As Good As Being There?

- Family Practice MD providing “mental health” services & treating “pain management issues”
- Developed health problems limiting mobility
- Began seeing new patients remotely
- Employed RN traveled to patient’s location
- Physician communicated with patients using Skype
- Physician felt Skype a “suitable communication system”
- Oklahoma Health Care Authority disagreed
- Placed on probation for 2 years plus education courses

Knittle A. Oklahoma doctor disciplined for using Skype to treat patients. NEWS OK
Touch Screen Medicine

- Patient admitted to hospital for cardiac surgery
- On admission patients/family provided with iPad
  - Special patient communication application (myCare)
  - Provided a “personalized Plan of Stay”
  - Allowed following of course with linked education modules
  - Patients reported progress during recovery including levels of pain, food intake, and mobility by “bi-directional interaction” with physicians and hospital
- Survey after discharge: 90% satisfaction
- Mt. Sinai satisfaction 95% (4.75 on 5 scale)

Communication Problems

- Arch Internal Medicine
- Plaintiff depositions
- Malpractice cases
- Patient and families
- Cited problems of communications and resultant problem relations

Communication Problems

- Arch Internal Medicine
- Plaintiff depositions
- Malpractice cases
- Patient and families
- Cited problems of communications and resultant problem relations
- Hospital Sentinel Events (Joint Commission)


The Prime Factor

- For Medical Malpractice Claims
  - Patient insurance status?
  - Physician specialty?
  - Breach in the standard of care rendered?
  - Judicial climate and density of attorneys?
  - **Inadequate or bad communications**!
- Initiating factor for other potential liabilities
- Increasing importance of understanding and responding to rapidly changing medical methods of communication
- Some methods by choice.........and some required!
Changing Communications

• Publication June 23, 2011
• “A new generation of physicians is embracing mobile technology…and they are far more likely to use mobile technology in clinical settings…”
• “Physicians are adopting mobile technology at a very high rate; this transcends practice settings and years of practice.”
• “Access to EMR data tops the physician wish-list…”
• The study: “…44% of physicians who do not yet have a mobile device intend to purchase one in 2011, indicating [use] will continue to grow very rapidly this year”

The Rapid Rise

• By May 2014

[Bar chart showing the use of devices: Tablets 54%, Smartphones 85%, Computers 99%]

The Patient Position

- Desire of patients to use electronic communication

On Line Medical Advice: 81%
MD Communication: 90%

MD & Patient Communications

- Hospital information systems (HISs)
- Clinical decision support systems (CDSSs) & Applications
- Picture Archiving & Communication Systems (PACSs)
- Laboratory information systems (LISs)
- Internet & video
- Text (SMS) & Multimedia Message Service (MMS)
- E-mail
- Electronic Medical Records (EMRs)
- Electronic Health Records (EHRs)
The EMR & EHR Systems

- Institute of Medicine (IOM) Report
- Issued in 2003
- Key functions for safety, quality, and care efficiency that EMRs should support
  - Physician access to patient information, such as diagnoses, allergies, lab results, and medications.
  - Access to new and past test results among providers in multiple care settings.
  - Computerized provider order entry.
  - Computerized decision-support systems to prevent drug interactions and improve compliance with best practices.
  - Secure electronic communication among providers and patients.

Electronic Medical Records (EMR)

- HHS announcement May 22, 2013
- More than 50% of Eligible Professionals (EPs) have adopted the use of EMR

![Chart showing adoption of EMR from 2008 to 2014]
The Incentive Program

- American Recovery & Reinvestment Act 2009 (ARRA)
- Source of HITECH Act
- Called for “…incentive payments to Eligible Professionals (EP)” and hospitals “…that adopt and successfully demonstrate meaningful use of certified electronic health record (EHR) technology.”
- Final Rule (276 p) adopted July 28, 2010
- Required criteria, amount of payments, & Medicare payment “adjustments” for “failing to demonstrate meaningful use of certified EHR technology”

The Incentive Program

- “To receive an EHR incentive payment, providers have to show that they are meaningfully using their EHRs by meeting thresholds for a number of objectives. The EHR Incentive Programs are phased in three stages with increasing requirements.”
- Eligible Professionals (EP) on a calendar year
- EPs “…attest to demonstrating meaningful use every year to receive an incentive and avoid a Medicare payment adjustment.”
- Attestation during a “reporting period” e.g. 90 days in 2014.
The Incentive Program

- Also July 28, 2010 Final Rule (In force August 27, 2010)
- Adopted “initial set of standards, implementation specifications, and certification criteria, and to more closely align …with final meaningful use Stage 1 objectives and measures.”
- Adopted “…certification criteria…”
- Purpose of establishing the required capabilities and specifying the “…related standards and implementation specifications…” that Certified Electronic Health Record Technology (CEHRT) needed to support Meaningful Use Stage 1.


New Patient Communications

- Incentive program started in 2011 with MU Stage 1 and 2011 Edition Certified Electronic Health Record Technology (CEHRT) requirements
- MU Stage 2 was effective first in 2014 (Delayed "reporting period" 90 days for MU 2 in 2014)
- Full one year reporting period for 2015.
- MU Stage 1
  – 15 Core objectives
  – 5 Menu objectives from 10
- MU Stage 2
  – 17 Core objectives
  – 3 Menu objectives from 6
**Required Patient Communications**

- Two Core objective **requirements** in MU Stage 1
- “Protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities”
  - **Measure**: “Conduct ...a security risk analysis...and implement security updates as necessary and correct identified security deficiencies...”
- **Provide patients with an electronic copy of their health information, upon request**
  - **Measure**: “More than 50% of all unique patients of the EP... who request an electronic copy of their health information are provided it within 3 business days”

**New Required Patient Communications**

- Two requirements changed for MU Stage 2
- **Change of MU Stage 1 on providing electronic copies to:**
  - “Provide **patients the ability** to view online, download and transmit their health information within four business days of the information being available to the EP”
  - There **must** be ability of the patient “…to view online, download and transmit their health information [by] **more than 5 percent of patients seen** by the EP or admitted to an inpatient or emergency department of an eligible hospital or CAH [and to] view, download, or transmit to a third party their health information.”
New Required Patient Communications

• New additional objective requirement not found in MU Stage 1
  – #17: "Use secure electronic messaging to communicate with patients on relevant health information"
  – "Required that a secure message must be sent using the electronic messaging function of Certified EHR Technology by more than 5 percent of unique patients seen by an EP during the EHR reporting period"

• Accomplished by….

What Position?

• Medical office search service,
  – "We are searching for a full time Patient Portal Assistant in the Health Information Management department. This position will assist patients in accessing and using our patient portal in both inpatient and outpatient settings. The Patient Portal Assistant will ensure that we meet our Meaningful Use goals for portal access by explaining the portal to patients, helping with password issues, creating materials to encourage the use of the portals and explain the process, and meeting one on one and in groups with patients.”

The Patient Portal

- “A patient portal is a secure online website that gives patients convenient 24-hour access to personal health information from anywhere with an Internet connection.” (HHS)
- Government movement through MU for “patient engagement”
- Portal by design “… to facilitate secure, private communication and provide convenience to patients who wish to access their medical records online.”
- Usually developed by an EMR vendor used by the medical organization

Basic Portal Coverage

- By authentication methods (usernames and passwords) allows patient access to protected health information (PHI),
  - Recent doctor visits, discharge summaries, medications, immunizations, Lab results
  - Exchange secure e-mail with the medical office
  - Request prescription refills
  - Schedule non-urgent appointments
  - Check benefits and coverage
  - Update contact information
  - Make payments
  - Download and complete forms
  - View educational materials
Patient Portal Advice

• Reasons to develop
• Regulation required functions through the Certified EMR System
  – Patient viewing of EMR
  – Patient downloading of EMR information
  – Patient transmitting of EMR information
  – Patient messaging

• Patient Use and Physician Interest
  – 40% of patients unaware of medical office portal
  – 90% of patients desired online contact
  – 9% of physicians using portal for patient follow up

Patient Portal Advice

• Develop a good patient portal to assist in meeting the new required communications
• Comprehensive communications strategy
  – Consider the specific patient population
  – Keep a consistent practice message
• Patient surveys
• Security by multiple authentication levels and strong passwords
• Patient and staff education
• Ref: Gilbert M. How to Use a Patient Portal
Liabilities of Non Compliance

- CMS November 4, 2014: “...more than $25 billion in incentive payments have been made through Sept. 30 [2014].”
- “The Government Accountability Office (GAO) has warned that the Meaningful Use program may be at greater risk than other programs of making inappropriate payments...”
- HHS Office of Inspector (OIG) “...blasts CMS for not verifying the accuracy of providers' attestation information both before and after paying the incentive, leaving the program "vulnerable."
- CMS tracking by Medicare Meaningful Use Compliance Audits & payment “Adjustments”

Meaningful Use “Adjustments”

- Eligible Professionals (EPs) receiving incentives must show adherence to Meaningful Use (MU), i.e. “attestation” to adherence
- Using an active
  - “National Provider Identifier (NPI)” and
  - “…a National Plan and Provider Enumeration System (NPPES) web user account…”
- EPs attest to “…meaningful use every year to receive an incentive [$] and avoid a Medicare payment adjustment.”

Meaningful Use “Adjustments”

- In 2015…. if no EMR or
- If “….EP does not successfully demonstrate meaningful use of certified EHR technology”
  - “…the EP’s Medicare physician fee schedule amount for covered professional services will be subject to a payment adjustment.”
  - 2015 reduce 1%
  - 2016 reduce 2%
  - 2017 reduce 3%
  - Continue to 5% if fewer than 75% of EPs are in MU
- Avoided by adhering to (attesting to) MU

“Adjustment” Exceptions

- EPs who never demonstrated MU prior to 2014 must have demonstrated MU during a continuous 90 day period before October 1, 2014
- Two year exemption for those new to the practice of medicine
- Providers who practice in multiple locations but do not control the availability of certified EHR technology in all locations
- Extreme circumstances outside the provider’s control, e.g. practice closure or natural disaster
- Providers who have insufficient access to the internet or who are non-hospital based anesthesiologists, radiologists or pathologists
Meaningful Use Audits

- Audits of whether or not attestations of use are accurate.
- Estimated in 2015 to be 80,000 random audits
- Some not random and due to “red flags”
  - Exclusions inconsistent with other data
  - EHR systems known for problems
  - Combining scores, e.g. changing EHR systems
  - Attestation data inconsistent CNS supplemental data
- **Result:** Failure of one element = return of all incentives for the year and another audit until correct

---

Audit Advice

- Assurance of system certifications to 2014 Edition Certified Electronic Health Record Technology (CEHRT)
- Attestations “book of evidence” (documentation) & backup 6 years
- Test the truth of certified EHR representative claims by ensuring claims are consistent with the source of truth, i.e. CMS literature and/or the relevant Federal Rule.
- Be careful of patient mix, i.e. % of Medicare patients
- Assign MU to a team and/or individual with “audit committee” in place
- Prepare before getting the letter
Another MU Danger

- Chief Financial Officer of a Texas hospital
- Over a 4 month period filed attestations of MU which were inaccurate with collection of over $785,000
- Attestations were done under a different name
- EHRs were present, but primary reliance on paper records
- Directed EHR vendor to input data
- Minimal use of EHR though attestation to meaningful use done under regulations
- Physician hospital owner also involved


Another MU Danger

- The CMS warning
- “It is a crime to defraud the Federal Government and its programs. Punishment may involve imprisonment, significant fines, or both. In some states, providers and health care organizations may lose their licenses. Convictions also may result in exclusion from Medicare participation for a specified length of time. Medicare fraud may also result in civil liability.”
- An application….
Another MU Danger

- On basis of employee complaints DOJ filed action
- CFO was indicted for fraud and identity theft
- Alleged making “…false attestation for fiscal 2012 that [hospital] was a ‘meaningful user’ of electronic health records…”
- “Knowingly and willingly made materially false, fictitious and fraudulent statements and representations, and made and used false writings and documents” to defraud the EHR incentive program
- CFO indicted and received
- The MD convicted receiving 40+ years sentence

Website Communication

- “A patient portal is a secure online website that gives patients convenient 24-hour access to personal health information from anywhere with an Internet connection.” (HHS)
- Broader Internet use
- Survey
  – Physician professional use 67%
  – Physician networking 48%
- In one study 60% of physicians felt that use of the Internet “…improved the quality of patient care they delivered.”
The Website

- Internal Medicine specialist
- Established a practice website
- Not associated with the limited EHR system
- Site contained practice information
- Also contained section for patient questions
- Questions received were reviewed
- Answers to the questions were posted on the site using only patient’s initials
- Problem?

The Privacy Concern

- “…portal is a secure online website…” for privacy and security of patient medical information (HHS)
- The concern of Required protection of health information stored or transmitted under HIPAA & related rules
- Individually identifiable health information that is:
  - (1) Created or received by a health care provider, health plan, employer, or health care clearing house,
  - (2) Relates to the past, present, or future physical or mental health or condition of an 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; and
  - (i) That identifies the individual or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual
The Privacy Concern

- Individually identifiable health information
- **Protected Health Information** (PHI)
  - “...Individually identifiable health information that is:
    - (i) Transmitted by electronic media;
    - (ii) Maintained in electronic media; or
    - (iii) Transmitted or maintained in any other form or medium.”
  - Not considered protected information in
    - Education records (1)(i) or
    - Employment records (1)(iii)
- The PHI is the information that must be **secure** from exposure or “**breach**”

HHS OCR HIPAA Administrative Simplification Regulation Text §160.103 Definitions Site hhs.gov.

---

The Privacy Concern

- “**Breach**” means the acquisition, access, use, or disclosure of protected health information in a manner...which compromises the security or privacy of the protected health information.”
- Section of regulations concerning breach contains a section:
  - “Notification in the Case of Breach of Unsecured Protected Health Information”...
- “**Unsecured protected health information**” means protected health information that is **not rendered unusable, unreadable, or indecipherable** to unauthorized persons through the use of a technology or methodology specified by the Secretary…”

HHS OCR HIPAA Administrative Simplification Regulation Text §160.103 Definitions Site hhs.gov.
The Privacy Concern

- April 2009 HHS issued information “guidance” on how to render PHI “unusable, unreadable, or indecipherable”
- Electronic information (data states)
  - At rest - Encryption
  - In motion - Encryption
  - In use - Encryption
  - Disposed - Destruction
- Guidance documents from NIST on each
- “Encryption is an easy method for making lost information unusable, unreadable and indiscernible” Dir OCR

Patient Website Advice

- Advance organization of content and keep current
- Avoid any direct patient comment or advice
- Disclosures that could influence patients’ understanding or use of the information, products or services offered on the website
- Website information “truthful, not misleading, accurate, concise, and easy to understand”
- Reference educational materials and literature
- Use clear identification and contact information
- Assign site responsibility & monitoring
- Do not identify patients or use PHI
  - Study of blog information allowed 17% patient ID
Is It Patient Information?

- Individually identifiable health information (IIHI)
- Protected Health Information (PHI)
  - “Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.”
- How is it identified?
- By any one of the following:
  - Name
  - Geographic subdivisions e.g. zip codes

Department Health & Human Services Office for Civil Rights. HIPAA Administrative Simplification Regulation Text §164.304 Definitions. Site hhs.gov

Is It Patient Information?

- Dates:
  - Any related date, e.g. DOB, Admission date
- Numbers:
  - Telephone numbers
  - Fax numbers
  - SS numbers
  - Medical record numbers
  - Health Plan numbers
  - Account numbers
  - License/certificate numbers
  - Internet Protocol (IP)
  - Vehicle identifiers
  - Email addresses
  - Web URLs
  - Device identifiers /Serial
  - Biometric identifiers
  - Full face photo or comp
  - Any unique code, number, or characteristic
- CE “…does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.”

Department Health & Human Services Office for Civil Rights. HIPAA Administrative Simplification Regulation Text §164.304 Definitions. Site hhs.gov
Physicians & Internet Social Media

- Professional Social Media use

<table>
<thead>
<tr>
<th></th>
<th>MD Social Media</th>
<th>Patient Desire Social Media</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online Social Network (OSN)</td>
<td>42%</td>
<td>56%</td>
</tr>
<tr>
<td>Patient Portals</td>
<td>15%</td>
<td>67%</td>
</tr>
</tbody>
</table>


The Request

- Internal Medicine physician
- Maintains a practice website and a practice Facebook site
- Facebook information includes practice activities, etc
- A patient who has been seen in the medical office sends a “Friend” request to the physician
- The physician has no other contact outside of the physician-patient relationship
- The request is accepted.
- Problem?

McMahon M. Professionalism in the Use of Social Media. AMA CEJA Report 8-4-10. Site: www.themedicalbag.com
Online Social Networks (OSN)

- Physicians in practice survey
  - Received patient “Friend” requests 35% (rejected 58%)
  - Accessed for patient or patient family members 16%
  - Use would have improved patient interactions 49%
  - Security concerns 80%

- Conclusion
  - Contacts generally initiated by patients
  - OSN interaction with patients is an ethical problem?
  - Patient interaction not ethically acceptable either socially or professionally 68%


Online Social Networks (OSN)

- “The boundary that exists in the patient-physician relationship is something to consider when physicians take part in social networks and post content online…boundary is the defining characteristic of the professional relationship, in which respect, trust, and the patient’s well-being are paramount.” (AMA Council on Ethical & Judicial Affairs)

- Online “friendships” outside the physician patient relationship are “problematic” frequently leading to loss of respect and disagreement

- Opening of personal information….no way back

Social Media Site Advice

- The Social Media Page, e.g. Facebook (as websites)
  - Do not try to answer individual patients or diagnosis
  - Direct information collectively to patients
  - Post only on professional matters
  - Do not post patient photos, recordings, or any patient identifiable information without written authorization
    - If necessary best done on web pages
- General Social Media
  - Establish a practice SM policy for any involvement
  - Use separate personal and professional SM sites

The Consultation

- Internal Medicine physician received a night call from a current patient
- Patient related a problem
- MD entered into a Skype conversation in which the patient described the problems and demonstrated an arm problem
- The problem was discussed
- The MD advised the patient on activity and called a prescription to a local pharmacy
- Problem became worse and patient very unhappy
- Potential problem? (earlier case)
Video Patient Communication (iATV)

- Use of Interactive tele-video (I ATV) for patients
- “…online chat services such as Skype allow doctors to meet with patients in a quick and convenient capacity”
- Physician use of cameras & web platforms is “absolutely increasing”
- A good thing in patient communications?
  - Well known company (MS)
  - Available
  - Easy to use
  - Free
- However…..

Skype-like messaging systems
- “…does not meet Health Insurance Portability and Accountability Act (HIPAA) standards for web-based security, meaning privileged health conversations on Skype between physicians and patients are vulnerable to hackers”
- For most “…similar free web-based communication platforms relying on proprietary voice over Internet technology”
  - Audit Trail:
    - “Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.”

More Patients Meeting With Doctors Via Web Programs Such as Skype. News Archive.
See Four Reasons to Think Twice About Using Skype for Telehealth.

Akpan N. Oklahoma Doctor Reprimanded for Prescribing Narcotics via Skype. Medical Daily.
Department Health & Human Services Office for Civil Rights. HIPAA Administrative Simplification Regulation Text Site hhs.gov.
The Video Advice

- Products and technology are not “HIPAA compliant”
- Physicians or other Covered Entities (CEs) are compliant or not…
  - Based on the capabilities of the product and use of the product, e.g. Skype, etc.
- Always aim for compliance
- Inadvisable
  - *Healthcare providers not using encryption is “simply imprudent”*. Dir OCR
- Also applies to ignoring obvious potential liabilities
- Applies to other types of patient e-transmissions…

Lost in Transit

- Dermatologist attending professional meeting
- Meeting in a different hotel
- Used cab transportation
- MD left smartphone in the cab
- No adequate phone security measures
- Cab driver attempted to return phone
- Attempting to locate owner information was able to read PHI in patient text messages on phone
- PHI breach
- Security of SMS or texting & **messaging systems**
MD Use of Text Messaging

- Use of text messaging
  - 57% Specialty MDs
  - 73% All MDs

- Preferred for
  - Efficiency
  - Speed
  - Response
  - Multi-media

Using the SMS

- Short Message Service [SMS or texting] “messaging is inherently non-secure and noncompliant with safety and privacy regulations under the Health Information Portability and Accountability Act (HIPAA).”
- Joint Commission 2011 for “orders”
  - “is not acceptable for physicians or licensed independent practitioners to text orders for patients to the hospital or other healthcare setting.”
- No recipient authentication
- No record retention
Texting and EMR

- Communications containing PHI are part of the medical record, e.g. letters, phone calls, etc.
- Text messaging is also part of the medical record
- Retention in the record
  - Documentation for care and defense
  - Requirements of regulations: retention (designated record set for PHI “Used, in whole or in part, by or for the covered entity to make decisions about individuals”)
  - Availability for patient access (portals or otherwise)
- Patients have a right to request change to the medical record by amendment
  - Request through portal or office

Cepelewicz B. Text Messaging With Patients: Steps Physician Must Take to Avoid Liability. Medical Economics.

The OCR Position

- Investigation by OCR
- Correction Action Plan (CAP) for Cardiology practice
  - “Covered Entity’s risk management plan must implement security measures sufficient to reduce risks and vulnerabilities to ePHI to a reasonable and appropriate level for ePHI in text messages that are transmitted to or from or stored on a portable device.”
  - Practice must have “…technical security measures to guard against unauthorized access to ePHI transmitted over an electronic communications network [and] that includes text messaging of ePHI.”
- Civil Money Penalty (CMP): $100,000

Messaging Advice

- Determine if messaging use will be allowed
- Policies that consider,
  - What ("registered") mobile devices will be used, protection, & encryption (complete mobile device use policy)
  - Obtain patient consent (or not) and detail e.g. #s, type of content, etc. (documented)
  - Authentication process (who received?)
  - Retain messages for medical record
  - Data center storage & Audit controls (auditing, monitoring, & accessibility)
  - Business Associate Agreements

Received Without Request

- Internal Medicine specialist treats patient over 1 year
- Patient is currently on medications
- MD receives a standard SMS text message from the patient with attached photograph of skin area
- Patient describes complaint in message
- Requests information from the physician on treatment and continued use of medication
- Information now on MDs smartphone as well as servers
- Does MD have a HIPAA potential liability?
Messaging Advice

• Physician use
  – For non urgent information
  – Use only approved systems (by policy) not std. SMS
  – Retain or delete messages by defined protocols
  – Check telephone numbers and update
    • Survey: 38% of text PHI to the wrong person
  – Send minimal information (even within TPH)
  – Clear mobile device before disposal
  – Use clear messaging without shorthand
  – Content may be used in malpractice litigation

• The other major messaging use

The Patient Email Preferences

<table>
<thead>
<tr>
<th></th>
<th>Telephone</th>
<th>Email</th>
<th>Txt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appointment Reminders</td>
<td>59%</td>
<td>29%</td>
<td></td>
</tr>
<tr>
<td>Between Visit Care</td>
<td>45%</td>
<td>49%</td>
<td></td>
</tr>
<tr>
<td>Education</td>
<td>28%</td>
<td>68%</td>
<td></td>
</tr>
<tr>
<td>Seasonal Notices</td>
<td>37%</td>
<td>55%</td>
<td></td>
</tr>
<tr>
<td>Recall Information</td>
<td>45%</td>
<td>50%</td>
<td></td>
</tr>
</tbody>
</table>

PHI and use of Email

• As other e-communications PHI is protected by the HIPAA regulations (Security Rule)
• Wide use and wide potential liabilities
• Protection by making PHI in Email “secure” using encryption (National Institute of Standards & Technology (NIST) standards) affording protection against breach
• When directed to patients unsecured Email is allowed
  – “…notify the individual that there may be some level of risk that the information in the email could be read by a third party.”
  – No responsibility during transmission or afterward
  – Document notification

PHI and use of Email

• Caution about Email requests for provision of PHI
• Patient requests for PHI to be sent to 3rd parties
  – Allowed under regulations
  – Requires “reasonable policies” to identify person requesting PHI to be sent
  – Request must be “made in writing”
  – Clear identity of 3rd party recipient
  – Clear description of “where to send” the PHI copy
  – Policies to assure correct entry of provided Email address…not a correct address
The Decision: Talk or Text or....?

- More categories of communication
- Simpler methods in 20th century, e.g. face to face & telephone or paper records & mail
- Expanded to include smartphone video & conferencing or EHR, SMS, MMS, Email, & portals
- **Synchronous** vs. asynchronous
  - Confirmation of receipt
  - Positive ID of those in discussion
  - Immediate questions and responses
  - Additional non verbal communication

Talk or Text Advice

- Delays, e.g. time and place
- Interruptions
- Distractions
- Information change with transfer
- **Recommendations**
  - **Use synchronous**
    - Urgent or emergent situations
    - Immediate response or clarifications needed
    - Complicated explanations are needed
    - When patient care improved by both or synchronous
    - Need for visualizing patient perceptions

---

Horwitz L. et al. Physician Communications in the 21st Century: To Talk or To Text. JAMA.
Talk or Text Advice

– Use asynchronous
  • Routine non urgent
  • Alerts and notifications
  • “Durable” conversation or documentation is needed
  • Information timelines are needed
  • Information distribution is needed
  • When MD time is limited
  • When involved information is limited
– Consider combining both when situations allow
– One method usually not appropriate for all situations

General e-Communications Advice

• Have policies, procedures, & tracking methods in place for use of all types of e-communications being used
• Workforce training on those in use including privacy & security issues and events of breach
• Do the periodic "risk analysis". Regulation required
• Require security measures on all mobile devices
• Assure medical record entry of all PHI messaging
• Use only secured messaging
• Assure all vendor e-communication programs have documented capabilities for HIPAA & state law

Horwitz L. et al. Physician Communications in the 21st Century. To Talk or To Text. JAMA.
Summary

- Increasing prevalence of electronic communications required by government and desired by patients
- Necessity of understanding the methods of use
- Understanding the associated regulatory requirements e.g. HIPAA and state
- “…facilitate the physician-patient relationship [and] they can also … may lessen the quality of the [patient] interactions”
- Selecting those appropriate for type of practice and patients
- Whatever method(s) used ….policies and procedures in place including staff training for every method used
- Periodic review and updating as technology and practice needs change