail, e.g.,
 - May text without PHI
 - Type of PHI that may be communicated via text
 - Use of encryption or other secure, approved safeguards
 - Confirm recipient before sending
 - Review texts before sending
 - Limit to minimum necessary PHI



✓ Review and update policies re texting, e.g.,

- Assume others nearby may read the text
- Do not let others use device
- Immediate notice of lost mobile device
- Guidance and process for inputting appropriate information into medical record
 - Which texts or e-mails should be input
 - Who may input the texts or e-mails
 - Authorization



✓ Beware "bring your own device (BYOD)" policies

- Address privacy and security issues.
- Coordinate policies with HIPAA requirements, including patient access and record retention.
- Train or educate members of workforce, medical staff, business associates, and others as appropriate.



✓ Look for compliant solutions, e.g.,

- Protect against unauthorized access
- Encrypt texts and e-mails
- Secure attachments
- Recipient must sign in with password to view PHI
- Limited address book
- Remote text deletion
- Notification when text is delivered/read
- Retain records for 5 years
- Protect against unauthorized deletions or modification



Additional Resources





www.hhs.gov/ocr/privacy/

IIPAA for Professionals ×				_	٥	×
$\epsilon \rightarrow c$	Secure https://www.hhs.gov/hipaa/for-professiona	ls/index.html			☆ *	:
	HHS.gov	U.S. Department of Health & Human Services	5			
	Health Information Privac					
	I'm looking for	HHS A-Z Index				
	HIPAA for Individuals	Filing a Complaint HIPAA for Professionals Newsroom				
	HHS > HIPAA Home > HIPAA for Professiona	ls				
	HIPAA for Professionals	Text Resize 🗛 🗛 🛛 Print 喜 Share 🛐 😏 🔸				
	Privacy +	HIPAA for Professionals				
	Security +	To improve the efficiency and effectiveness of the health care system, the <u>Health Insurance Portability</u> and <u>Accountability Act of 1996 (HIPAA)</u> , Public Law 104-191, included Administrative Simplification				
	Breach Notification +	provisions that required HHS to adopt national standards for electronic health care transactions and code sets, unique health identifiers, and security. At the same time, Congress recognized that				
	Compliance & Enforcement +	advances in electronic technology could erode the privacy of health information. Consequently, Congress incorporated into HIPAA provisions that mandated the adoption of Federal privacy protections for individually identifiable health information.				
	Special Topics +	• HHS published a final Privacy Pule in December 2000, which was later modified in August 2002				
	🤅 🧿 📜 💲 🖬 💁 🛞		~ Ÿ) ঢ় <	») 9:22 ») 8/28	2 PM 3/2017

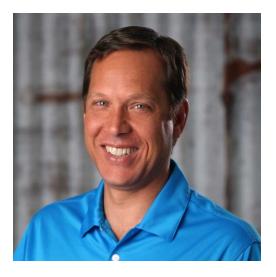
https://www.hollandhart.com/healthcare#overview





Questions

Bo Ferger bo@rhinogram.com (423) 800-7644



Kim C. Stanger <u>kcstanger@hollandhart.com</u> (208) 383-3913



