Cyber Risk Assessment

Version 160301

Checklist
For Office Practices

© 2016, Michael S. Victoroff, MD

Contents

Foreword

- **Health Information Technology (HIT) exposes providers to several kinds of liability — besides "malpractice"**
- **There's more to it than just HIPAA**
- **HIT threats need to be understood and defended against**
- **It's not optional**

Federal and State laws (HIPAA, ACA and others) impose specific requirements on medical practices regarding information security and privacy. Some of these are:

- The Privacy Rule
- The Security Rule
- The Breach Notification Rule
- The Enforcement Rule

Violations of Federal and State laws and regulations may be prosecuted outside the professional liability mechanisms that providers are familiar with, and are not typically covered by professional liability ("malpractice") insurance.

In addition to statutory civil and criminal liabilities, everyone who manages Protected Health Information (PHI) and other kinds of confidential information (for example, employee records, business records, trade secrets) is subject to lawsuits by parties who claim injuries from information loss, breach and misuse. Moreover, there are standards besides HIPAA (e.g., Payment Card Industry rules) that medical practices may be required to comply with.

While there may *also* be professional liability associated with privacy and security failures, it is vital that providers understand that most traditional "malpractice" insurance does not cover investigation, defense, notification or mitigation costs resulting from data loss or breach, and particularly does not cover civil and criminal penalties – which can be substantial. Practitioners are encouraged to discuss *Cyber Liability* coverage with their insurance carriers.

This collection of resources is provided to assist the medical community in learning and thinking about health information technology for the benefit of our patients and in the interest of safe and effective medical practice. It is not comprehensive or tailored for the needs of any particular specialty or facility, which may have risks and exposures that are not addressed in this outline. Please send feedback, corrections and questions.

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

Dr. Victoroff is among the first group of physicians to become board certified in the specialty of Clinical Informatics (he is also board certified in Family Practice). He 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 he is a consultant to Parity Computing, Inc., 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 a 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 received 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 material; and they do not endorse any product mentioned as being superior to any competitor, or as meeting the needs of any specific user. 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 systems 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., Ste. 400, 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

Introduction

HIPAA[1] *requires* practitioners who create, receive, maintain (store) or transmit patient information electronically to "Conduct accurate and thorough assessment of the potential risks and vulnerabilities to the **confidentiality, integrity and availability** of electronic protected health information (ePHI) held by the covered entity."[2] [CFR164.308(a)(1)(ii)(A).] In 2009, this requirement was extended to Business Associates.[3] In addition, many States have legislation that expands responsibilities of covered entities beyond Federal requirements.

This is not optional. The U.S. Office for Civil Rights (OCR) is responsible for enforcing HIPAA. If the practice finds itself facing a complaint or an OCR audit, one of the first documents it will be required to produce is this risk assessment, and its policies and procedures.

HIPAA is only one of many standards that apply to information privacy and security. Other Federal and State laws and regulations, obligations built into many commercial contracts – and common civil liability – form a complex web of accountability for every entity that collects, generates, stores or transmits information. Even information holders that are not "covered entities" under HIPAA's definition are subject to legal liability for privacy and security practices.

In addition to protecting information in electronic forms, healthcare practitioners are responsible for safeguarding PHI in all forms, including paper, verbal and other media. *While this document focuses on ePHI, much of it applies to information that is not in electronic form.*

The Structure of a Risk Assessment

An information systems risk assessment draws on 2 kinds of expertise:

- The knowledge of the users who purchased, configured and operate the system – and who know how it's supposed to work from day to day.
- The knowledge of experts who understand the design and function of the technology – and its vulnerabilities and how to protect it.

Occasionally, both kinds of knowledge might be found in the same people, but in most IT environments a team effort is required, often calling upon outside consultants (see *Your Security Consultant*, p. 10).

1. Identify your information vulnerabilities and threats (risk audit)
    a. Inventory the PHI you're responsible for
    b. Inventory the electronic devices you're responsible for (local and remote)
    c. Inventory the people who have access to your PHI and devices (internal and external)
    d. Note the ways your PHI and devices are vulnerable
    e. Identify your threats
2. Audit defenses already in place – your own, plus those of Business Associates, vendors, suppliers, etc.
    a. Vendors and technology partners who create, receive, maintain or transmit PHI are HIPAA Business Associates (and need BA Agreements)

[1] "Security Standards for the Protection of Electronic Protected Health Information (ePHI)" [45 CFR Part 160 and Part 164, Subparts A and C], commonly known as the Security Rule.

[2] www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidance.html

[3] 2013 update: http://www.gpo.gov/fdsys/pkg/CFR-2013-title45-vol1/xml/CFR-2013-title45-vol1-sec164-308.xml

   b. Some vendors (e.g., your banker) may not handle PHI (so are not BAs, from HIPAA's point of view), but still may be exposed to other kinds of confidential business (or personal) information
3. Estimate the chance (risk) that each given threat might occur
4. Predict the harm (impact) if it occurred
5. Assess measures to block vulnerabilities, neutralize threats, reduce risks and mitigate impacts
   a. Survey and evaluate Physical, Technical and Administrative safeguards
   b. This may include testing safeguards by attempting to penetrate them
6. Make a plan that prioritizes your defenses in a sensible way
   a. Greatest risks vs. greatest harms
   b. Simplest, cheapest, quickest safeguards first; more and better ones in a continuing cycle of improvement
   c. Compliance with legal, professional, industry and community standards
7. Implement new defenses as appropriate
8. Document your work!
   a. The process of writing your Risk Assessment begins with the very first draft, and simply becomes more detailed with each version
9. Lather, rinse, repeat

It is important to realize that compliance with laws and regulations does not in itself comprise a security plan. Organizations fully compliant with current standards have information failures, and are still subject to liability and penalties when this occurs.

Vulnerability, Threat, Risk and Impact

A **vulnerability** is a weakness that provides an opening for a harmful event.

> *Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.* [NIST SP 800-30 (rev1)]].

A **threat** is something that can cause a harmful event.

> *Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.* [NIST SP 800-30 (rev1)].

A **risk** is the likelihood of a harmful event happening.

> *A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.* [NIST SP 800-30 (rev1)]

An **impact** is the kind of effect a harmful event would have on people, organizations and property (e.g., legal, operational, reputational, business or financial).

> *The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.* [NIST SP 800-30 (rev1)]

Examples of threats[4]

Environmental

Fire, flood, tsunami, earthquake, volcanic eruptions, lightning, severe weather, smoke, dust, insects, rodents, chemical fumes, sprinkler activation, water leakage - pipe breakage, hole in roof, condensation, explosion - nearby gas line, chemical plant, tank farm, munitions depot, vibration - nearby railroad track, jet traffic, construction site, electromagnetic interference, electrostatic discharge.

Physical

Unauthorized facility access, theft, vandalism, sabotage, extortion, terrorism/bomb threat, labor unrest - employees and support contractors, war/civil unrest, improper transportation - equipment dropped, submerged, exposed to weather or x-rayed in transit, improper mounting/storage - equipment exposed to bumps, kicks or weather, spillage/droppage - hazardous materials permitted near equipment (e.g. food, liquids), magnets/magnetic tools - can erase data or damage sensitive equipment, collision - fork lift, auto, plane, wheelchair, trip hazards/falls - equipment poses personnel hazards, fire hazards - flammable materials stored nearby, power outage, extreme/unstable temperatures, extreme/unstable humidity, unsafe environment - unfit for human occupation, facility inaccessibility - blocked ingress, inability to cut power - during fire, flood, etc., electrical noise/bad ground - suggested by flickering lights or jittery workstation displays, improper maintenance - unqualified support or preventive maintenance behind schedule, personnel unavailability - inability to contact operations or support personnel, telephone failure - inability to contact site from outside, inability to call out, service completely unavailable, inappropriate fire suppression - water, foam, PKP, Halon, inappropriate trash disposal - sensitive data released in an unauthorized manner.

Technical and Administrative

Improper/inadequate procedure - foreseeable events not supported by complete and accurate documentation and training, improper operation - operating equipment beyond capacity or outside of manufacturer's constraints, improper hardware configuration - prescribed hardware configured in other than the prescribed manner during installation, improper software configuration - prescribed software configured in other than the prescribed manner during installation, unauthorized hardware/ modification - adding other-than-prescribed hardware or making unauthorized modifications, unauthorized software/modification - adding other-than-prescribed software or making unauthorized modifications, unauthorized software duplication - creating copies of licensed software that are not covered by a valid license, unauthorized logical access - acquiring the use of a system for which no access has been authorized (as opposed to gaining physical access to the hardware), malfeasance (exceeding authorizations) - acquiring the use of a system in excess of that which has been authorized, unsanctioned use/exceeding licensing - utilizing authorized system resources for unauthorized purposes (resume, church bulletin, non-job-related e-mail or internet browsing) or exceeding a user licensing agreement, over- or under-classification - labeling of a resource at a higher or lower level of sensitivity than appropriate, malicious software - software whose purpose is to degrade system performance, modify or destroy data, steal resources or subvert security in any manner, hardware

[4] Adapted from http://www.hq.nasa.gov/security/it_threats_vulnerabilities.htm

error/failure [functionality] - hardware that stops providing the desired user services/resources, hardware error/failure [security] - hardware that stops providing the desired security services/ resources, software error/failure [functionality] - software that stops providing the desired user services/resources, software error/failure [security] - software that stops providing the desired security services/resources, media failure - storage media that stops retaining stored information in a retrievable/intact manner, data remanence - storage media that retains stored information in a retrievable/intact manner longer than desired (failure to totally erase), object reuse - a system providing the user with a storage object (e.g. memory or disk space) that contains useful information belonging to another user, communications failure/overload - a communications facility that stops providing service or is unable to provide service at the requested capacity, communications error - a communications facility that provides inaccurate service, data entry error - a system accepting erroneous data as legitimate, accidental software modification/deletion - deleting or otherwise making unavailable necessary software, accidental data modification/deletion - deleting or otherwise making unavailable necessary data, accidental data disclosure - inadvertently revealing sensitive data to an unauthorized user, repudiation - participating in a process or transaction but then denying having done so, masquerading - participating in a process or transaction but posing as another user, message playback - recording a legitimate transmission for retransmission at a later time in an attempt to gain unauthorized privileges, message flooding - generating an inordinately large quantity of transmissions in an attempt to make a system or service unavailable due to overload, line tapping - connecting to a communications facility in an unauthorized manner in an attempt to glean useful information, electronic emanations - information-bearing spurious emissions associated with all electronic equipment (prevented by tempest equipment or shielding), geo-location - a system inadvertently revealing the current physical location of a user.

Examples of vulnerabilities

Complicated user interface, default passwords not changed, disposal of storage media without deleting data, equipment sensitivity to changes in voltage, equipment sensitivity to moisture and contaminants, equipment sensitivity to temperature, inadequate cabling security, inadequate capacity management, inadequate change management, inadequate classification of information, inadequate control of physical access, inadequate maintenance, inadequate network management, inadequate or irregular backup, inadequate password management, inadequate physical protection, inadequate protection of cryptographic keys, inadequate replacement of older equipment, inadequate security awareness, inadequate segregation of duties, inadequate segregation of operational and testing facilities, inadequate supervision of employees, inadequate supervision of vendors, inadequate training of employees, incomplete specification for software development, insufficient software testing, lack of access control policy, lack of clean desk and clear screen policy, lack of control over the input and output data, lack of internal documentation, lack of or poor implementation of internal audit, lack of policy for the use of cryptography, lack of procedure for removing access rights upon termination of employment, lack of protection for mobile equipment, lack of redundancy, lack of systems for identification and authentication, lack of validation of the processed data, location vulnerable to flooding, poor selection of test data, single copy, too much power in one person, uncontrolled copying of data, uncontrolled download from the internet, uncontrolled use of information systems, undocumented software, unmotivated employees, unprotected public network connections, user rights are not reviewed regularly.

Examples of impacts

Clinical error, delay of diagnosis or treatment, wrong patient, wrong site, wrong drug, wrong procedure, wrong dose, privacy breach, injury to professional/patient/staff reputation, civil liability,

criminal liability, financial costs/liability, employer/owner/officer liability, financial loss, data loss, data corruption, data unavailable, billing error, lost revenue, lost time/resources, property loss/damage, personal injury.

Intrinsic and extrinsic risks

All healthcare processes and tools have *intrinsic* risks. This is the nature of things, and part of the reason behind informed consent. For most things like medicines, procedures and equipment, the risk is of accidents and unintentional errors and side effects. Healthcare is fundamentally altruistic, and its safety measures are traditionally not concentrated on defending against crime.

However, information technology is associated with substantial *extrinsic* risks. These are dangers arising from deliberate sabotage, interference and malice. Introducing HIT to the healthcare environment has the unfortunate side effect of inviting hackers, international criminal networks, casual pranksters and snoops – and even terrorists – to test the defenses of electronic systems. Professional criminals with advanced IT skills recognize the value of the information kept in healthcare databases, and systematically attack them. And, even amateur interference with critical systems can be lethal.

This second category of risk is not yet fully appreciated among healthcare providers, many of whom are unprepared for the nature and determination of the adversaries they must now deal with. Some serious dangers accompany – without nullifying –the extraordinary benefits of HIT.

Safeguards

Defenses fall into 3 general domains:

1. **Physical** – Devices, controls and countermeasures such as locks, doors, keys, fences, ID badges, signs, emergency power supplies, receptionists, guards, etc.
2. **Technical** – Devices, controls and countermeasures such as anti-virus, encryption, passwords, firewalls, software updates, access control lists, off-site backup, etc.
3. **Administrative** – Devices, controls and countermeasures such as training, policies, audits, IT support, credentialing, background checks, disaster plan, etc.

The Privacy Rule applies to *all forms* of PHI: electronic, written and verbal. (The Security Rule covers only PHI in electronic form.)

> *The Privacy Rule's safeguards standard is flexible and does not prescribe any specific practices or actions that must be taken by covered entities. This allows entities of different sizes, functions, and needs to adequately protect the privacy of PHI as appropriate to their circumstances. However, since each covered entity chooses the safeguards that best meet its individual needs, the types of protections applied may not be the same across all participants exchanging electronic health information to or through a health information organization (HIO), and some participants may not be covered entities.*[5]

[5] http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/safeguards.pdf

Office for Civil Rights Investigations

Areas where the OCR finds the most problems

1. Risk assessment has not been done
2. Policies and procedures aren't current
3. Security training is inadequate
4. Workforce clearance (background checks, credentials) is inadequate
5. Workstations are not effectively secured
6. Encryption is not in place

Areas where the OCR tends to focus its investigation

- Risk analysis and management
- Security training
- Physical security of facilities and mobile devices
- Off-site access and use of ePHI from remote locations
- Storage of ePHI on portable devices and media
- Disposal of equipment containing ePHI
- Business associate agreements and contracts
- Data encryption
- Virus protection
- Technical safeguards in place to protect ePHI
- Monitoring of access to ePHI

Your Security Consultant

Information security gets very technical, very fast. ("Have you changed the default Admin ID and Password on your Wi-Fi router?" "Do you have a secure API Gateway?") Even IT experts use consultants. Few individuals have the knowledge to evaluate, implement and test the full range of threats and safeguards involved with health information systems, especially in large facilities. Even if you were comprehensively knowledgeable, you can't test your own system any more than a neurosurgeon can operate on his/her own head.

Security consultants are like other professionals; lawyers, doctors, engineers. Everybody specializes. Some are best at physical security (locks, alarms, surveillance, disaster preparedness); some specialize in software and human vulnerabilities (viruses, hacking, phishing, social engineering); some perform "penetration testing" (trying to hack into your system electronically, break in physically, trick employees into disclosing passwords over the phone, etc.). Some give expert legal or insurance advice (HIPAA, employment practices, liability coverage, etc.) Cyber security represents yet another expense and commitment, and you must not underestimate its importance.

On-site providers, staff and trainers are the best resources to catalog your IT assets and their uses. They are certainly the ones to review your *clinical information practices* (see p. 17). But, you will also need to engage one or more experts versed in health IT, law and insurance to work through the checklists below.

Collaboration

Whatever resources you call on for IT support, you need to involve them in the clinical enterprise. Integrating HIT experts with clinical staff activities is still uncommon in most organizations, and represents an important opportunity for safety and security planning.

Asset Inventory

"Information Assets" are *Confidential Information* and various kinds of property and resources used to manage it. Confidential information includes Protected Health Information (PHI) as well as important business information such as credit card numbers, banking and legal records, employee records, etc.

It is important to keep records of all your hardware, software and vendors – but particularly the ones that create, receive, maintain or transmit PHI. These are necessary for business accounting, and also to manage warrantees, support, upgrades, updates, patches, fixes, insurance, etc., as well as being able to identify which external entities are HIPAA Business Associates. This information is also vital in recovering from disaster. There is no universal format for keeping these records; the scope and level of detail needed is unique to each organization. A spreadsheet is adequate for most office practices. There are numerous software applications available for organizations that need to track a large number of assets across a workforce or multiple locations.

> *The Office of the National Coordinator has released a **"Risk Assessment Tool"** for medical practices (see p. 25) that can guide this process.*

Some items to consider tracking

Information

- Patient records (PHI)
- Business records
- Insurance records
- Legal records
- Personnel records

Hardware

- Device name, model number, serial number
- Date purchased, vendor, price, quantity
- Extended warranty, service contract
- Support/service resources
- Insurance coverage

Software

- Name, version, serial number or "activation key"
- Date purchased/licensed, vendor, price, quantity
- License expiration, terms, active licenses assigned
- Device(s) where installed
- Support/service contract, helpdesk

Vendors and resources

- Vendor name, sales contact, support contact
- Products purchased/licensed, terms
- Warranty/support terms

Emergency contacts and resources

- Administrators, support techs
- Password vault
- Fire, flood, HVAC, power, facility management
- Backup system

Insurance

- Agency, representative, underwriter, contacts
- Terms and dates of coverage
- Assets covered

EHR Safety Checklists

Here are some checklists to help prompt you with ideas for your audit and planning. They are not comprehensive and will not necessarily apply to your particular IT environment.

INVENTORY – INFORMATION ASSETS

A patient record count is one of the factors that determine what controls are reasonable for you to undertake (and what your insurance needs may be). At any moment in time, you should be able to declare, definitively, the number of individual patient records in your control and where they are located. It should also be possible for you – or your legal representative in case you are not able – to locate and produce valid copies of all records critical to running your operation.

	Where is your Confidential Information…?	Record count	Encrypted	Secured	No	?
1	Desktop computers, local drives		☐	☐	☐	☐
2	On-site server		☐	☐	☐	☐
3	Cloud/off-site server (e.g., GoogleDocs, Dropbox, etc.)		☐	☐	☐	☐
4	Laptops		☐	☐	☐	☐
5	Tablets		☐	☐	☐	☐
6	Smartphones		☐	☐	☐	☐
7	External/portable hard drives		☐	☐	☐	☐
8	CDs/DVDs/VHS/Other Media		☐	☐	☐	☐
9	USB “flash” drives		☐	☐	☐	☐
10	Tapes or other removable media		☐	☐	☐	☐
11	Printers, scanners, fax machines with internal memory (data cache)		☐	☐	☐	☐
12	On-site paper charts, files		☐	☐	☐	☐
13	On-site X-ray film, media		☐	☐	☐	☐
14	On-site other durables and artifacts (e.g., specimens)		☐	☐	☐	☐
15	Off-site physical storage		☐	☐	☐	☐

	Where is your Confidential Information…?	Record count	Encrypted	Secured	No	?
16	Outside billing service		☐	☐	☐	☐
17	(more…)		☐	☐	☐	☐

* "Encrypted" means unreadable without a key, even if the file is stolen. "Secured" means protected from theft/loss but not encrypted.

INVENTORY – PEOPLE

The most vulnerable component of any information system is the people who work with it.

	Who has access to your PHI…?	Controlled	?
18	Clinical staff (doc, midlevel, nurse, medical assistant)	☐	☐
19	Non-clinical staff (receptionist, office manager, transcriptionist)	☐	☐
20	Others who work in your facility (maintenance, cleaning, carpenter)	☐	☐
21	Professional consultants (accountant, attorney, financial/insurance advisor)	☐	☐
22	Contractors and Business Associates (e.g., IT support, consultants, billing service)	☐	☐
23	Liability insurance carrier	☐	☐
24	Part-time/temporary staff, agency staff	☐	☐
25	Patients, visitors, guests, salespeople, pharma reps	☐	☐
26	Staff family members and guests	☐	☐
27	Inspectors, auditors, reviewers, law enforcement	☐	☐
28	Patient portal	☐	☐
29	Social media (website, Facebook, Twitter, Sermo, LinkedIn, YouTube, etc.)	☐	☐
30	(more…)	☐	☐

* "Controlled" means they have passwords, keys, badges or other verifiable access to PHI and are subject to some form of control, monitoring and/or accountability.

PHYSICAL SAFEGUARDS

	What are your physical safeguards?	Yes	No	+/-	?
31	There is access control to enter the premises	☐	☐	☐	☐
32	The premises are locked after (during?) business hours	☐	☐	☐	☐
33	Intrusion alarms are used after (during?) business hours	☐	☐	☐	☐
34	Unescorted visitors are prevented from entering secure parts of the premises	☐	☐	☐	☐
35	There are "safety" areas for shelter against armed intruders	☐	☐	☐	☐
36	Removable media are physically secured when not in use	☐	☐	☐	☐
37	Smoke/fire alarms are functional	☐	☐	☐	☐
38	Water/flood alarms are in use where appropriate	☐	☐	☐	☐
39	Fire protection systems are designed not to damage electronic devices	☐	☐	☐	☐
40	Electronic components are protected from power surges/spikes	☐	☐	☐	☐
41	Critical components are powered through uninterruptable power supplies	☐	☐	☐	☐
42	Critical components are physically protected from intrusion and accidents	☐	☐	☐	☐
43	Devices are protected from theft	☐	☐	☐	☐
44	Name badges, access cards, etc., are inventoried and controlled	☐	☐	☐	☐
45	There is video surveillance	☐	☐	☐	☐
46	There is off-site backup	☐	☐	☐	☐
47	Documents to be destroyed are disposed of securely	☐	☐	☐	☐
48	Devices storing confidential information are disposed of securely	☐	☐	☐	☐

	What are your physical safeguards?	Yes	No	+/-	?
49	(more…)	☐	☐	☐	☐

ADMININSTRATIVE SAFEGUARDS

	What are your administrative safeguards?	Yes	No	+/-	?
	POLICIES AND ROLES				
50	A written document detailing the security policy is available on demand	☐	☐	☐	☐
51	A written document detailing the privacy policy is available on demand	☐	☐	☐	☐
52	There is a designated “Privacy Officer”	☐	☐	☐	☐
53	There is a designated “Security Officer”	☐	☐	☐	☐
54	Policies are reviewed as part of the orientation of new personnel	☐	☐	☐	☐
55	Policies are reviewed/updated periodically with staff input	☐	☐	☐	☐
56	Policies address data retention, backup and recovery, including e-mail	☐	☐	☐	☐
57	Policies address PHI access (e.g., who, what, where, how) and monitoring	☐	☐	☐	☐
58	Periodic privacy and security audits are performed	☐	☐	☐	☐
59	There is a plan of action for each type of foreseeable emergency, with a written reference guide for staff	☐	☐	☐	☐
60	Drills and rehearsals are periodically done for various emergencies (e.g., data breach, active shooter, biological/toxicological exposure, power failure)	☐	☐	☐	☐
61	There is a clear procedure for managing a suspected or actual privacy breach	☐	☐	☐	☐
62	Policies address retention/archiving/destruction/disposal of physical records, images, media, devices, computers, photocopiers, etc.	☐	☐	☐	☐
63	Policies address retention/archiving/destruction of ePHI	☐	☐	☐	☐
64	Policies address transfer of records with providers leaving the practice	☐	☐	☐	☐
65	Policies address workstation access and use	☐	☐	☐	☐
66	Policies address employee use of social media	☐	☐	☐	☐
67	Policies address use and protection of mobile devices	☐	☐	☐	☐
68	There are different levels of security for users with different job functions	☐	☐	☐	☐
69	There is a process with accountability for policy development and assessment	☐	☐	☐	☐
70	Policies address sanctions for violations	☐	☐	☐	☐
71	There is a process for evaluating the safety and compatibility of software and devices before installation	☐	☐	☐	☐
72	There is a schedule for monitoring for, and installing updates, fixes and patches to operating systems, applications, utilities and middleware	☐	☐	☐	☐
73	There is a schedule for periodically testing firewalls, antivirus software, malware and phishing defenses, and looking for evidence of penetration	☐	☐	☐	☐
74	There is user input into policy development	☐	☐	☐	☐
75	CPO, CSIO, CIO, CMIO, CLO, CMO, CNO, CEO et al. regularly communicate	☐	☐	☐	☐
76	IT staff/consultants regularly attend clinical staff meetings and have opportunities to “shadow” clinical users	☐	☐	☐	☐
77	Legal and ethics committees directly interact with privacy/security personnel	☐	☐	☐	☐
78	Policies address information use, ownership and confidentiality (e.g., intellectual property, copyright, trademark, trade secrets)	☐	☐	☐	☐
79	HIPAA Business Associate Agreements are in place with all vendors and contractors who create, receive, maintain (store) or transmit PHI	☐	☐	☐	☐
80	Organizational data sharing agreements are in place where appropriate	☐	☐	☐	☐
81	Policies address the use of portable devices (e.g., laptops, tablets, smartphones, flash drives, CDs/DVDs)	☐	☐	☐	☐

	What are your administrative safeguards?	Yes	No	+/-	?
82	Policies address removing data from the system (downloading, transmitting, printing, faxing, e-mailing, telecommuting)	☐	☐	☐	☐
83	Policies address personal use of information technology, including personal data storage, personal messages, personal internet use, personal software	☐	☐	☐	☐
84	Policies address which images (in an image archiving system) constitute the "official" medical record	☐	☐	☐	☐
85	Inventories of PHI, devices and authorized personnel are maintained accurately and are readily available	☐	☐	☐	☐
	ACCESS CONTROLS				
86	Policies address password management (e.g., complexity, strength provisioning, de-provisioning, expiration, sharing)	☐	☐	☐	☐
87	Passwords are unique for each user, kept confidential and not shared	☐	☐	☐	☐
88	There is a process for de-provisioning access for employees leaving the practice (e.g., inactivating passwords, returning devices, data, etc.)	☐	☐	☐	☐
89	Users are forced to change passwords periodically	☐	☐	☐	☐
90	Users are prompted to change passwords periodically	☐	☐	☐	☐
91	Records are kept of physical access to the facility by staff (especially after hours) and visitors ("Visitor Log")	☐	☐	☐	☐
92	Records are kept of maintenance to critical physical systems	☐	☐	☐	☐
93	Access logs are periodically reviewed for anomalies	☐	☐	☐	☐
	TRAINING & SUPPORT				
94	Privacy and security training are mandatory for everyone	☐	☐	☐	☐
95	Staff is acquainted with the risk of "phishing" scams and impersonation risks	☐	☐	☐	☐
96	There is a process for training employees on new applications	☐	☐	☐	☐
97	There is a process for documenting training	☐	☐	☐	☐
98	There is a process for evaluating correct use and adequate skills among users	☐	☐	☐	☐
99	There is a helpdesk or equivalent function, with emergency availability	☐	☐	☐	☐
	OTHER				
100	(more…)	☐	☐	☐	☐

TECHNICAL SAFEGUARDS

	What are your technical safeguards?	Yes	No	+/-	?
	GENERAL				
101	Appropriate firewalls are in place	☐	☐	☐	☐
102	Firewalls are up-to-date	☐	☐	☐	☐
103	Sensitive data is encrypted at rest	☐	☐	☐	☐
104	Sensitive data is encrypted during transmission	☐	☐	☐	☐
105	Unencrypted data is protected by strong access controls	☐	☐	☐	☐
106	Encryption meets current technical standards	☐	☐	☐	☐
107	Anti-virus, anti-phishing, anti-spyware/adware protections are in use; updates are timely installed	☐	☐	☐	☐
108	Data is backed up; backup files are encrypted	☐	☐	☐	☐
109	Data backup (on-site and off-site) and restore functions are regularly tested	☐	☐	☐	☐
110	Computer screens lock during inactivity and prior to staff leaving the office	☐	☐	☐	☐
111	Operating systems and software updates are timely applied	☐	☐	☐	☐
112	Routers and Wi-Fi access points are secured; Wi-Fi is encrypted; default administrator ID and password have been changed	☐	☐	☐	☐

	What are your technical safeguards?	Yes	No	+/-	?
113	Devices are password protected	☐	☐	☐	☐
114	Devices are encrypted	☐	☐	☐	☐
115	Technology is in place to implement access policies (as above)	☐	☐	☐	☐
116	Periodic audits are done of what software is installed and what it does	☐	☐	☐	☐
117	Periodic audits are done of devices connected to the system and what they do	☐	☐	☐	☐
118	Mobile devices have remote location/lockdown capability	☐	☐	☐	☐
119	Access to confidential information is monitored and logged; log files are periodically reviewed for accuracy and impact	☐	☐	☐	☐
120	User privileges are tested, monitored and controlled	☐	☐	☐	☐
121	E-mail system for internal users is encrypted and protected	☐	☐	☐	☐
122	Text messaging system for internal users is encrypted and protected	☐	☐	☐	☐
123	There is a secure messaging system for communicating with external users	☐	☐	☐	☐
124	Websites are protected with appropriate permissions and privileges	☐	☐	☐	☐
125	There are audit trails (metadata) capturing user-level data of transactions (e.g., “view,” “edit,” “delete,” “copy/paste,” “print,” etc.)	☐	☐	☐	☐
126	Multiple logins by a single user are monitored or restricted	☐	☐	☐	☐
127	Critical functions are tested after software updates	☐	☐	☐	☐
128	It is possible to determine which devices are accessing your data at any time	☐	☐	☐	☐
	TECHNICAL ACCESS CONTROLS				
129	Users are associated with unique passwords, tokens, biometric measures, or other means of definitive identification	☐	☐	☐	☐
130	Access to confidential information is controlled using unique IDs	☐	☐	☐	☐
131	Access to confidential information is restricted with respect to certain functions (e.g., read-only, edit, print, etc.)	☐	☐	☐	☐
132	Access to confidential information is restricted according to user roles	☐	☐	☐	☐
133	There is a procedure for emergency access to critical information	☐	☐	☐	☐
134	Users are automatically logged-off after a period of inactivity	☐	☐	☐	☐
135	Screens are automatically locked after a period of inactivity	☐	☐	☐	☐
136	The author (person or entity) for every transaction can be authenticated	☐	☐	☐	☐
137	There are controls protecting the integrity of electronically transmitted PHI	☐	☐	☐	☐
138	The organization is compliant with the Payment Card Industry (PCI) security standard if credit cards are processed	☐	☐	☐	☐
139	(more…)	☐	☐	☐	☐

DISASTER PLAN

A vital part of insuring information *availability* is to have a plan for each plausible disaster scenario that might impact the facility. Typical risks that should be considered include:

Natural

Tornado, hail, wind, blizzard, ice storm, flood, hurricane, storm surge; fire, lightning, pandemic, etc.

Human

Biological, nuclear, incendiary, chemical, explosive (BNICE); terrorism – cyber, food, water, infrastructure, hostages; active shooter, etc.

Disruption (accompany other disasters)

Personnel; electrical power, heating, air quality; transportation (food, water, ambulance, family, work); communications (phone, fax, news, internet); emergency services (police, ambulance, fire, hazmat); basic needs (shelter, food, water, sewer, clothing, medicine); family separation

	What is your disaster plan?	Yes	No	+/-	?
140	There is a disaster/continuity plan in the event of technology failure, power or communication interruption, or other catastrophe	☐	☐	☐	☐
141	There is a communication "tree"	☐	☐	☐	☐
142	Critical contact information is available on-site and off-site	☐	☐	☐	☐
143	There are contingencies for operating without electronic records, fax, phone, power, order entry, result reporting, etc.	☐	☐	☐	☐
144	There is a contingency plan for providing service at a different physical site	☐	☐	☐	☐
	OTHER				
145	(more…)	☐	☐	☐	☐

CLINICAL INFORMATION PRACTICES

This category of suggestions does not directly pertain to security and privacy, but highlights issues that have been shown to causes errors – and liability – in the use of healthcare information technology. Some suggestions may be considered "good practices." Others are alternative ways to address common risks. Nothing below represents a standard of practice.

	How good are your clinical information practices?	Yes	No	+/-	?
	GENERAL DOCUMENTATION				
146	Visit notes/dictation are recorded within 24 hours of the encounter	☐	☐	☐	☐
147	Visit notes/dictation are recorded within 7 days of the encounter	☐	☐	☐	☐
148	Dates of dictation and transcription are recorded	☐	☐	☐	☐
149	Users take a specific action (e.g., e-signature) to validate authorship	☐	☐	☐	☐
150	Authors validate entries within 24 hours of creation	☐	☐	☐	☐
151	The system "locks" entries after a defined period following creation	☐	☐	☐	☐
152	There is a method for correcting errors in notes directly within the note	☐	☐	☐	☐
153	There are alerting systems for missing documentation, orders without results, results without disposition, messages without replies, etc.	☐	☐	☐	☐
154	The "date-the-encounter-occurred" is evident for every entry	☐	☐	☐	☐
155	The system records user ID every time ePHI is created or changed	☐	☐	☐	☐
156	The system records user ID every time ePHI is viewed, printed or transmitted	☐	☐	☐	☐
157	The system tracks changes made after original entries are authenticated	☐	☐	☐	☐
158	Patient and provider identities are evident for every entry (onscreen and printed)	☐	☐	☐	☐
159	The author of every entry can be identified (including changes, additions and corrections)	☐	☐	☐	☐
160	A record of adverse reactions/contraindications (sometimes mislabeled "allergies") is displayed consistently and prominently	☐	☐	☐	☐
161	If there is a prescribing system, it is activated and used correctly	☐	☐	☐	☐
162	The prescribing system alerts prescribers about contraindications	☐	☐	☐	☐
163	The system alerts prescribers about duplication, interactions, dose, etc.	☐	☐	☐	☐

	How good are your clinical information practices?	Yes	No	+/-	?
164	Documentation clearly distinguishes between "not recorded," "not asked/examined," "asked/examined and normal," etc.	☐	☐	☐	☐
165	Adverse reactions/contraindications (often misnamed "Allergies") are verified at each visit	☐	☐	☐	☐
166	There is a method for indicating documentation is complete for a given visit	☐	☐	☐	☐
167	An individualized note is created for each patient encounter	☐	☐	☐	☐
168	The system requires authors to review entries prior to authentication	☐	☐	☐	☐
169	The system has ways to reduce the opportunity for orders, results, commutations to be filed without review	☐	☐	☐	☐
170	Periodic audits are done of the quality of documentation	☐	☐	☐	☐
171	Prescription documentation (including office samples) includes date, prescriber, form, dose, quantity, instructions, indication, and refills	☐	☐	☐	☐
172	Notes created with voice recognition are proofread for meaningful errors	☐	☐	☐	☐
173	All significant patient communications (including phone calls, e-mails, verbal contacts) are documented in the record	☐	☐	☐	☐
174	There is a process for verifying/reconciling record content with patients	☐	☐	☐	☐
	AUTO-POPULATED DATA				
175	The copy/paste function has been disabled	☐	☐	☐	☐
176	Policies stipulate whether and how the copy/paste function may be used	☐	☐	☐	☐
177	Fields that have been auto-populated by the system are reviewed/corrected at the time of documentation	☐	☐	☐	☐
178	Automatic paste-forward function is not used	☐	☐	☐	☐
179	Prior visit data is not automatically pasted forward into subsequent records	☐	☐	☐	☐
180	The system requires an affirmative decision and action by a clinician before certain critical actions (e.g., resolving problems, inactivating medications, deleting allergies, refilling prescriptions, acknowledging results)	☐	☐	☐	☐
181	Policies address how "copy/paste" will be used	☐	☐	☐	☐
182	Dropdown lists and templates are periodically reviewed by clinical staff	☐	☐	☐	☐
	DECISION SUPPORT				
183	Alerts, warnings, prompts, reminders, guidelines, etc. are periodically tested, reviewed and updated	☐	☐	☐	☐
184	Alerts, guidelines, etc. can be overridden or disabled under certain conditions	☐	☐	☐	☐
185	An audit trail is created when alerts, guidelines, etc. are overridden	☐	☐	☐	☐
186	Authorship and accountability for alerts, guidelines, etc. is clear	☐	☐	☐	☐
187	Legal responsibility for errors caused by alerts, guidelines, etc. is clear	☐	☐	☐	☐
	COMMUNICATION				
188	The practice uses e-mail to communicate with patients	☐	☐	☐	☐
189	The practice uses a secure messaging system to communicate with patients	☐	☐	☐	☐
190	The practice uses e-mail to communicate with providers, facilities, etc.	☐	☐	☐	☐
191	The practice uses a secure messaging system for providers, facilities, etc.	☐	☐	☐	☐
192	Incoming faxes are protected from loss or inappropriate disclosure	☐	☐	☐	☐
193	Incoming messages (from all sources) are reviewed before being saved	☐	☐	☐	☐
	RECALL, TRACKING, FOLLOW-UP				
194	There is a clinical tracking/reminder system	☐	☐	☐	☐
195	Tracking system monitors when items are due, delinquent and resolved	☐	☐	☐	☐
196	Tracking system can accommodate any type of future item/agenda	☐	☐	☐	☐
197	Tracking system monitors certain standard items (e.g., preventive procedures)	☐	☐	☐	☐
198	Tracking system triggers an alert/message when items are due	☐	☐	☐	☐

	How good are your clinical information practices?	Yes	No	+/-	?
199	Tracking system triggers an alert/message when items are delinquent	☐	☐	☐	☐
200	Tracking system changes the status of items as workflow progresses (e.g., status "received" changed to status "reviewed")	☐	☐	☐	☐
201	Tracking system can contact involved parties (e.g., patients, clinicians, staff, consultants)	☐	☐	☐	☐
202	Tracking system generates regular and on-demand reports	☐	☐	☐	☐
	IMPORT, ARCHIVING, RETENTION				
203	External paper documents are scanned into the EMR	☐	☐	☐	☐
204	Legacy paper documents are scanned into the EMR	☐	☐	☐	☐
205	Scanned documents are reviewed by a clinician	☐	☐	☐	☐
206	Scanned documents are verified before originals are destroyed	☐	☐	☐	☐
207	Incoming legacy/external paper documents are summarized by a clinician	☐	☐	☐	☐
208	If paper documents are not 100% scanned, all originals are retrievable	☐	☐	☐	☐
209	Effort is made to obtain prior records on all patients	☐	☐	☐	☐
210	There is a consistent process for obtaining prior records on all patients	☐	☐	☐	☐
211	Electronic image files are acquired, viewed, stored, transmitted, etc. in accord with industry standards	☐	☐	☐	☐
	RECORD INPUT AND OUTPUT				
212	A paper copy of a "visit record" can be readily generated	☐	☐	☐	☐
213	Printed visit records show (in a format easily used by readers): a. Date of visit b. Date documentation completed c. Provider identity (and author identity, if different) d. A note meeting applicable documentation standards e. Essential data, assessments, procedures, treatments and follow up plan f. Date printed Printed visit records do not contain: g. Irrelevant, redundant or confusing administrative/technical data that has minimal or no clinical value	☐	☐	☐	☐
214	A paper copy of the "complete patient chart" can be readily generated	☐	☐	☐	☐
215	Printed "complete patient charts" contain (in a format easily used by readers): a. All visit notes b. All results, reports, referrals, consultations and correspondence c. All external records received from other providers d. All records of communications (phone, e-mail, etc.) e. All other information appropriately requested f. Date printed	☐	☐	☐	☐
216	Outgoing records are reviewed for accuracy and completeness	☐	☐	☐	☐
217	An electronic copy of a "visit record" and a "complete patient chart" can be readily generated	☐	☐	☐	☐
218	There is a system to ensure that written documentation of phone calls or requests for medication refills are scanned into the EMR	☐	☐	☐	☐
219	Visual displays of patient information are usable and do not induce user errors	☐	☐	☐	☐
220	The record can be viewed during the visit by both physician and patient	☐	☐	☐	☐
221	The practitioner's process for interacting with the patient and the chart fosters good human interaction as well as effective data collection	☐	☐	☐	☐
222	Erroneous entries can be readily corrected and erroneous or misleading data is removed from the display	☐	☐	☐	☐

	How good are your clinical information practices?	Yes	No	+/-	?
223	If record locking is used, an amended/corrected entry is clearly connected with the original erroneous/incomplete entry	☐	☐	☐	☐
224	(more…)	☐	☐	☐	☐

THREAT MATRIX TEMPLATE (Duplicate as needed)

	Threat	Risk (Probability)			Impact (Effect)			Safeguards
		High	Med	Low	High	Med	Low	
		☐	☐	☐	☐	☐	☐	
		☐	☐	☐	☐	☐	☐	
		☐	☐	☐	☐	☐	☐	
		☐	☐	☐	☐	☐	☐	
		☐	☐	☐	☐	☐	☐	
		☐	☐	☐	☐	☐	☐	
		☐	☐	☐	☐	☐	☐	
		☐	☐	☐	☐	☐	☐	
		☐	☐	☐	☐	☐	☐	
		☐	☐	☐	☐	☐	☐	
		☐	☐	☐	☐	☐	☐	
		☐	☐	☐	☐	☐	☐	
		☐	☐	☐	☐	☐	☐	

Establishing a Culture of Safety

A "High Reliability Organization" is one that succeeds in avoiding adverse events in an environment where accidents are expected in the normal course of operations, because of risks and complexity. High Reliability Organizations have a recognizable "culture of safety."

	Does your organization have a "Culture of Safety?"	Yes	?
225	There is visible leadership commitment to safety as a priority	☐	☐
226	There is a blame-free environment for reporting errors, hazards, issues and adverse events	☐	☐
227	Staff are actively encouraged to report errors, hazards, issues and adverse events	☐	☐
228	Staff have confidence that reports will be acted upon	☐	☐
229	Proper and effective channels for reporting are well known among staff	☐	☐
230	There is an effective system for collecting and analyzing errors, hazards, issues and events	☐	☐
231	(more…)	☐	☐

Record Privacy Checklist

Security and *privacy* are not the same. Security addresses the requirements to insure the confidentiality, integrity and availability of clinical data. Privacy defines and limits the circumstances in which an individual's protected heath information may be used or disclosed.[6] Covered entities are bound by both the HIPAA Security and Privacy Rules.

	How are your record privacy practices?	Yes	No	+/-	?
232	There is a designated Privacy Officer	☐	☐	☐	☐
233	Patients are provided with required HIPAA forms and instructions	☐	☐	☐	☐
234	There are written policies and procedures addressing the processes for use and disclosure of protected information	☐	☐	☐	☐
235	Training addresses use and disclosure of protected information	☐	☐	☐	☐
236	The EHR has functionality for sequestering/segregating sensitive portions of the chart, at patient request, and to meet federal, state or local regulations (e.g., alcohol/drug treatment records)	☐	☐	☐	☐
237	There is a mechanism for tracking who has accessed patient information	☐	☐	☐	☐
238	A record of disclosures/access to PHI apart from treatment, payment or healthcare operations can be provided to patients on request	☐	☐	☐	☐
239	There is a process whereby patients can amend their medical records	☐	☐	☐	☐
240	There is a process whereby patients can restrict information from being released to a health plan if they are paying for a service out-of-pocket	☐	☐	☐	☐
241	There is a process for accommodating reasonable patient requests to use/not use specific channels of communication (e.g., cell phone)	☐	☐	☐	☐
242	There is a process for accommodating a patient's request not to use their information for treatment, payment or healthcare operations purposes	☐	☐	☐	☐
243	There are procedures whereby individuals may complain about the covered entity's compliance with its privacy policies and procedures and the Privacy Rule; the procedures are explained in the covered entity's privacy practices notice	☐	☐	☐	☐

[6] http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/

	How are your record privacy practices?	Yes	No	+/-	?
244	The covered entity identifies to whom individuals can submit complaints and advises that complaints can also be submitted to the Secretary of HHS	☐	☐	☐	☐
245	Patients are not required to waive any right under the Privacy Rule as a condition for obtaining treatment, payment, enrollment or benefits eligibility	☐	☐	☐	☐
246	The covered entity maintains copies of its written policies and procedures, notices, complaints and other actions, activities, and designations that the Privacy Rule requires to be documented, for 6 years	☐	☐	☐	☐
247	(more…)	☐	☐	☐	☐

Insurance Inventory Checklist

Every physician is familiar with Professional Medical Liability Insurance (PLI), which covers negligent acts performed in the course of practicing medicine.

*However, many risks falling under the rubric of **cyber liability** do not fit the definition of "medical malpractice," and are not covered by standard med-mal insurance.* Separate insurance policies are available that cover many risks that apply to health information technology and electronic information. Providers and healthcare facilities/organizations should investigate insurance options available to them to help defend claims that can arise from adverse events related to HIT.

In addition, physicians can be exposed to a variety of other legal risks that may be excluded from "standard" professional liability policies.

Not all risks are insurable. For example, HIPAA violations, allegations of fraud/abuse and other charges can be brought against practitioners that expose them to criminal fines and other penalties – *which may not be legally insurable.* In some cases, insurance might cover legal defense costs, but not fines if the defendant is found culpable. Insurance policies exclude deliberate illegal activity. Some policies insure employers from criminal activity by their employees (as long as the employer was unaware).

The following list is for guidance only. It is not comprehensive and does not address numerous terms of coverage and exclusions that differ among carriers and policies.

	What insurance do you need?	Have	Need	Ask
	PROFESSIONAL LIABILITY ("MALPRACTICE")			
248	Professional liability – Individual	☐	☐	☐
249	Professional liability – Group	☐	☐	☐
250	Professional liability – Directors & Officers	☐	☐	☐
251	Errors & omissions – other	☐	☐	☐
	CYBER LIABILITY			
252	Multimedia risks	☐	☐	☐
253	Security & privacy risks	☐	☐	☐
254	Regulatory defense and penalties *	☐	☐	☐
255	Breach response	☐	☐	☐
256	Network asset protection	☐	☐	☐
257	Business interruption	☐	☐	☐

	What insurance do you need?	Have	Need	Ask
258	Cyber extortion/terrorism	☐	☐	☐
	OTHER			
259	General liability	☐	☐	☐
260	Employment practices liability	☐	☐	☐
261	Billing error, fraud/abuse, regulatory defense (EMTALA, HIPAA, STARK, etc.) *	☐	☐	☐
262	Employee criminal acts	☐	☐	☐
263	Fiduciary liability	☐	☐	☐
264	ERISA-required fidelity bond	☐	☐	☐
265	Property & casualty	☐	☐	☐
266	Business continuity	☐	☐	☐
267	Commercial vehicle	☐	☐	☐
268	Workers' compensation	☐	☐	☐
269	Group health	☐	☐	☐
270	Key person life/disability	☐	☐	☐
271	Personal auto	☐	☐	☐
272	Personal umbrella	☐	☐	☐
273	(more…)	☐	☐	☐

* Where insurable

Report an EHR-Related Event

There are statutory requirements for reporting HIPAA-related events. In addition, cyber-liability insurance coverage may have specific reporting requirements for non-HIPAA events (e.g., extortion demands, copyright infringement notices, etc.) Professional liability ("malpractice") insurance may also have requirements for prompt reporting of potential liability events.

- It is critical to report any potential liability exposure to your insurance carrier as soon as it is recognized. This sets the clock on a number of processes for legal and technical mitigation.
- If you have a single-contact for different kinds of events, be sure all practice administrators know who that is.
- If you have agencies to report to besides your insurance carrier (e.g., a Patient Safety Organization), your administrators need to know exactly how and what to communicate to each of them.

Resources for HIT Privacy, Security and Safety

Office of the National Coordinator for Health Information Technology (ONC)

- www.HealthIT.gov
- Mobile devices at HealthIT.gov: http://www.healthit.gov/providers-professionals/how-can-you-protect-and-secure-health-information-when-using-mobile-device
- Security and risk auditing: www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf
- SAFER Guides:

  https://www.healthit.gov/safer/safer-guides

Office for Civil Rights

- Health Information Privacy/HIPAA resources
- http://www.hhs.gov/ocr/privacy/index.html
- Videos on privacy and security specifically for providers.
    - www.youtube.com/watch?v=mX-QL9PoePU (HIPAA Privacy: Final Omnibus Rule)
    - www.youtube.com/watch?v=QWRn2r5R7ts (Security Rule)
    - www.medscape.org/viewarticle/781892?src=ocr (MEDSCAPE CME credit)
    - www.medscape.org/viewarticle/762170?src=ocr (MEDSCAPE CME credit)

The National Institute of Standards & Technology

- A wealth of information available for download about security and the risk auditing process
- http://csrc.nist.gov/
- Guide for Conducting Risk Assessments http://www.nist.gov/manuscript-publication-search.cfm?pub_id=912091

The Agency for Healthcare Research and Quality (AHRQ)

- Standardized reporting formats for patient safety events, including HIT-specific events
- Software and device reporting form: https://www.psoppc.org/c/document_library/get_file?uuid=75912503-7bd1-4e99-a678-5dbb70008e95&groupId=10218
- Hazard Manager: http://healthit.ahrq.gov/sites/default/files/docs/citation/HealthITHazardManagerFinalReport.pdf

ONC SECURITY RISK ASSESSMENT TOOL

- In March 2014, the ONC released a software "Risk Assessment Tool" that can be downloaded by covered entities to help develop their RAs. This is potentially very useful and contains lots of "HELP" and information about definitions, policies and legal requirements. It is tightly aligned with HIPAA and follows the templates provided in other ONC publications. There is a bit of a learning curve, but many users may find this application helpful.
    - There are versions for Windows and iPad: http://www.healthit.gov/providers-professionals/security-risk-assessment-tool
    - User's Guide: http://www.healthit.gov/sites/default/files/risk_assessment_user_guide_final_3_26_2014.pdf

Appendix A: Federal Regulations and References

The Security Rule

The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.[7]

The Security Rule requires Covered Entities (CEs) to conduct a risk assessment to identify risks and vulnerabilities to ePHI. However, "The standard does not dictate how CEs are to perform the risk assessment or provide specific insight into the approach for assessing risk around ePHI."[8]

CMS has published a series of papers that provide guidance to small practices (and also larger organizations) for implementing the Security Rule. The full collection is available from COPIC.

1 – Security 101 for Covered Entities
http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/security101.pdf

2 – Security Standards: Administrative Safeguards
http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf

3 – Security Standards: Physical Safeguards
http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/physsafeguards.pdf

4 – Security Standards: Technical Safeguards
http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf

5 – Security Standards: Organizational, Policies & Procedures and Documentation Requirements
http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/pprequirements.pdf

6 – Basics of Risk Management
http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf

7 – Implementation for the Small Provider
http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/smallprovider.pdf

The Privacy Rule

"The HIPAA Privacy Rule [45 CFR Part 160 and Subparts A and E of Part 164] establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health

[7] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/
[8] CMS Office of E-Health Standards and Services, 2008 HIPAA Compliance Reviews, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/cmscompliancerev08.pdf

care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections."[9]

The Breach Notification Rule

The HIPAA Breach Notification Rule requires "HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC), apply to vendors of personal health records and their third party service providers, pursuant to section 13407 of the HITECH Act."[10]

The Enforcement Rule

"The HIPAA Enforcement Rule [45 CFR Part 160, Subparts C, D, and E] contains provisions relating to compliance and investigations, the imposition of civil money penalties for violations of the HIPAA Administrative Simplification Rules, and procedures for hearings."[11]

[9] http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/
[10] http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html
[11] http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/index.html

Index