Electronic Communication in Medical Practice

Version 130401

A Guide for Practitioners

Reproduction and online availability provided by

COPIC

Better Medicine • Better Lives

Contents

Foreword

Communication is good.
Technology is good.
Electronic communication should offer important value to medical practitioners.

But, electronic connectivity comes at a price. Clinicians who take advantage of electronic media to help them better manage medical information find themselves devoting considerable time, thought and money to investigating, critiquing, purchasing, configuring, installing, securing, maintaining, training, updating, supporting, revising, repairing, uninstalling, recycling, and otherwise managing the complex systems required.

All this comes with a dense learning agenda that can rival any other educational activity. The overhead in knowledge acquisition can be daunting, and has already demonstrated that it can distract significantly from other critical practice-related agendas.

COPIC has provided this collection of resources to assist the medical community in learning and thinking about electronic communications technology for the benefit of our patients and in the interest of safe and effective medical practice. We welcome feedback, suggestions and questions.

Michael S. Victoroff, MD
mvictoroff@copic.com
720-858-6130

Dr. Victoroff is a Risk Management Consultant at COPIC, where most of his efforts are focused on liability aspects of electronic health information systems, including health records, communication devices and decision support systems. He created COPIC's Taxonomy for classifying occurrences and claims, and provides evidence-based data for many of COPIC's research and teaching activities.

Dr. Victoroff is also Chief Medical Officer at Lynxcare, which provides health record analysis and Certified Health Record Summaries for patients with complex conditions; and Chief Medical Officer at Amara Health Analytics, which specializes in natural language processing for science and healthcare. He has 30 years of experience in medical informatics. In 1989, he developed ChartR®, an electronic medical record system, and sold it commercially for 8 years. He is an Associate Clinical Professor at the University of Colorado School of Medicine and a member of ASTM Subcommittee E31 on Healthcare Informatics. He is a graduate of St. John's College (Annapolis) and Baylor College of Medicine. He did his residency in Family Practice at the University of Rochester and a Robert Wood Johnson Foundation fellowship in Biomedical Ethics. He practiced family medicine and obstetrics in Colorado for 19 years and was named "Colorado Family Physician of the Year" in 1996. He has been a Medical Director for Aetna and a private investigator for Clinical Toxicology, Ltd. He has published numerous articles on bioethics, medical informatics, managed care, medical errors and patient safety.

A note about commercial products. It is impossible to discuss current technology without referring to some dominant vendors and products by name, such as Microsoft®, Windows®, Apple®, Google®, etc. It would be disingenuous and confusing to refer to such products generically. Neither COPIC nor Dr. Victoroff have commercial relationships with any technology vendor discussed in this presentation; and they do not endorse any product mentioned as being superior to any competitor, or as meeting the needs of any specific practitioner. Where products or vendors are named, it is because their brands are either ubiquitous in the healthcare environment, helpful for an understanding of the general material, or representative of classes of products with which the audience should be familiar.

This guide was developed by Michael S. Victoroff, MD to support information provided during presentations made regarding risks associated with electronic communication in health care practices.

The content is provided for informational purposes only and does not guarantee compliance with Federal or state laws; nor does it represent legal advice. This information is not intended to be exhaustive or definitive regarding electronic communications technology, privacy or security, and may not be applicable to all health care providers and settings. Rapidly evolving standards and circumstances may make some content out-of-date or inaccurate. Readers are encouraged to seek expert advice when evaluating the applicability of this information to their own situations.

Reproduction and online availability provided by

COPIC
Better Medicine • Better Lives

www.callcopic.com

Colorado: 7351 E. Lowry Blvd., Denver, CO 80230 | p: 800.421.1834 or 720.858.6000 | f: 720.858.6001

Nebraska: 233 South 13th St., Ste. 1200, Lincoln, NE 68508 | p: 800.421.1834 or 402.438.7600 | f: 877.263.6665

Liability Risks Of Health Information Technology

- Malpractice, cyber liability, general liability, property & casualty, defamation, privacy (HIPAA), Directors and & Officers, employment practices, product liability, practice continuity (revenue loss), etc.
- Only malpractice is covered by professional liability insurance

COPIC Cyber-Liability Coverage

- Upon policy renewal after 1/1/2013, COPIC provides coverage for:
    - **Multimedia liability –** *Coverage for online and offline media; including copyright/ trademark infringement, libel/slander, advertising, plagiarism and personal injury*
    - **Security and privacy liability –** *Coverage for third party claims alleging a financial loss as a result of a network security or privacy breach; including both online and offline information, virus attacks, denial of service and failure to prevent transmission of malicious code*
    - **Privacy regulatory defense and penalties –** *Coverage for defense costs and fines/penalties for violations of privacy regulations, including but not limited to HIPAA and the new Hi-Tech Act*
    - **Breach response and notification expenses, patient support and credit monitoring –** *All reasonable legal, public relations, advertising, IT forensic, credit monitoring and postage expenses incurred for a privacy breach response*
    - **Network asset protection –** *Reasonable and necessary expenses and costs required to recover and/or replace data that is compromised, damaged, lost, erased or corrupted; including business interruption and income loss as a result of the interruption of the insured's computer system*
    - **Cyber extortion and terrorism –** *Extortion expenses and extortion monies as a direct result of a credible cyber extortion threat; income loss and expense due to interruption of the computer system directly caused by an act of terrorism*
- Annual aggregate limits
    - Individual – $100,000
    - Group – (1): $100,000; (2-10): 200,000; (11-20): 300,000; (21+): 500,000

Report an EHR-Related Event

- COPIC insured: Report occurrences involving Information Technology to a COPIC Risk Management Nurse in the same fashion as any other potential adverse event
- Non-COPIC Insured: If you are comfortable sharing information and want to contribute to the study of medical error, please report actual or potential adverse events to Dr. Victoroff.
    - *Be aware that reports shared with anyone except your attorney or certain protected organizations are potentially discoverable in legal proceedings!*
- Software, hardware or system malfunction, usability problem, patient injury, potentially hazardous condition
    - mvictoroff@copic.com
    - 720-858-6130

Communication Channels

- **Traditional:** Standard mail, standard e-mail, webmail, patient chart (paper, EHR), wireless networks & devices, phone, fax, pager (including cell)
- **Newer:** Secure e-mail, text messaging, smartphone, tablet, telepresence (audio, video), portals (patient, professional), Virtual Private Networks (VPNs), patient controlled health records (PHRs)
- **HIPAA:** The Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information (PHI)." [45 C.F.R. §160.103]

Risk Analysis

- www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidance.html
- HIPAA requires practices to "conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the **confidentiality, integrity and availability** of electronic protected health information held by the [organization]."
- Other important elements of risk analysis include possession, authenticity, non-repudiation, utility, etc.
- Threats
  - Threats are things that can damage an asset.
  - Human error, hardware failure, natural disaster, data corruption, loss, theft, diversion, bugs, upgrades, patches, malware (viruses, worms, Trojans), interception, interruption, power failure, software malfunction, misuse, poor design, etc.
  - Disproportionate attention has been given to privacy breach, because of the serious attention this is receiving at the Federal level.
  - Each practice must evaluate its particular threats, which may be unique.

NIST and OCR

- The National Institute of Standards & Technology has a wealth of information available for download about security and the risk auditing process.
  - http://csrc.nist.gov/
- The Office of the National Coordinator for Health Information Technology does, too.
  - www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf

eRisk Considerations for Online Communication

- See Appendix A: Medical eRisk Considerations for Online Communication, p. 19
- Use the most secure medium consistent with the need
- Know your correspondent

- Establish clear ground rules
    - Obtain consent
- Transmit minimum necessary PHI
- Retain documentation
- Don't expose PHI on social media
    - Including "professional" websites
- Be professional
- Keep your devices secure and well maintained

Telemedicine Definitions

- **COPIC:** "The provision of clinical medicine whereby health care information is transferred via telephone, Internet or other networks for the purpose of consulting and sometimes performing remote medical procedures or examinations." [PLI 1/1/13]
- **Colorado Medical Practice Act:** "The delivery of medical services and any diagnosis, consultation, or treatment using interactive audio, interactive video, or interactive data communication." [12-36-102.5]
- **Nebraska Telehealth Act:** "The use of telecommunications technology by a health care practitioner to deliver health care services within his or her scope of practice at a site other than the site where the patient is located; any contact between a patient and a health care practitioner relating to the health care diagnosis or treatment of such patient through telehealth but does not include a telephone conversation, electronic mail message, or facsimile transmission between a health care practitioner and a patient or a consultation between two health care practitioners. [71-8503]
- **Medicare/Medicaid:** "… multimedia communications equipment that includes, at a minimum, audio and video equipment permitting two-way, real-time interactive communication between the patient and distant site physician or practitioner. Telephones, facsimile machines, and electronic mail systems do not meet the definition of an interactive telecommunications system." [42 C.F.R. 410.78]

Technologies

Phone, Fax and Pager

- These legacy technologies are not governed under the rules for "electronic storage or transmission" of Protected Health Information under the HIPAA Security Rule
    - Exception: If a computer (e.g., fax server or fax software) is used to store or process it
- However, they *are* governed by the HIPAA Privacy Rule
- EHRs should be thought of as communications devices; however, this presentation is not intended to discuss the myriad legal and technical hazards associated with EHRs
- This discussion is focused particularly upon these hazards:
    - **Security/Confidentiality:** Passwords, protection of data at rest, remote access technologies
    - **Accuracy/Integrity:** Auto-populated fields
    - **Usability/Availability:** Difficulty in recognizing important information due to "data camouflage"

Remote Access

- Using a remote computer for anything that can be done on your local computer
  - Mobile computing
  - Technical support
- Typically very secure: Can use one-time passwords
  - Drawback: Requires a PC always on & connected
- **Vendors:** MS Remote Desktop, Apple Remote Desktop, GoToMyPC, LogMeIn, Cisco
- **Search Terms:** remote access, remote desktop

Virtual Desktop

- Secure and powerful
- Typically needs technical support for initial setup, configuration
- **Search terms:** VPN, virtualization, virtual desktop

Smartphones

- Ubiquitous
- Useful, powerful
  - Web, text, GPS, apps, voice, e-mail, voicemail, remote access to other systems
- Risky
  - Loss, theft, breach
  - Misdirection, dysfunction, failure, distraction
  - Lost availability, power, connectivity
  - Content may not get into the medical record
- CDMA (Verizon, Sprint)
  - Dominates in much of U.S.
- GSM (AT&T, T-Mobile)
  - Lots of U.S. (only choice in Europe)
- Secure for voice and data
- Digital signal, encrypted, multi-frequency channel hopping, etc.
- Can be tapped at the service provider level
- Phones may also use Wi-Fi
  - Totally different technology, benefits, risks
  - Security varies from extremely secure to extremely insecure

Identity Management (Validation, Verification, Authorization)

- **Access management**
  - Something you **KNOW**: Password, PIN, mother's maiden name, airspeed of swallow
  - Something you **HAVE**: Key, ID card, flash drive, chip, decoder ring
  - Something you **ARE**: Fingerprint, retina, iris, voice, face, DNA

    - Something you **DO**: Signature, keystroke-timing, gait
    - Some**WHERE** you are: GPS, terminal ID
- Two-factor authentication typically involves a password plus one other method

Passwords

- Passwords alone (single-factor authentication), no matter how complex, do not provide strong protection
    - Almost any password can be cracked, hacked, guessed, discovered or bypassed
- **Weak passwords:** password, passw0rd, 0000, asdf, 123456,Fluffy, superman, 3035551212, ashley, 030682, qwerty, abc123, monkey, letmein, trustno1, dragon, baseball, 111111, iloveyou, master, football, princess, rockyou, michael
- **Strong passwords:** Longer than 10 characters. "MaryHadaLittleLamb" is stronger than 4%6Td$7. "MHALLIFWWASAETMWTLWSTG" (first letters of each word in the song) is much stronger.
- **Tricks** for generating passwords
    - **tbatsTdgagttW** ("Twas brillig, and the slithy toves did gyre and gimbal in the wabe"). Mnemonic: Carroll
    - **4s&7yaoFbfotCanN** ("Four score and seven years ago, our fathers brought forth on this continent a new nation"). Mnemonic: Address
    - **0scysbtDeL** ("Oh, say can you see, by the dawn's early light"). Mnemonic: Key
    - **(2b)r(-2b)=Q** ("To be, or not to be, that is the question"). Mnemonic: Danish
- **Mnemonics:** Don't be obvious
- **Rotation:** Your application may require you to have a system to generate a different password every 90 days. Many systems will not allow you to repeat a password among your last 24
- **Password vault:** Software applications that keep passwords in a file – protected by a password
- **Password generators:** Commercial applications that automatically generate difficult passwords according to your specifications
    - Pass phrase: A longer string of characters that you readily remember *("Gallia est omnis divisa in partes tres, quarum unam incolunt Belgae, aliam Aquitani, tertiam qui ipsorum lingua Celtae, nostra Galli appellantur.")*
    - Don't use the Lord's Prayer, Pledge of Allegiance, etc.
    - QWERTY substitution (a=! e=@ i=# o=$ u=% y=^ so, monkey = m$nk@^)
    - The "dyslexic E" (numeral 3)
    - Capitalized nouns (or adjectives, etc.)
    - Deliberate mizzpelling
    - Symbol substitution: and=&, for=4, l=1, i=!, o=Ø
- **Security questions:** Many organizations ask for "answers only you would know" to common questions.
    - Mother's maiden name
    - Your first car
    - Your favorite color

Many of these answers are available in public records (not to mention Facebook). **So LIE!**

  - Mother's maiden name: Oldsmobile
  - Your first car: Pomegranate
  - Your favorite color: Chicago

- **Vendors:** 1Password, Apple (OS), Firefox, Kaspersky, Keepass, Lastpass, Microsoft (OS), Norton, Password Vault, RoboForm, SafePass, Sxipper
- **Search terms:** password manager, password vault, password generator
- Many ways to verify identity: Iris, PIN, face, voice, glyph, token, retina, password, fingerprint, etc. You simply have to use *something*.

Provisioning and De-provisioning

- **Collect:** Company provided phone/PDA, keys, ID badge/card, parking pass, credit card, phone card, discount card, tokens for printer, copier, scanner, prescription pads
- **Review/inspect/wipe:** Personal phone/PDA, office PC, laptop, personal PC, laptop, tablet, smartphone
- **Deactivate:** Passwords, e-mail, credentials, remote access software, internal privileges (website editing, financial systems), external privileges (banking, ordering, e-Prescribing)
- **Edit:** Company directory, access control list, website, marketing materials, corporate documents, e-mail auto-reply, call schedule, emergency contacts, insurance coverage
- **Inventory:** PHI on personal devices, open/incomplete tasks
- **Notify:** Patients, business associates (lab, pharmacy), insurance carriers, accountant, payroll
- Similar process on termination, promotion, reassignment

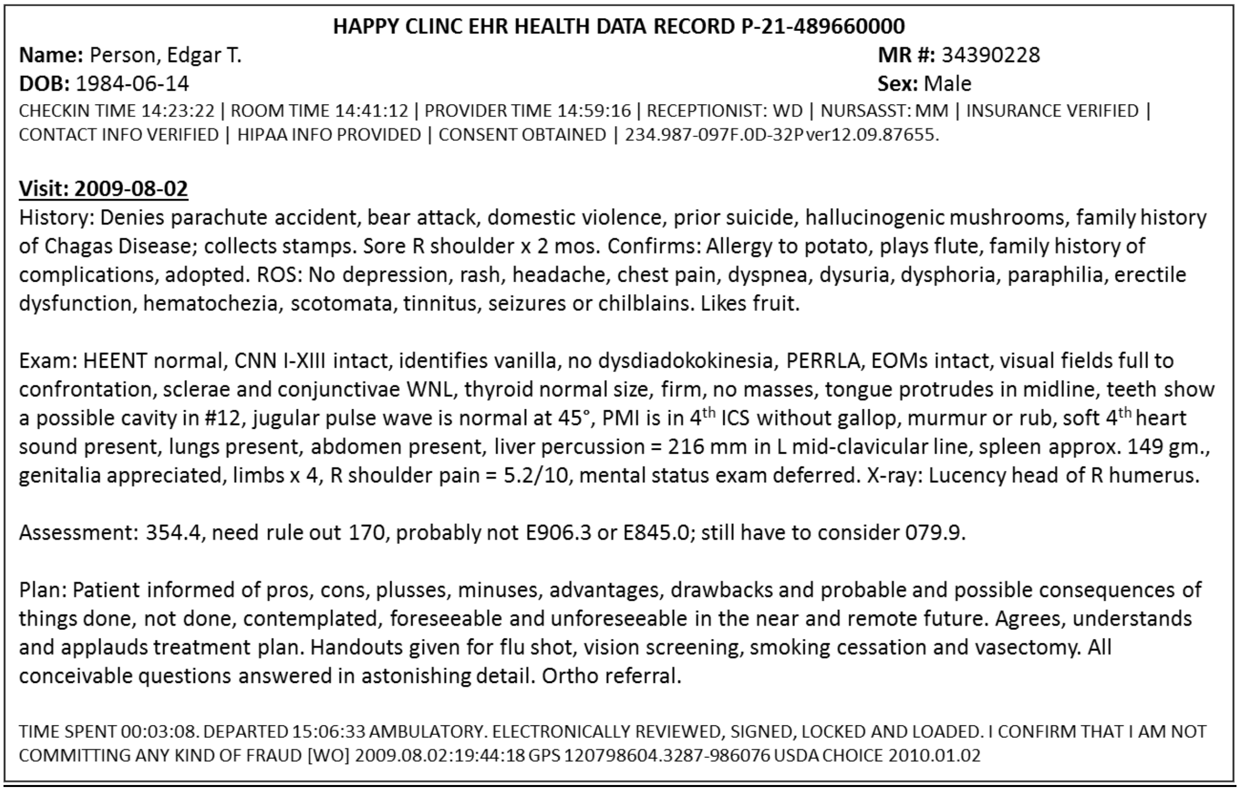
Protecting Data at Rest

- **Removable devices:** Backup media, tapes, DVDs, flash drives, CDs/DVDs, laptops, tablets, smartphones, obsolete/unused devices
- **Local devices** can be stolen, diverted: Local drives, servers, network storage (NAS), desktop PCs, printer/fax (sometimes store information)
- **Vendors:** BitDefender, CheckPoint, Credant, McAfee, Microsoft (Bitlocker), IronKey, Oracle, PKWare, Sophos, Symantec/PGP, Trend Micro, TrueCrypt, Trustwave, WinMagic
- **Search terms:** encryption vendors, data security, drive encryption, laptop security, smartphone security
- Remember secure **physical destruction** for discarded storage media (certificate of destruction)
- Destruction of data on hard drives can also be accomplished through **disk wiping software**.
  - Vendors: Knoll Ontrack, Disk Wipe, KillDisk, DBAN, Sourceforge

Documentation vs. Communication

- Do not confuse a good medical record with a useful legal document
- Primary function of the record is communication
- "High-Fiber" records contain non-essential filler, and may camouflage important information

Documentation at the cost of communication



HAPPY CLINC EHR HEALTH DATA RECORD P-21-489660000

Name: Person, Edgar T. **MR #:** 34390228
DOB: 1984-06-14 **Sex:** Male
CHECKIN TIME 14:23:22 | ROOM TIME 14:41:12 | PROVIDER TIME 14:59:16 | RECEPTIONIST: WD | NURSASST: MM | INSURANCE VERIFIED | CONTACT INFO VERIFIED | HIPAA INFO PROVIDED | CONSENT OBTAINED | 234.987-097F.0D-32Pver12.09.87655.

Visit: 2009-08-02
History: Denies parachute accident, bear attack, domestic violence, prior suicide, hallucinogenic mushrooms, family history of Chagas Disease; collects stamps. Sore R shoulder x 2 mos. Confirms: Allergy to potato, plays flute, family history of complications, adopted. ROS: No depression, rash, headache, chest pain, dyspnea, dysuria, dysphoria, paraphilia, erectile dysfunction, hematochezia, scotomata, tinnitus, seizures or chilblains. Likes fruit.

Exam: HEENT normal, CNN I-XIII intact, identifies vanilla, no dysdiadokokinesia, PERRLA, EOMs intact, visual fields full to confrontation, sclerae and conjunctivae WNL, thyroid normal size, firm, no masses, tongue protrudes in midline, teeth show a possible cavity in #12, jugular pulse wave is normal at 45°, PMI is in 4th ICS without gallop, murmur or rub, soft 4th heart sound present, lungs present, abdomen present, liver percussion = 216 mm in L mid-clavicular line, spleen approx. 149 gm., genitalia appreciated, limbs x 4, R shoulder pain = 5.2/10, mental status exam deferred. X-ray: Lucency head of R humerus.

Assessment: 354.4, need rule out 170, probably not E906.3 or E845.0; still have to consider 079.9.

Plan: Patient informed of pros, cons, plusses, minuses, advantages, drawbacks and probable and possible consequences of things done, not done, contemplated, foreseeable and unforeseeable in the near and remote future. Agrees, understands and applauds treatment plan. Handouts given for flu shot, vision screening, smoking cessation and vasectomy. All conceivable questions answered in astonishing detail. Ortho referral.

TIME SPENT 00:03:08. DEPARTED 15:06:33 AMBULATORY. ELECTRONICALLY REVIEWED, SIGNED, LOCKED AND LOADED. I CONFIRM THAT I AM NOT COMMITTING ANY KIND OF FRAUD [WO] 2009.08.02:19:44:18 GPS 120798604.3287-986076 USDA CHOICE 2010.01.02

Medical Identity Theft

- Criminals can impersonate a physician to prescribe meds or submit fraudulent charges
- Criminals can impersonate a patient to receive medical services
- Underground market for stolen identities
  - Windows or Apple password hacker – costs $50
  - Wireless network sniffer/cracker – costs $50
  - Password “recovery” software for most applications – costs $100-500
  - A full identity that can be used to obtain a bank account – yields $200
  - A hacker expects to steal thousands of identities

Securing a Wi-Fi Network

- 50% have no encryption – are you kidding?
- WEP encryption – bad
- WPA/WPA2 encryption – good
- Change the router’s default username & password
  - Default address, username and passwords for popular routers are all well known
- Turn off ID broadcast
- Consider MAC address filtering

- Strong firewall & antivirus
- Strong password
- Open networks (Starbucks, airports, etc.) are very dangerous
- Hacking into a network, discovering a WEP key (weak encryption), decrypting the passwords and taking over all computers on the network is a beginner's exercise
- Wireless networks throughout the world are easily discoverable

Text Messaging

- PRO
  - No training
  - Fast, reliable
  - Asynchronous
  - Can be forwarded *
  - Multiple recipients
  - Universal connectivity
  - Ubiquitous, handy, portable
  - More effective than "pages"
  - Users already have the device
  - Timestamp & audit trail possible
  - Threading (permits reply on subject)
  - Secure in transit (modestly encrypted)
- CON
  - Wrong numbers!
  - No receipt verification *
  - Cannot show escalations
  - Device may not be secure *
  - Can't incorporate into EHR *
  - Device may not be available
  - Cannot default to next on-call
  - Cannot ensure priority delivery
  - Only works over cellular networks
  - Can't integrate with staff directory *
  - Vulnerable to phishing and spoofing
  - Messages may persist after deletion
  - Selective forwarding may not be available
  - Content is threaded by recipient, not subject
  - Can't separate professional messages from friends/family
  - No priority ring tones or repeat notifications for critical messages *

* Added functionality available with add-on apps; but not with off-the-shelf device.

- Secure TM vendors
  - CoreText, IQMax, Medigram, qliqsoft, TigerText, TrustText
- Joint Commission
  - www.jointcommission.org/standards_information/jcfaqdetails.aspx?StandardsFaqId=401&ProgramId=1
  - *"It is not acceptable for physicians or licensed independent practitioners to text orders for patients to the hospital or other healthcare setting. This method provides no ability to verify the identity of the person sending the text and there is no way to keep the original message as validation of what is entered into the medical record."*

Mobile Computing

- Wi-Fi defenses
  - Strong firewall

  - Turn off file sharing
  - Block incoming traffic
  - Use SSL-enabled e-mail
  - Use HTTPS enabled web sites
  - Turn off Wi-Fi adapter when not using it
  - Don’t keep anything important on your device
  - Create a secure partition
  - Consider a password manager
  - Cloud passwords
  - One-time passwords
  - VPN
- Lost Laptop/Phone Defense
  - **Laptop:** Locate, alert, lock, wipe
  - **Phone:** Same, plus call your carrier to deactivate
  - **Vendors:** Lo-Jack, Lookout, many others
  - **Search Terms:** laptop theft protection, laptop recovery, laptop security, cell phone security, cell phone recovery

Cloud Computing

- Hosted server
- Many vendors (e.g., Amazon, Google, Microsoft, Verizon)
- Pro:
  - Powerful, flexible, secure
  - All sensitive data is on a “server farm”
  - Multiple users, strong security, backup is provided by the service
- Con:
  - Needs internet access to connect
  - Downtime, other availability risks
  - Large services are hacker targets

Social Media

- Sermo, LinkedIn, Facebook, Twitter, etc. are not private! You’re on national TV
- Blurring the relational context invites boundary violations
- **Advertising:** Consumer protection laws may hold you to fulfill promises you publish
- **Socializing:** Consider what you want patients, employees, colleagues to know about your personal life – and *never* expose confidential medical information, even obliquely
- **Sharing photographs:** Serious privacy breaches (or personal embarrassment) created by thoughtless use

The HIPAA Privacy Standard vs. Meaningful Use Standard

- Encryption is not “required.” It is “addressable.”
    - “Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.”
    - [45 CFR 164.312 (e)(2)(ii)]
- MU Stage 2 Objective
    - “Use secure electronic messaging to communicate with patients on relevant health information.”
    - [Federal Register / Vol. 77, No 45 / Wednesday, March 7, 2012 p. 13843]
- A breach is typically investigated after the fact
    - If your risk analysis is found to be inadequate, you could be in violation.
    - “Addressable” does not mean “optional”
    - Is it “appropriate?”
- **Bottom line:** We’re all going to be using messaging

Use Cases for Electronic Messaging

- Standard E-mail (POP)
    - Post Office Protocol (e.g., typical Outlook mail – someone@something.com)
    - Not encrypted
    - But may be reasonable if patient understands risks
- Secure E-mail
    - E.g., Microsoft Exchange Server, Google Apps for Business
    - Easy, transparent once set up, secure (encrypted) if *both parties* on same server
    - Attachments are encrypted, too
    - Can also be accomplished by exchanging a Digital Certificate (see below)
- Webmail (e.g., Hotmail.com, Yahoo.com)
    - Typically free or low cost
    - Not encrypted or secure
    - Attractive target for hackers
- Web access to a secure mail server
    - E.g., Microsoft Web Access (OWA)
    - Different from “Webmail” (above)
    - Can be as secure as the server
    - Guard the password
- Encrypted attachments
    - E.g., Adobe PDF encrypted with a password, MS Word also.
    - Can go by any route, even unsecure, because attachment is encrypted
    - Have to figure out how to get the password to the recipient

- Secure mail delivery system
  - Many vendors and services (e.g., Zixmail, Proofpoint, ReachMyDoctor, Voltage)
  - Used by many large providers, Universities, etc.
  - Highly secure
  - Can be initiated by either party, once it's set up
  - Needs registration process
- Texting
  - On phone, normally uses the cell phone channel
  - Some forms of "Instant Messaging" may use Wi-Fi
  - Security is comparable to phone (digitized at each end, but not encrypted at the vendor)
  - Purged regularly, but there is a period of discoverability

Secure Portals

- Patient or professional
- Need registration
  - Identity verification
- Tightly siloed
  - All users must be "internal" (registered)
  - No cross-registration (federation) among different systems
- User account maintenance
  - Password validation, rotation, recovery, inactivation
  - Support, updates
- When one individual has to manage multiple accounts, it gets burdensome

Technical Tips

Setting Up Secure E-mail

- Messages entirely inside an organization's firewall
  - All users have trusted identities and credentials within the same organization, e.g., a group practice all sharing the same @thispractice.com address
  - Use a secure mail server (e.g., MS Exchange)
- Message that cross the firewall
  - Some users are outside the organization but identities are trusted, e.g., colleagues, patients, business associates
  - All parties have exchanged digital certificates from a Certificate Authority, OR
  - All parties registered on a common, secure web portal, OR
  - All parties subscribe to a common, secure e-mail service, OR
  - One party initiates a secure e-mail transaction and others reply using that service, OR
  - All PHI is contained in encrypted attachments (this requires a password to be exchanged)
- Vendors: 4securemail, Comodo, Cyphersend, DataMotion, Edgewave, Hushmail, McAfee, ReachMyDoctor, Proofpoint, S-mail, Verisign, Voltage, Zixmail.

Setting Up Encrypted E-mail in MS Outlook

Microsoft Outlook makes it possible to exchange encrypted e-mail (using PKI technology) with trusted correspondents. Setting this up is a bit technical. But, once it's set up, you don't have to do any maintenance as long as you maintain your Digital Signature and your trusted correspondents maintain theirs.

Your first steps

A. Obtain a "Digital Signature Certificate"
   1. Choose a Certificate Authority (a trusted issuer of certificates: Symantec/VeriSign, Thawte, PGP, others)
   2. Decide which E-mail account you're going to use
      a) You can own multiple Certificates, but can only use one per E-mail account
      b) The Certificate is permanently "bound" to that E-mail identity

B. Fill out the registration form
   1. You will need to choose a "passphrase"
      a) Keep it secure – it's the proof that you own this Certificate
   2. Pay a fee, if required
   3. Receive an E-mail verification from the Certificate Authority
   4. Respond to the E-mail to validate your E-mail address (you may be given a link to click)

C. Install your Certificate in Outlook. The process is a little different for each version of Outlook.
   1. The Certificate Authority will transmit the Certificate to you electronically (a dialog box may pop up on your screen)
   2. You can choose some security options
   3. In Outlook 2010:
      a) Go to File | Options | Trust Center | Trust Center Settings
      b) Follow the prompts
   4. You can install the Certificate on multiple computers, tablets, etc. by repeating this process

D. Send a message, *signed but not encrypted,* with your Certificate to your trusted correspondent
   1. You will see a "seal" on the right-hand corner, indicating the message is signed by a trusted identity.

Your correspondent's steps

A. Obtain their own Digital Certificate
   1. May be from any Certificate Authority

B. Install it in their own Outlook

C. Open your signed (but not encrypted) initial message from their Inbox

D. Add your identity (this E-mail account) to their Outlook Contacts
   1. Right-click on your name in the "From" field and follow the menu
   2. If you are already in the Contact list, go through the process of "Add as Contact" again (this will update your entry with your Certificate)

E. Using your trusted E-mail from Outlook Contacts, your correspondent needs to send you a signed or encrypted message
    1. If the message is encrypted, there will be a padlock at the right-hand corner
    2. If the message is signed, there will be a seal at the right-hand corner

Your final step

A. You receive your correspondent's message

B. Note that it has a symbol in the right-hand corner (padlock or seal)

C. Add the correspondent who sent it (in the "From" field) to your Outlook Contacts
    1. Right-click on the name and follow the menu
    2. *Do this even if the person is already in your Contact list*. It will update their entry with the certified identity for that E-mail address

D. From now on, your messages to each other will be encrypted and/or signed as you wish
    1. Outlook automatically encrypts messages and attachments to this person when you send them
    2. Outlook automatically decrypts messages and attachments from this person when you receive them

Large File Transfer

- Typical E-mail attachments are limited to 2-10 MB; but, medical records can be BIG: 10-100 MB (not counting images)
    - Compression (with/without encryption)
        - Vendors: PKZip, WinZip
    - File Transfer Protocol (SFTP)
        - Set up your own FTP server (separate from mail server)
        - Upload to an FTP service on the web. You can encrypt before sending, or the service can encrypt. Recipient gets e-mail: "You have a file to download."
        - Vendors: YouSendIt, DropBox, Microsoft SharePoint, Microsoft SkyDrive

Appendix A: Medical eRisk Considerations for Online Communication

The following Medical eRisk Considerations were developed by the iHealth Alliance and are provided for informational purposes only.

The use of Electronic Health Records (EHRs) and online services is increasingly common in everyday physician practice. The unique concerns and risks inherent in this form of communication have prompted the development of the "Medical eRisk Considerations." The Medical eRisk ("Electronic Risk") Considerations were initially created in 2000 by the eRisk Working Group for Healthcare, a consortium including professional liability carriers, medical societies, and state licensing boards.

These Considerations are meant to serve as general suggestions and do not serve as professional advice of any kind. Clinicians are advised and encouraged to conduct their own independent research and seek further guidance on any specific questions or issues related to the subject matter herein from independent professionals. Full or partial adherence with any of these considerations imposes no obligation on any of the members of the eRisk Working Group, the iHealth Alliance or any other person or entity to offer any benefits of any kind to Clinicians such as lowering premiums, provide coverage of any claims, or offer any other benefits.

The Medical eRisk Considerations stress the following critical factors:

- Maintain patient confidentiality, privacy, security and authentication. Know and follow state and federal laws regarding patient privacy.
- Obtain informed consent for online services; privacy protocols; and privacy rights. Prevention of unauthorized computer access.
- Limit online communications to existing patients.
- Discourage use of online communications for medical emergencies. Understand social media liability risks.
- Understand state licensing jurisdiction regarding online communication outside your state. Understand your responsibility for educational materials provided online to your patient.
- Document all online patient communications in the medical record – even "deleted" information is discoverable. Manage your fee-based consultations – charging can raise expectations re quality and thoroughness.
- You are responsible for the information shared with patients on your practice Web site – is it accurate and current? Verify on-line pharmacies through the Verified Internet Pharmacy Practice Sites program: http://www.nabp.net/programs/accreditation/vipps/
- Use extra caution when using online services to diagnose and treat new conditions.
- **Personal Health Records:** Patient responsibility for content and for informing you of important changes.

EHR Liability Risks

- You are responsible for patient medical information to which you have reasonable access – from whatever source. Know the source of your e-Prescribing Drug Information and Clinical Decision Support – ensure they comply with your specialty standards and have the full updated FDA approved labels and alerts.
- EHR patient questionnaires may use automated algorithms that record issues requiring your follow-up.
- Use caution when overriding or disabling alerts, warnings, reminders and embedded practice guidelines – "Alert Fatigue."
- Use caution in copying and pasting patient notes – avoid incorrect information in your EHR. Auto-populated fields may lead to incorrect patient information being recorded in the EHR.
- All your interactions with the EHR are time/date tracked and discoverable. Read your EHR contract carefully, particularly regarding liability.
- Don't allow the computer to become a barrier between you and your patients.

The Medical eRisk Considerations were initially developed by the eRisk Working Group for Healthcare, a consortium of professional liability carriers, medical societies and state licensure board representatives. They are meant to provide information to healthcare providers related to the use of electronic clinical systems, including Electronic Health Records (EHRs), and online communication and services with patients.

These Considerations are meant to serve as general suggestions and do not serve as professional advice of any kind. Clinicians are advised and encouraged to conduct their own independent research and seek further guidance on any specific questions or issues related to the subject matter herein from independent professionals. Full or partial adherence with any of these considerations imposes no obligation on any of the members of the eRisk Working Group, the iHealth Alliance or any other person or entity to offer any benefits of any kind to Clinicians such as lowering premiums, provide coverage of any claims, or offer any other benefits.

General Principles

The legal rules, ethical guidelines and professional etiquette that govern and guide traditional treatment and communications between the healthcare provider and patient are equally applicable to EHRs, email, Web sites, list serves, Personal Health Records (PHRs), social media and other electronic services and communications. However, this technology introduces special concerns and risks as follows:

1. **Confidentiality.** The healthcare clinician is responsible for protecting patient privacy and guarding against unauthorized access to and/or use of patient healthcare information. This responsibility extends to the use of network services that have an appropriate level of privacy and security as required under HIPAA. Following are key considerations:
    a. **Privacy and Security.** Online communications between healthcare clinicians and patients should be conducted over a secure network, with provisions for privacy and security,

including encryption, in accordance with HIPAA. Standard email services do not meet the requirements under HIPAA.

Note: With respect to email specifically, clinicians are encouraged to add a disclosure to the bottom of their standard, non-secure email service stating that "this email is not secure, and is not for use by patients or for healthcare purposes in general."

b. **Authentication.** Healthcare clinicians have responsibility for taking reasonable steps to authenticate the identity of correspondent(s) in electronic communication and to ensure that recipients of information are authorized to receive it. Authentication of the patient or an authorized patient proxy (i.e., parent of a minor, authorized family member, etc.) for patient-provider online communication including the delivery of patient data is important in order to ensure patient privacy and confidentiality. Clinicians are encouraged to follow these suggestions for patient authentication:

   i. Have a written patient authentication protocol for all practice personnel and require them to understand and adhere to it.

   ii. Establish minimum standards for patient authentication when a patient is new to a practice or not well known.

   iii. Keep an electronic or paper record of each patient authenticated for online communication or data exchange. The record should include the following:

      1. Name of the patient
      2. Date of authentication
      3. Name of practice staff authenticating the patient
      4. Means used to authenticate the patient

   iv. Providers should not offer, promote or encourage patients to participate in online healthcare services where patient authentication is not addressed.

2. **Unauthorized Access to Computers.** Unauthorized physical access to computers can compromise patient information. Practices should establish procedures to guard against unauthorized access to computers with technologies such as automatic log-out and password protection.

3. **Informed Consent.** Prior to the initiation of online communication between healthcare clinician and patient, informed consent should be obtained regarding the appropriate use and limitations of this form of communication. Clinicians should develop written protocols for online communications, such as avoiding emergency use, heightened consideration of use for sensitive medical topics, and setting expectations for response times. Clinicians should also exercise discretion when selecting patients for the use of online services to ensure that they are capable of electronic communication and will be compliant. These guidelines should be documented in the clinician's practice policy manuals.

4. **Pre-Existing Clinician-Patient Relationship.** Healthcare clinicians may increase their liability exposure by initiating a clinician-patient relationship online. Online communications of any kind are best suited for patients previously seen and evaluated in an office setting.

5. **Licensing Jurisdiction.** Online interactions between a healthcare clinician and a patient are subject to requirements of state licensure. Communications online with a patient, outside of the state in which the clinician holds a license, may subject the clinician to increased risk. For example, pathologists, radiologists and other clinicians interpreting specimens, slides or images sent through interstate commerce for a primary diagnosis that becomes part of the patient's medical record should have a license to practice medicine in the state in which the patient presents for diagnosis or where the specimen is taken or the image is made. Intra-specialty consultation generally does not require in-state licensure, provided the consultation is requested by a physician licensed within the state and is referenced in a report he or she issues. Physicians are advised to check with their state's medical board to determine their licensure requirements.

6. **Sensitive Subject Matter.** Clinicians should advise patients of the risks that information the patient may consider sensitive might be inadvertently accessed by someone not authorized to see it, such as information on mental health, substance abuse, reproductive history, sexually transmitted diseases, drug and alcohol problems, genetic disorders and HIV status.

   Some states have laws about special classes of health information, such as HIV or mental health. Clinicians should follow state law in obtaining approval from the patient to exchange those classes of information. Some states may prohibit electronic transfer of specific classes of information regardless of patient consent.

7. **Patient Education and Care Management.** Healthcare clinicians are responsible for the information that they make available to their patients online. Information that is provided to patients through PHRs, automated patient education programs, care management and other online services should come either directly from the healthcare clinician or from a recognized, credible and authoritative source.

8. **Emergency Subject Matter.** Clinicians should discourage use of online communication to address medical emergencies such as chest pain, shortness of breath, high fever, physical trauma or bleeding during pregnancy. Instruct patients to call the office or go to an emergency department for emergency issues. Physicians should consider including a disclaimer on Web pages and emails reminding patients that emergency subject matter is not appropriate for electronic communication.

9. **Medical Records.** A permanent record of online communications relevant to the ongoing medical care of the patient should be maintained as part of the patient's medical record, whether that record is paper or electronic. Accurate and thorough documentation is effective risk management.

   Providers and patients should be aware that email and online information, including PHRs and consultations, are not erased from a computer's hard drive when deleted and are discoverable in litigation. Therefore all communicated information should be accurate and professional.

Practice Web Site Considerations.

1. **Authoritative Information.** Healthcare clinicians are responsible for the information they make available to their patients online. Information that is provided on a medical practice Web site or provided to a patient via secure email or other online services should come either directly from the healthcare clinician or from a recognized and credible source.

2. **Commercial Information.** Web sites and online communications of an advertising, promotional or marketing nature may unrealistically raise patient expectations and subject clinicians to increased liability. Liability risks include implicit guarantees or implied warranty and potential violation of consumer protection laws designed to guard against deceptive business practices. This is particularly true when cosmetic procedures, off-label drug use, and non-FDA approved procedures are promoted.

3. **Links to Third Party Web Sites and Other Sources of Information.** Clinicians are encouraged to post a disclaimer page between their Web site and a link to any third party Web site/information that advises patients and other visitors that they are leaving the clinician practice Web site and that the clinician and the practice do not assume any responsibility for the content or the privacy of other Web sites linked to the practice Web site.

Online Clinical Consultations

An Online Clinical Consultation is a consultation between a clinician and a patient, similar to an office visit or a call that would be documented in the patient’s chart, but conducted online via a secure messaging service. The clinician has the same obligations for patient care and follow-up as in face-to-face, written and telephone consultations. An online consultation should be substantive and specific to the patient’s personal health status.

The following are additional considerations for fee-based online consultations:

1. **Informed Consent.** Prior to initiating an online consultation, the healthcare clinician should obtain the patient’s informed consent to participate in the consultation, including discussing appropriate expectations, disclaimers and any fees that may be imposed.

2. **Fee Disclosure.** Patients should be clearly informed about any charges that might be incurred and be made aware that charges may not be reimbursed by the patient’s health insurance.

3. **Identity Disclosure.** Clinical information that is provided to the patient during the course of an online consultation should come from, or be reviewed by, the consulting clinician whose identity should be made clear to the patient.

4. **Available Information.** Healthcare clinicians should state and document that the consultation is based only upon information made available by the patient to the clinician during or prior to the online consultation, including referring to the patient’s chart when appropriate and, therefore, may not be an adequate substitute for an office visit.

5. **Online Clinical Consultation vs. Online Diagnosis and Treatment.** Clinicians should distinguish between an online consultation related to a known pre-existing condition and the diagnosis and treatment of new conditions addressed for the first time online. The diagnosis and treatment of new conditions online may compromise patient safety and increase liability exposure. When a clinician declines to diagnose a new condition online, he or she should communicate the importance of immediate office follow-up to the patient and document this information in the patient's office medical record. When the patient presents at the office, the clinician should document the time lapse between deferring the online consultation and the patient's arrival in the office.

6. **Follow-Up Plans.** An online consultation should include an explicit follow-up plan, as clinically indicated, that is clearly communicated to the patient.

7. **Internet Pharmacies.** There are potential risks when patients are referred to online pharmacies. The National Association of Boards of Pharmacy has a Verified Internet Pharmacy Practice Sites (VIPPS) program (http://www.nabp.net/programs/accreditation/vipps/). Pharmacies in compliance with its standards show the VIPPS seal of approval on their home page.

Social Media Liability Risks

Social media (YouTube, Twitter, Facebook, MySpace, blogs, etc.) are used by physicians for physician-to-physician networking. However, these types of media are not appropriate for physician-patient communications, because they are too informal and lack an atmosphere of professionalism – making it easy to lapse into casual conversation and inadvertently cross the boundary between personal and professional relationships. The following recommendations are made regarding the use of social media:

1. Do not discuss individual patients, dispense medical advice, respond to clinical questions from patients or otherwise "practice medicine" on these sites. These types of media do not use HIPAA-compliant secure networks, and inadvertently disclosing a patient's health information will violate HIPAA.

2. Presume that anything you say or post is in the public domain, and remember that anything typed or e-mailed creates a permanent record that is subject to discovery.

3. Physician office practices should have written confidentiality and communication policies with employees that clearly forbid online disclosure or discussion of patient health information.

Personal Health Records

PHRs introduce potential risks. When clinicians offer a PHR service to their patients, the patients/caregivers should be required to accept a PHR Terms of Service Agreement, either online through the PHR service provided or in writing from the practice, which, at a minimum, should include the following:

1. The PHR service is distinct from the medical record maintained by the physician or healthcare provider. Entries in the PHR do not become part of the medical record unless and until they are

formally accepted for inclusion by the clinician. When information is imported from a PHR into the clinician's record, its origin should be documented.

2. It should be made clear to patients that physicians are not responsible for knowing the information contained within a PHR except when they have consulted it in association with a formal office visit or Online Clinical Consultation.

3. Patients are responsible for notifying their healthcare clinician(s) if they have a PHR.

4. The PHR is not a substitute for directly communicating the patient's medical information to his or her physician in a traditional format (in-person, by telephone, etc.). Patients should not assume that their Personal Health Record has ever been seen or reviewed by their clinician(s).

5. It is the patient's responsibility to notify their healthcare provider(s) when new information appears in their PHR – whether they personally update it or it is automatically updated by third parties (health plans and other insurers, pharmacies, laboratories, etc.).

6. The provider should make it clear that the responsibility for the accuracy of the information in the PHR remains with the patient or caregiver as the owner of the record.

7. Developing and maintaining a PHR on a clinician practice Web site requires that patients have a pre-existing relationship with that clinician.

8. Materials and information available through the PHR are for informational purposes only and are not a substitute for professional medical advice.

9. Patients/caregivers should agree that they will contact their clinician if they have any questions about their medical condition or if they need medical help.

10. Patients/caregivers should agree that if they need emergency medical help, they should immediately call 911, their local emergency number, their physician, or go to an emergency department.

11. Patients/caregivers should agree that their User ID and Password are their responsibility to protect from unauthorized access and use by third parties.

Electronic Health Record Liability Risks

The EHR has the potential to advance the practice of good medicine. However, when new technologies are adopted, there are always unanticipated consequences. Real and potential liability risks are beginning to be recognized, and it is important for physicians to become familiar with them.

1. Doctors are responsible for information to which they have reasonable access – and there may be increased access to e-health data from outside the practice that enters the practice EHR or Web site or is accessed from the practice EHR or Web site, i.e. hospital charts, consultants' reports, lab results

and radiology reports, community medication histories, etc. If patient injury results from a failure to access or utilize available patient information, the physician may be held liable.

2. **e-Prescribing** is being rapidly adopted, driven by federal financial incentives, and is currently used by approximately 25% of office practices. It works as follows:

    a. Most electronic prescriptions are transmitted via a Surescripts network (they have data on 200 million insureds) to all chain pharmacies, 60% of independent pharmacies and most insurance formularies.

    b. Most EHRs have an e-Prescribing module, and e-Prescribing is a required capability under the federal financial incentives for Meaningful Use of EHRs.

    c. Standalone e-Prescribing software is also available at no cost from Allscripts and the National e-Prescribing Patient Safety Initiative (NEPSI).

    d. Most programs also check for drug interactions, dosage errors, medication allergies and patient-specific medication factors.

    e. Office prescription renewal requests can be synchronized with this system and with some Personal Health Records.

    f. e-Prescribing encourages patients to fill prescriptions (currently 20% do not), because the prescription is sent to the pharmacy electronically and is ready to be picked up when they arrive.

    g. Costs are lowered by flagging generic and “on-formulary” drugs.

    However, practices are exposed to community medication histories through e-Prescribing; i.e., Dr A renews a medication, and his e-Prescribing program sends an alert advising him that it could interact with another drug. He has not prescribed that drug – so his office staff will have to contact the patient to identify who has, and then Dr A will have to contact Dr X to “negotiate” which drug will be discontinued or changed. If failure to do so results in patient injury from a drug interaction, the physician may be liable.

3. Many EHRs provide e-Prescribing drug information and Clinical Decision Support, and the government’s Meaningful Use requirements mandate minimum functionalities in both of these areas. Clinicians should know the source of the drug and Clinical Decision Support information in their EHRs, because the standards to which they may be held accountable are the clinical standards for their specialty and the information in FDA-approved drug labels or drug Alerts.

4. Doctors may ignore, override or disable alerts, warnings, reminders and embedded practice guidelines – due to “alert fatigue.” If it can be shown that following an alert or guideline would have prevented an adverse patient event, the physician may be found liable for failing to follow it.

5. Meaningful Use requires online patient connectivity, and many EHRs have patient questionnaires that utilize an algorithm to interview the patient. These questionnaires often address, and

memorialize in the record, issues that many physicians are simply not prepared to pursue (depression, substance abuse, etc.). Lack of or incomplete follow-up can create potential liability – and there is a clear record for the plaintiff's attorney to follow.

6. Vendor contracts may attempt to shift medical liability risks resulting from faulty software design or decision support data onto the physician. They may also provide that the vendor has rights to utilize patient or provider data. Read these contracts carefully.

7. **Electronic Discovery:** Lawyers may request not only printed copies of the EHR but also the "raw" e-data for metadata analysis, i.e. log-on time, what was reviewed and for how long, what changes or additions were made – and when, log-off time, etc. Smart phone and email records are also discoverable. Physicians need to know that all of their interactions with the EHR are time-tracked and discoverable.

8. Doctors may "copy" information from a prior note or visit and "paste" it into a new note or visit (known as "cloning"), making changes where appropriate or documenting by exception. This may result in irrelevant over-documentation and the patient may appear to have more or less complex problems since the prior encounter. By substituting a word processor for the physician's thoughtful review and analysis, the narrative documentation of daily events and the patient's progress may be lost, thereby compromising the record of the patient's course. The quality of notes and documentation may be further compromised by the use of templates.

9. EHRs may auto-populate fields in the History and Physical (from data derived from data fields in a prior H&P) and in Procedure Notes (from personalized or packaged templates). While over-documentation may facilitate billing, if erroneous or outdated information is entered, it may increase liability. For example: An internist was deposed and his EHR was the medical record. Some of the auto-populated fields contained obviously wrong information, and at deposition the plaintiff's attorney asked these questions:

   a. "So is the information in this record accurate or not?"
   b. "Do you bother looking at your records?"
   c. "If these 'auto-populated' fields are incorrect, can we trust anything in this record?"
   d. "Do you deliver the same level of care as you do in record keeping?"

   Templates with drop down menus facilitate data entry. However, they are usually integrated with other automated features, and an entry error may be perpetuated elsewhere in the EHR – and overlooked, resulting in a new potential for error. Erroneous information, once entered into the EHR, is easily perpetuated and disseminated.

10. The computer may become a barrier between the doctor and patient – as the doctor fills-in a computer template that diverts attention from the patient and restricts creative thinking. This may weaken the doctor-patient relationship.

Reprinted with permission from the iHealth Alliance and PDR Network.

Appendix B: Electronic Communication (E-mail) Agreement

[This document should be individualized for the practice]

Electronic (online) communications include e-mail, webmail, secure messaging, electronic file transfer, text messaging and internet "portals" to exchange information between computers, tablets, smartphones. These can be useful ways for patients and healthcare providers to communicate, in addition to more usual visits and phone calls.

Advantages

- E-mail is a simple, convenient and popular way of connecting; many people use it regularly
- Messages can be sent and received without needing both parties online at the same time
- Messages can be saved, copied and forwarded; they keep a record of what was said
- Some messaging systems are encrypted to help keep information private
- Some questions and issues can be handled by online messaging without a phone call or visit

Disadvantages

- E-mail devices and connections can fail, messages can be lost or sent to the wrong person
- There is no way to know if a message was ever received
- Messages can contain typing mistakes
- If the other party is away or their device is turned off, messages might not be seen promptly
- It is possible for a dishonest person to send a false message or impersonate a patient or a doctor
- If both parties are not online at the same time, there is no opportunity to clarify misunderstandings
- Saved copies or messages sent in error can't be erased or retracted
- Messages can contain viruses that can damage systems or steal information
- Some medical questions and issues cannot be handled through online messaging

Our E-mail Policies

1. **No emergencies or urgent messages.** E-mail is not to be used for emergencies or urgent messages. We do not monitor our In-Box constantly. You can send a message any time, but we may not read it until the next business day. We check messages during regular work hours, and answer them in the order received. We try to deal with messages within 1 work day, but circumstances could cause us to fall behind. Use the telephone if you need a response right away. Of course, in a life-threatening emergency call 911.

2. **Uses.** Our practice accepts E-mail messages for these purposes:

    a. **General messages** like making or changing appointments, billing issues, or other questions that can be answered by any appropriate staff person. [Use ________________________]

    b. **Medical questions.** Our providers may give their professional E-mail addresses to you for medical questions. Although they might sometimes reply after hours, you should not expect providers to monitoring their mail continuously. Even on-call it's likely the provider is not sitting at a computer. Again, if you have a problem that needs attention right away, use the telephone. [Use ________________________]

    c. **Prescription renewals.** You can request refills of medicines we have previously prescribed, the same way as leaving a phone message. If we have a question for you, we may respond by E-mail or phone. [Use ________________________]

3. **Part of the record.** E-mail messages are considered part of your medical record. Our policies for record privacy and appropriate uses of medical information apply to messages we send to each other.
4. **Security.** You need to protect the E-mail address you give us, to make sure our communications remain private. This is the only way we can trust that messages from your E-mail are really from you, and messages we send are not going to someone else. If we aren't sure about a message, we will try to contact you in some other way.
5. **Availability.** If you ask us to use E-mail to communicate with you, we will assume that you check your In-Box at reasonable intervals. We don't guarantee that we will respond to your messages and we understand you can't guarantee that you will respond to ours. In cases of uncertainty, we will try other ways of communicating.
6. **Sensitive medical information.** We can't always know what information you consider especially private. We take care with all medical records, but we know that some facts are more sensitive than others. Because E-mail can't be guaranteed 100% secure, please don't put extremely sensitive matters in messages without considering this.
7. **Voluntary.** Using E-mail is voluntary for both of us. If we feel you are using E-mail inappropriately (or, if we think your address has been hacked by an imposter), we may block your messages. If you decide you don't want to receive E-mail from us any longer, just let us know.
8. **Changes of address.** If your E-mail address changes, you need to let us know.
9. **Non-essential uses.** We will only use your E-mail address for important communications related to our practice. We will not give your E-mail address to anyone who is not part of our practice. Please don't send non-essential messages to us, because they slow down our ability to respond to the important ones.
10. **Mistakes.** Mistakes happen. If you believe you have received or sent a message by mistake, or one that contains errors, please let us know. You should delete messages that are not intended for you.
11. **Other risks.** In addition to those above, electronic communication can have other risks and disadvantages that might cause inconvenience or harm. Everyone using E-mail needs to use good judgment about these valuable technologies, and must remember that there are alternatives that would be better for some situations.

Acknowledgement and Agreement

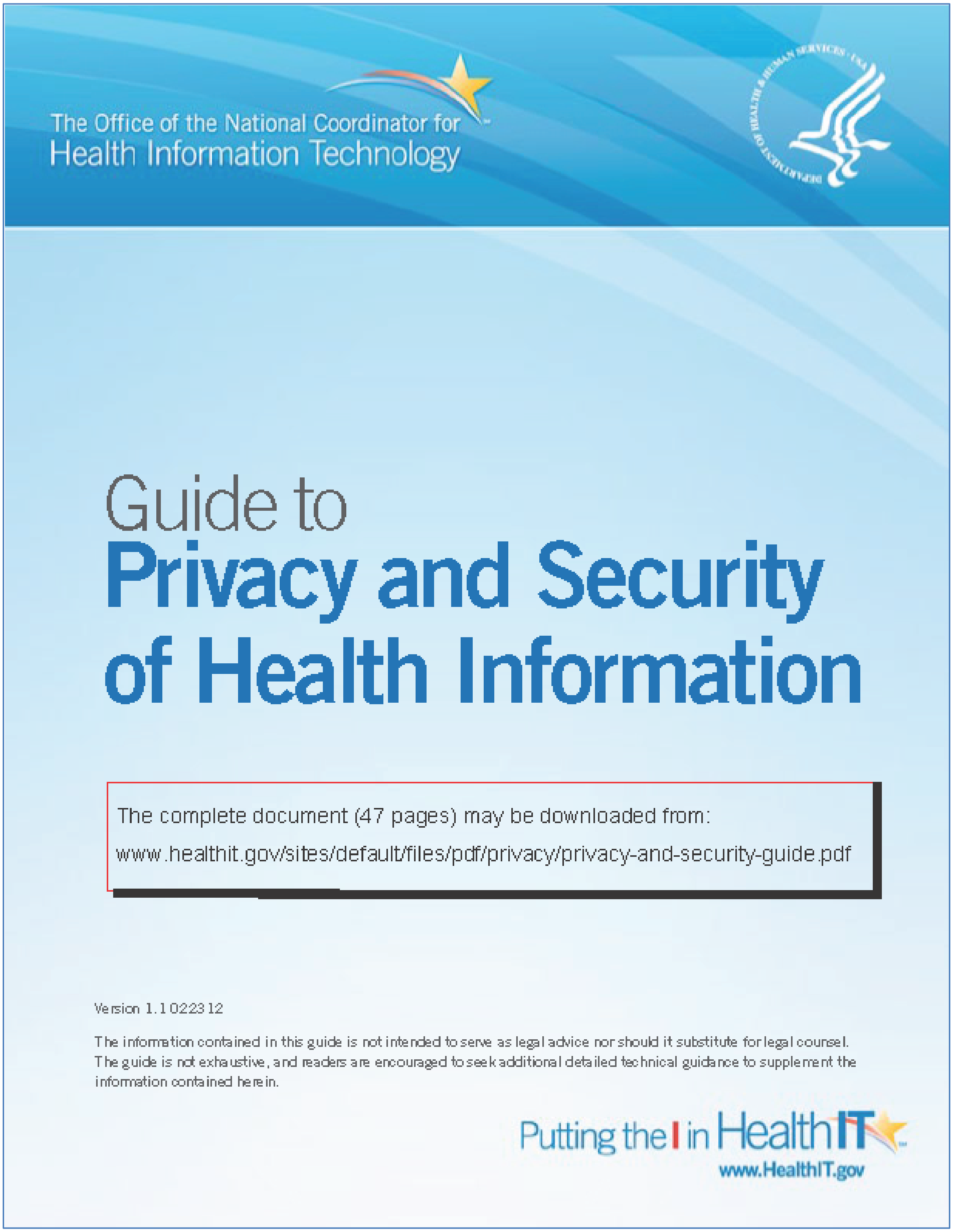
I acknowledge that I have read this form. I understand that electronic (online) communication has risks, including possible risks not mentioned above. I agree to abide by the policies described above. I agree to use reasonable judgment with regard to any messages I send or receive. I do not have any unanswered questions about what this Agreement requires.

Patient (or legal representative) name: ______________________________

Signature: ______________________ Date: ______________________

E-mail address to be used: ______________________________

Appendix C: Guide to Privacy and Security of Health Information



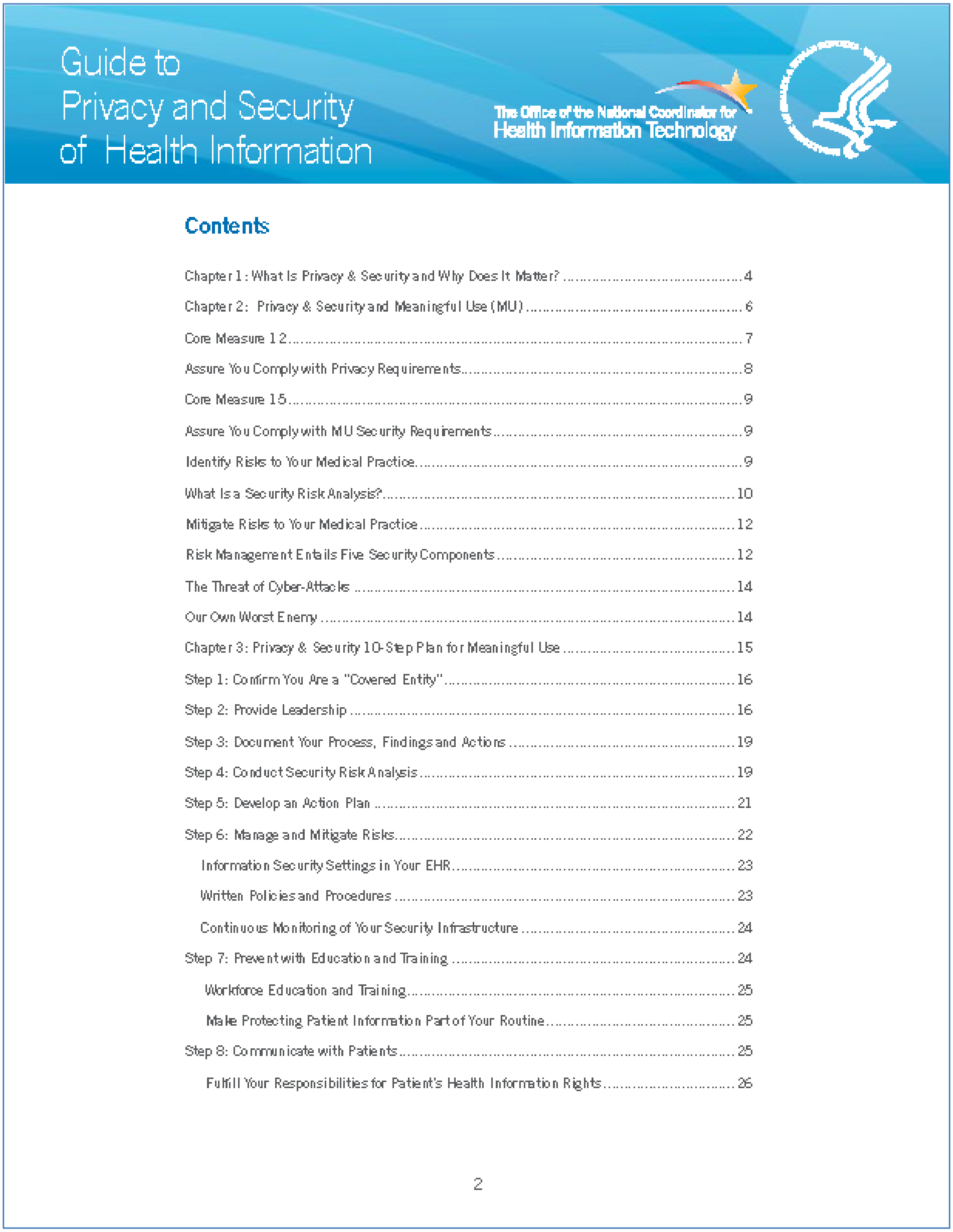
The Office of the National Coordinator for
Health Information Technology

Guide to
Privacy and Security
of Health Information

The complete document (47 pages) may be downloaded from:
www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

Version 1.1 022312

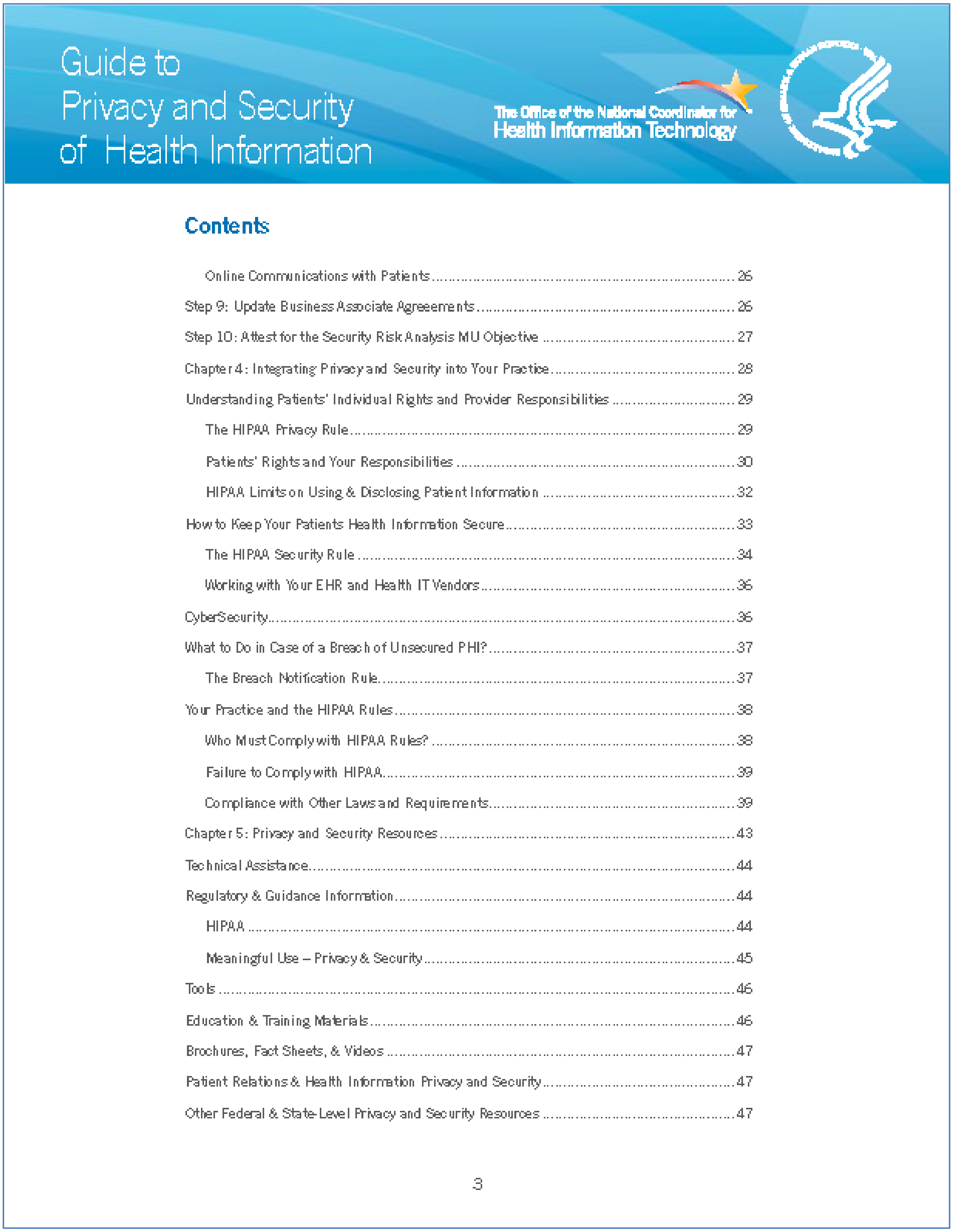
The information contained in this guide is not intended to serve as legal advice nor should it substitute for legal counsel. The guide is not exhaustive, and readers are encouraged to seek additional detailed technical guidance to supplement the information contained herein.



Guide to Privacy and Security of Health Information

The Office of the National Coordinator for Health Information Technology

Contents

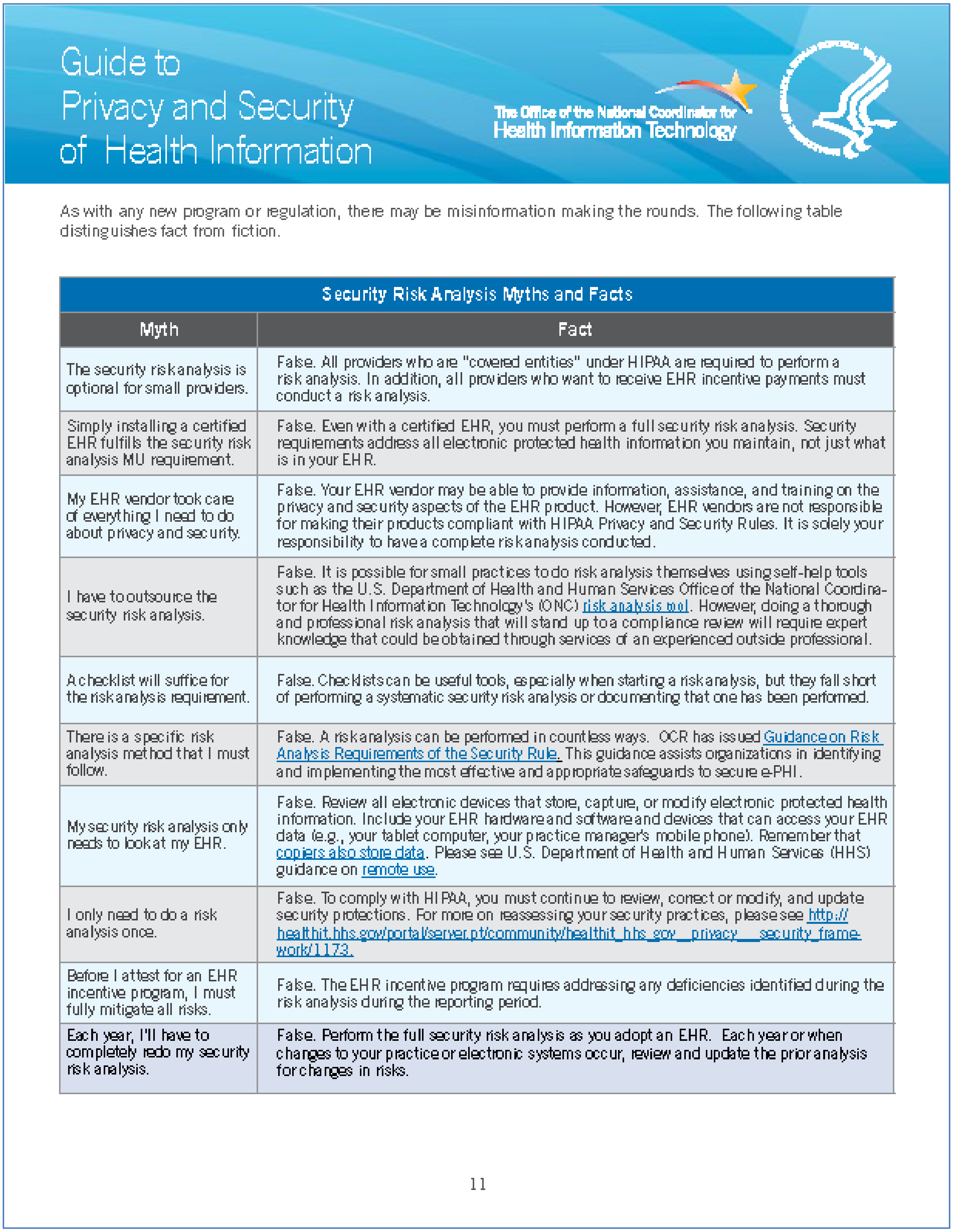


Guide to
Privacy and Security
of Health Information

The Office of the National Coordinator for
Health Information Technology

Contents

3



Guide to Privacy and Security of Health Information

The Office of the National Coordinator for
Health Information Technology

As with any new program or regulation, there may be misinformation making the rounds. The following table distinguishes fact from fiction.

Security Risk Analysis Myths and Facts	
Myth	**Fact**
The security risk analysis is optional for small providers.	False. All providers who are "covered entities" under HIPAA are required to perform a risk analysis. In addition, all providers who want to receive EHR incentive payments must conduct a risk analysis.
Simply installing a certified EHR fulfills the security risk analysis MU requirement.	False. Even with a certified EHR, you must perform a full security risk analysis. Security requirements address all electronic protected health information you maintain, not just what is in your EHR.
My EHR vendor took care of everything I need to do about privacy and security.	False. Your EHR vendor may be able to provide information, assistance, and training on the privacy and security aspects of the EHR product. However, EHR vendors are not responsible for making their products compliant with HIPAA Privacy and Security Rules. It is solely your responsibility to have a complete risk analysis conducted.
I have to outsource the security risk analysis.	False. It is possible for small practices to do risk analysis themselves using self-help tools such as the U.S. Department of Health and Human Services Office of the National Coordinator for Health Information Technology's (ONC) risk analysis tool. However, doing a thorough and professional risk analysis that will stand up to a compliance review will require expert knowledge that could be obtained through services of an experienced outside professional.
A checklist will suffice for the risk analysis requirement.	False. Checklists can be useful tools, especially when starting a risk analysis, but they fall short of performing a systematic security risk analysis or documenting that one has been performed.
There is a specific risk analysis method that I must follow.	False. A risk analysis can be performed in countless ways. OCR has issued Guidance on Risk Analysis Requirements of the Security Rule. This guidance assists organizations in identifying and implementing the most effective and appropriate safeguards to secure e-PHI.
My security risk analysis only needs to look at my EHR.	False. Review all electronic devices that store, capture, or modify electronic protected health information. Include your EHR hardware and software and devices that can access your EHR data (e.g., your tablet computer, your practice manager's mobile phone). Remember that copiers also store data. Please see U.S. Department of Health and Human Services (HHS) guidance on remote use.
I only need to do a risk analysis once.	False. To comply with HIPAA, you must continue to review, correct or modify, and update security protections. For more on reassessing your security practices, please see http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__privacy___security_framework/1173.
Before I attest for an EHR incentive program, I must fully mitigate all risks.	False. The EHR incentive program requires addressing any deficiencies identified during the risk analysis during the reporting period.
Each year, I'll have to completely redo my security risk analysis.	False. Perform the full security risk analysis as you adopt an EHR. Each year or when changes to your practice or electronic systems occur, review and update the prior analysis for changes in risks.

11

Index