The HIPAA Privacy Rule

HIPAA establishes a foundation of Federal protections for Protected Health Information (PHI). HIPAA’s big brother, The Omnibus Rule added new patient right’s, changes in breach reporting and other requirements your practice must understand. Fines can be severe, $10,000 to $50,000 minimum mandatory civil monetary penalties (CMP) for “Willful Neglect”. HIPAA violations carry prison time for workforce members, up to 10 years for the intentional misuse of PHI for personal gain or malicious purposes. A violation of a person’s HIPAA rights is a violation of their constitutional rights and thus HIPAA violations are investigated by the Office for Civil Rights (OCR). The best way to avoid involvement with the OCR is to protect the records you are entrusted with in the same manner you want your personal health records safeguarded. Knowledge is the key to protecting patient privacy and your practice’s reputation. This pamphlet is a concise review of HIPAA Privacy Rules and methods to follow the HIPAA Security Rule.

Each office must assign a HIPAA Privacy Officer and HIPAA Security Officer or a single position, the HIPAA Compliance Officer. Make sure you know your practice’s HIPAA Compliance Officer, how to identify and report a security breach and the basics of the HIPAA Privacy Rule. Knowing the patient’s rights better than the patients is the very best method to avoid Office for Civil Rights (OCR) investigations, audits and compliance reviews.

Key Definitions

Protected Health Information (PHI): 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 when combined with treatment, payment or operations information. Privacy Rule at 45 CFR 164.501 gives the following definitions.

- "Treatment” generally means the provision, coordination, or management of health care and related services among health care providers or by a health care provider with a third party, consultation between health care providers regarding a patient, or the referral of a patient from one health care provider to another.
- "Payment” encompasses the various activities of health care providers to obtain payment or be reimbursed for their services and of a health plan to obtain premiums, to fulfill their coverage responsibilities and provide benefits under the plan, and to obtain or provide reimbursement for the provision of health care. In addition to the general definition, the Privacy Rule provides examples of common payment activities which include, but are not limited to:
  - Determining eligibility or coverage under a plan & adjudicating claims;
  - Risk adjustments;
  - Billing and collection activities;
  - Reviewing health care services for medical necessity, coverage, justification of charges, and the like;
  - Utilization review activities; and
  - Disclosures to consumer reporting agencies (limited to specified identifying information about the individual, his or her payment history,
and identifying information about the covered entity).

- **Health care operations** are certain administrative, financial, legal, and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment. These activities, which are limited to the activities listed in the definition of “health care operations” at 45 CFR 164.501, include:
  - Conducting quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, and case management and care coordination;
  - Reviewing the competence or qualifications of health care professionals, evaluating provider and health plan performance, training health care and non-health care professionals, accreditation, certification, licensing, or credentialing activities;
  - Conducting or arranging for medical review, legal, and auditing services, including fraud and abuse detection and compliance programs;
  - Business planning and development, such as conducting cost management & planning analyses related to managing & operating the entity; &
  - Business management and general administrative activities, including those related to implementing and complying with the Privacy Rule and other Administrative Simplification Rules, customer service, resolution of internal grievances, sale or transfer of assets.

**Minimum Necessary Standard**

The **Minimum Necessary Standard** is a key protection of the HIPAA Privacy Rule. It is based on accessing or disclosing protected health information only when it is medically necessary to satisfy a particular purpose or carry out a function. The minimum necessary standard requires covered entities and business associates evaluate their organization and enhance safeguards that limit unnecessary or inappropriate access to and disclosure of PHI. The Privacy Rule’s requirements for minimum necessary are designed to be sufficiently flexible to accommodate the various circumstances of any business. The Minimum Necessary Standard requires all staff members utilize the same procedures to access their own and/or family and friends PHI in the same manner as patients would be required. When requesting charts from other offices, minimum necessary does not apply, however guidelines suggest you only request the information needed for it’s intended medical purpose.

*Don’t ask for the whole chart if you do not need the whole chart. Just because you have access, does not give you the right to access.*

**Breach:** there is a default presumption that any acquisition, access, use, or disclosure of PHI in a manner not permitted by the HIPAA Privacy Rule is a breach unless the covered entity or business associate “demonstrates that there is a low probability that the [PHI] has been compromised based on a risk assessment.” Document all breaches with the Breach Incident Report and give to the HIPAA Compliance Officer as soon as possible. See page 22 and 23.
Patients’ Rights Under HIPAA

RIGHT # 1 - Right to Access

Updated Information on the HIPAA Privacy Rule as of June 1, 2016

Providing individuals with easy access to their health information (PHI) empowers them to be more in control of decisions regarding their health and well-being. Individuals with access to their health information are better able to monitor chronic conditions, adhere to treatment plans, find and fix errors in their health records, track progress in wellness or disease management programs, and directly contribute their information to research. (Precision Medicine Initiative)

Patient’s Have a Right To Access ALL PHI Maintained by Your Practice

Patients have access to their “designated record set” which includes Medical records and billing records about individuals maintained by or for a covered health care provider; enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or other records that are used, in whole or in part, by or for the covered entity to make decisions about individuals. (See Page 9)

Verification is Required and Must be Documented

The Privacy Rule requires a covered entity to take reasonable steps to verify the identity of an individual making a request for access. Verification by be in written or oral form and must be documented.

Unreasonable Measures

A covered entity may not impose unreasonable measures on an individual requesting access that serve as barriers to or unreasonably delay the individual from obtaining access. For example, a doctor may not require an individual:

1) Who wants a copy of her medical record mailed to her home address to physically come to the doctor’s office to request access and provide proof of identity in person.
2) To use a web portal for requesting access, as not all individuals will have ready access to the portal.
3) To mail an access request, as this would unreasonably delay the covered entity’s receipt of the request and thus, the individual’s access.

The Privacy Rule requires a covered entity to provide the individual with access to the PHI in the form and format requested, if readily producible in that form and format. Where an individual requests an electronic copy of PHI that a covered entity maintains only on paper, the covered entity is required to provide the individual with an electronic copy if it is readily producible electronically, ie you have a scanner. A covered entity is not expected to tolerate unacceptable levels of risk to the security of the PHI on its systems in responding to requests for access; whether the individual’s requested mode of transfer or transmission presents such an unacceptable level of risk will depend on the covered entity’s Security Rule risk analysis.
Patient’s Have A Right to Have Records Emailed To Themselves
Mail and email are generally considered readily producible by all covered entities. If the individual requested that the covered entity transmit the PHI in an unsecured manner (e.g., unencrypted), and, after being warned of the security risks to the PHI associated with the unsecure transmission, maintained her preference to have the PHI sent in that manner, the covered entity is not responsible for a disclosure of PHI while in transmission to the designated third party, including any breach notification obligations that would otherwise be required. Further, a covered entity is not liable for what happens to the PHI once the designated third party receives the information as directed.

Time Limits to Grant Access/Copies
Access to the individual must be provided no later than 30 calendar days from receiving the individual’s request. The 30 calendar days is an outer limit and covered entities are encouraged to respond as soon as possible. Indeed, a covered entity may have the capacity to provide individuals with almost instantaneous or very prompt electronic access to the PHI.

Allowable Fees for Medical Records
The Privacy Rule permits a covered entity to impose a reasonable, cost based fee if the individual requests a copy of the PHI. The fee may include only the cost of:
(1) labor for copying the PHI;
(2) supplies for creating the paper copy or electronic media (USB drive);
(3) postage.

The fee may not include costs associated with verification; documentation; searching for and retrieving the PHI; maintaining systems; recouping capital for data access, storage, or infrastructure; or other costs not listed above even if such costs are authorized by State law. Outsourcing of medical record requests: Administrative and other costs associated with outsourcing the function of responding to individual requests for access cannot be the basis for any fees charged to individuals for providing that access.

Labor for copying includes only: Photocopying paper PHI; Scanning paper PHI into an electronic format; Converting electronic information in one format to the format requested by or agreed to by the individual; Transferring (e.g., uploading, downloading, attaching, burning) electronic PHI from a covered entity’s system to a webbased portal (where the PHI is not already maintained in or accessible through the portal), portable media, email, app, personal health record, or other manner of delivery of the PHI; Creating and executing a mailing or email with the responsive PHI. Covered entities must inform the individual in advance of the approximate fee that may be charged for copies of the PHI. This includes disclosure of costs for paper and electronic records. The following methods may be used.

<table>
<thead>
<tr>
<th>Flat Fee</th>
<th>Actual Costs</th>
<th>Average Costs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Per page fees are not allowed for records provided in digital format: thumb drive, CD. Flat fee is set at a maximum of $6.50 to include postage if records are mailed. You Must Post charges for Medical Records in lobby and/or web site.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Patients’ Right to Direct PHI to 3rd Party

A covered entity must transmit an individual’s PHI directly to another person or entity designated by the individual. The individual’s request must be in writing, signed by the individual, and clearly identify the designated person or entity and where to send the PHI. Written access requests by individuals to have a copy of their PHI sent to a third party are subject to the same fee limitations in the Privacy Rule that apply to requests by individuals to have a copy of their PHI sent to themselves. This is true regardless of whether the access request was submitted to the covered entity by the individual directly or forwarded to the covered entity by a third party on behalf and at the direction of the individual. Where the third party is initiating a request for PHI on its own behalf, with the individual’s HIPAA authorization (or pursuant to another permissible disclosure provision in the Privacy Rule), the access fee limitations do not apply. On behalf of individual – Fee Limitations Apply.

The HIPAA Privacy Rule provides individuals with the right to inspect their PHI held in a designated record set, either in addition to obtaining copies or in lieu thereof, and requires covered entities to arrange with the individual for a convenient time and place to inspect the PHI. There can be no charge for the patient to inspect their records nor may a covered entity charge an individual who, while inspecting her PHI, takes notes, uses a smart phone or other device to take pictures of the PHI, or uses other personal resources to capture the information. If the individual is making the copies of PHI using her own resources, the covered entity may not charge a fee for those copies, as the copying is being done by the individual and not the entity.

Denial of Access - Except in certain circumstances, patients have the right to review and/or obtain copies of their “designated record set”. Patients do not have the right to inspect and copy psychotherapy notes, information that was intended for use in a civil, criminal, or administrative action; and information that cannot be disclosed to an individual under CLIA. Exceptions to the Privacy Rule are divided into two categories, denial without review and denial with review. Denial without Review include the following 5 conditions: 1) psychotherapy notes, 2) when the individual in an inmate in a correctional facility and providing access to information would endanger other inmates or correctional employees, 3) when the individual consented to the withholding of information for a research program and the program is still in progress, 4) when the Privacy Rule does not allow access, 5) when the information was received under a promise of confidentiality and disclosure would reveal the source of the information. Denial with Opportunity for Review by Another Physician include the following:

1) When a healthcare worker determines that the protected health information is likely to endanger the life or physical safety of the individual or another individual, 2) when the information identifies another individual that may be harmed as a result of the disclosure, 3) and when providing access to the protected health information might subject the individual to domestic violence, abuse, or neglect by the personal representative. A note, the standard is the physical endangerment of the patient or another person, extreme mental anxiety by itself does not allow you to deny access.
An important reminder, all requests to inspect or for copies should be documented and maintained for 6 years. This is for your protection.

**Special Notes on Psychotherapy Notes**
To use or disclose psychotherapy notes for most purposes, including treatment, payment and health care operations, a covered entity must obtain specific authorization from the individual that is distinct from any authorization for use and disclosure of other PHI. Individuals are not automatically entitled to have access to psychotherapy notes. Psychotherapy notes must be filed separately from the designated record set.

**RIGHT # 2 - Requested Amendments to Protected Health Information**
The Privacy Rule grants individuals the right to request amendments to their protected health information. Generally, a CE must honor the request unless it has determined that the information is accurate and complete. If the record is deemed to be correct your office can deny this request. You must send the patient a letter stating the reason for the denial. At this point, HIPAA gives the patient a right to submit a brief statement of disagreement allowing them to give the reasons they feel their medical records are not accurate or complete. This information must follow the record and be provided to all providers relying on this information.

**RIGHT # 3 - Right to Request Confidential Communications**
HIPAA states that your practice must accommodate reasonable requests for alternative communications such as mailing to a P.O. Box or only calling the patient on their cell phone. Note: Make sure this information is documented so that billing, appointment setters and others will not send information to the wrong address or call the wrong phone number. Without a process in place your office will most likely violate the patient’s request and risk a complaint with HHS/OCR.

**RIGHT # 4 - Accounting of Disclosures**
Patients have the right to receive an Accounting of Disclosures for the past 6 years. You are not required to provide disclosures for payment, treatment or healthcare operations. These are considered routine disclosures. You must track and disclose upon request all non-routine disclosures such as state mandated reporting, tissue donation purposes, disclosures required by law (victims of crime, gunshot wounds, court ordered warrant, faxing information to the wrong location and any disclosure of patient information outside of “need to know”. You are not required to disclose the following; 1) payment, treatment or healthcare operations; 2) to the individual or their representative; 3) for disaster relief; 4) pursuant to an authorization; 5) a limited data set; 6) national security; 7) correctional institutions or law enforcement for inmates or those in lawful custody; and 8) permitted disclosures. Accounting of disclosures must be temporarily suspended upon written request by oversight agencies or law enforcement if the accounting would impede their activities. Make sure your practice tracks this information in a way it can be easily retrieved and disseminated upon written request. See page 15.
RIGHT # 5 - Restrictions to Protected Health Information
Restriction requests made by patients should be honored when possible, but are not required under HIPAA with one exception. Examples of other requests your office may honor or deny include; a request not to disclose certain parts of the protected health information; requests not to disclose information to certain individuals; and a request not to disclose certain information to other providers involved in the patient’s care. Make sure the request is in writing and that the approval or denial to the patient is documented and sent to the patient. You must honor all requests that the office has approved.

RIGHT # 6 - Right to Restrict Information to their Health Plan
The Omnibus Rule introduced one instance where denial of a patient’s requested restriction is not allowed. When a patient has a service or procedure performed and pays for the service or procedure out-of-pocket and in full the patient can require that your office not disclose this information to their insurance carrier. Be sure to “flag” this file so that it is not inadvertently disclosed during an insurance chart review.

RIGHT # 7 - Right to Receive Notice of Privacy Practices (NPP). Right to File a Privacy Complaint with Your Office or the Office for Civil Rights.
Your patients have a right to know how your practice may use and disclose protected health information. The Omnibus Rule updated this requirement to include the name and information of organizations which you electronically exchange information and additional patient disclosures. Omnibus also requires additional disclosures such as the right to restrict information given to insurance companies if the patient pays cash for the service or procedure. The Notice of Privacy Practices must be distributed no later than the first service in person service encounter. The additions made by Omnibus require that all patients sign that they have received the updated NPP. It is very important that the practice and its employees act in accordance with the information in their notices. There must be no retribution if the patient files a complaint, in fact, you want a patient to file a privacy complaint with your office instead of the Department of Health and Human Services/Office for Civil Rights. NPPs should be posted in a clear and prominent location. A summary of the NPP may be posted if the full NPP is “immediately available” to patients. Update patient notification every 3 years or whenever major changes are made to the NPP.

Health IT.gov Videos on Patients’ Right to Access
https://www.healthit.gov/access

The Health Insurance Portability and Accountability Act, or HIPAA, gives individuals the right to see and get copies of their health information, or share it with a third party, like a family member or a mobile device application. Having easy access to their health information empowers individuals to be more in control of decisions regarding their health and well-being. To help explain this important right to individuals and health care providers, ONC and OCR have developed easy-to-understand educational tools in English and Spanish.
ACCESS - General Right

The Privacy Rule generally requires HIPAA covered entities to provide individuals, upon request, with access to the protected health information (PHI) about them. This includes the right to inspect or obtain a copy, or both, of the PHI, as well as to direct the covered entity to transmit a copy to a designated person or entity of the individual's choice.

We note that a covered entity (or a business associate) may not circumvent the access fee limitations by treating individual requests for access like other HIPAA disclosures – such as by having an individual fill out a HIPAA authorization when the individual requests access to her PHI (including to direct a copy of the PHI to a third party). A HIPAA authorization is not required for individuals to request access to their PHI, including to direct a copy to a third party. Covered entities must take action within 30 days of the request; Covered entities must provide the PHI in the form and format and manner of access requested by the individual if it is “readily producible” in that manner; and The individual may be charged only a reasonable, cost based fee that complies with 45 CFR 164.524(c) (4). If requested by an individual, a covered entity must transmit an individual's PHI directly to another person or entity designated by the individual. The individual's request must be in writing, signed by the individual, and clearly identify the designated person or entity and where to send the PHI. The same requirements for providing the PHI to the individual, such as the timeliness requirements, fee limitations, prohibition on imposing unreasonable measures, and form and format requirements, apply when an individual directs that the PHI be sent to another person or entity.

Designated Record Set

With limited exceptions, the HIPAA Privacy Rule gives individuals the right to access, upon request, the medical and health information (protected health information or PHI) about them in one or more designated record sets maintained by or for the individuals’ health care providers and health plans (HIPAA covered entities). See 45 CFR 164.524. Designated record sets include medical records, billing records, payment and claims records, health plan enrollment records, case management records, as well as other records used, in whole or in part, by or for a covered entity to make decisions about individuals. See 45 CFR 164.501. Thus, individuals have a right to access a broad array of health information about themselves, whether maintained by a covered entity or by a business associate on the covered entity’s behalf, including medical records, billing and payment records, insurance information, clinical laboratory test reports, X-rays, wellness and disease management program information, and notes (such as clinical case notes or “SOAP” notes (a method of making notes in a patient’s chart), among other information generated from treating the individual or paying for the individual’s care or otherwise used to make decisions about individuals. In responding to a request for access, a covered entity is not, however, required to create new information, such as explanatory materials or analyses, that does not already exist in the designated record set. A covered entity is only required to provide access to the PHI to which the individual requests access.
Incidental Disclosure

Every risk of disclosure cannot be eliminated in your office. HIPAA allows for incidental disclosure as long as your organization has implemented reasonable safeguards and applied the minimum necessary standard. Incidental disclosure occurs when a proper disclosure is being made and another patient or staff member not involved in the patient’s care overhears or oversees PHI. The HIPAA Privacy Rule is not intended to impede these customary and essential communications and, thus, does not require that all risk of incidental use or disclosure be eliminated. Rather, the Rules permit certain incidental uses and disclosures of PHI to occur when the covered entity has in place reasonable safeguards with minimum necessary policies and procedures to protect an individual’s privacy. Use additional safeguards when sensitive PHI is involved such as lowering your voice and talking behind closed doors.

SECTION 1557 of the ACA

On May 18, 2016, the Department of Health and Human Services (HHS) published a final rule to implement Section 1557 of the Affordable Care Act (ACA).

Section 1557 is the nondiscrimination provision of the Affordable Care Act (ACA). The law prohibits discrimination on the basis of race, color, national origin, sex, age, or disability in certain health programs or activities. Section 1557 builds on long-standing and familiar Federal civil rights laws.

SECTION 1557

Mandates - Posting Notices of Nondiscrimination and signage explaining the availability of language services in the state's top 15 non-English languages & Using “qualified interpreters” in healthcare scenarios.

Grants - Individuals a private cause of action to sue healthcare organizations that fail to provide language services, based on disparate impact.

Prohibits - Minor children from interpreting except in for short-term emergencies. Adult family/friends from interpreting unless the patient specifically requests it. Healthcare staff from interpreting unless they are qualified and interpreting is an official job duty.

Requires - Provision of “meaningful access to each individual with limited English proficiency eligible to be served or likely to be encountered” from an organization receiving any HHS funding and any HHS-administered health program.
HIPAA Privacy Guide - Communicating with Family & Friends

HIPAA is a Valve, Not a Blockage

OCR GUIDANCE STATES:

**Question:** If a patient does not object, can a health care provider share or discuss health information with family, friends, or others involved in the care or payment for care?

**Answer:** Yes. As long as the patient does not object, a health care provider is allowed to share or discuss health information with family, friends, or others involved in patient care or payment for care. A provider may ask for permission, may tell the patient that he or she plans to discuss the information and give an opportunity to object, or may decide, using his or her professional judgment, that the patient does not object.

In any of these cases, a health care provider may discuss only the information that the person involved needs to know about the patient's care or payment for care.

*Here are some examples:*

- An emergency room doctor may discuss your treatment in front of your friend when you ask that your friend come into the treatment room.
- Your hospital may discuss your bill with your daughter who is with you at the hospital and has questions about the charges.
- Your doctor may talk to your sister who is driving you home from the hospital about your keeping your foot raised during the ride home.
- Your doctor may discuss the drugs you need to take with your health aide who has come with you to your appointment.
- Your nurse may tell you that she is going to tell your brother how you are doing, and then she may discuss your health status with your brother if you did not say that she should not.

**BUT:**

Your nurse may not discuss your condition with your brother if you tell her not to.

**OCR has stated they will not question your professional judgement as to involving family and friends.**
The HIPAA 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 and/or business associate.

Protecting protected health information is each staff member’s job and responsibility. You should always treat the privacy of protected health information as you would want your private medical information guarded and away from public view. Electronic protected health information is the prime target for cyber criminals and organized crime. You must be aware at all times of security policies and procedures that are in place to protect this valuable information. Security of electronic records is 25% IT security measures and 75% employee behavior. Your practice must build a “Culture of Compliance” that protects the confidentiality, integrity, and availability of the protected health information you create and store. This is done through training, policies and procedures and technology.

Security Practices

More than 60% of network malware infections are caused by social engineering.

The organization’s internet and email should only be used for purposes required for the administration of health care. You should not use company internet or email for personal purposes as it greatly increases the likelihood of computer malware (viruses) and data leakage. Absolutely no social media should be accessed unless it is for purposes of marketing the practice and its use should be approved by the HIPAA Compliance Officer.

Downloading software and other files must be approved by the HIPAA Compliance Officer and/or IT professional. This includes all browser add-ons and all executable programs with an (.exe, .bat or others) extension. Never disable the firewall or anti-virus/other protective software on your workstations.

Be aware when using email. Attachments are a common method cyber criminals use to spread malicious code. Should you suspect your computer has been accessed by an unauthorized person or if you suspect malware is on your computer, immediately report this to your HIPAA Compliance Officer.

Passwords are key to security. Passwords must be complex (minimum of 10 digits, upper and lower case letters, at least 2 numbers, and a special character). Never tell others your password, except the HIPAA Compliance Officer, and never write your password down and place it under your keyboard or on your monitor. Treat your user name and password as you would your signature as it legally identifies your access to the computer systems.

Never share your password or User ID, it is your digital identity.
There Is No Privacy Without Security.

Maintain a “Culture of Compliance”.
Always think about security.

Healthcare is Built on Trust.
Complete trust is required or patients may not be fully candid or inform you of all their medical conditions.

90% of All Malware Requires Human Interaction Before It Can Infect.
You are your company’s greatest security risk, knowledge and awareness are the tools that will help maintain your organization’s records in a safe and secure manner. Most hackers do not use sophisticated tools to infiltrate networks. Instead they take advantage of weak security practices. Here are the top 3 proactive security procedures you should employ in the workplace and at home.

Most Hackers Are Opportunists

1. Have a Strong Password. Make sure you use a strong password (i.e. usually 10 characters or more and includes uppercase and lowercase letters, numbers, and special characters like #$&*). Recent research suggests users could also consider using “passphrases,” which are sentences that may be easier to remember than a very complex password (e.g. “I got a pony for my 8th birthday!”) Do not use passwords or phrases that would be easy to guess, such as a pet’s name or your birthdate. See page 14 for tips on building a complex password.

2. Use Caution When Opening Email Attachments and Clicking on Hyperlinks. Always verify the return email address. If it feels suspicious do not open the attachment or click the hyperlink. If you are not expecting an attachment from the email sender, do not open unless you have verified it was sent by that person. Cyber criminals are using very complex and targeted email attacks. The rule, always be suspicious if the email contains an attachment or hyperlink.

3. Any use of the internet is a risk to your organization. Using the internet is about risk management. The office needs to verify insurance, look up other providers and many other useful and productive needs. Even though there is risk, it is reasonable and necessary risk. Unnecessary risk is using the organization’s internet access for personal uses such as shopping, social media and other non-business access. Cyber criminals target legitimate web sites so that one wrong click and your computer is infected and patient information is at risk. Use your own personal device, not connected to the organization’s wifi, to do your personal web browsing.

HIPAA is always being updated, make sure you stay aware of current requirements, rules and regulations that affect your organization.
Create Strong/Complex Passwords (from Microsoft Website)

Passwords are the first line of defense against break-ins to your online accounts and computer, tablet, or phone. Poorly chosen passwords can render your information vulnerable to criminals, so it’s important to make your passwords strong.

To help you create strong passwords, follow the same network security guidelines required of all Microsoft employees:

Strong/Complex passwords are phrases (or sentences)
1) at least ten (10) characters long—longer is better—
2) that include at least three of the following: uppercase and lowercase letters, numerals, punctuation marks, and symbols.

Give passwords the thought they deserve, and make them memorable. One way is to base them on the title of a favorite song or book, or a familiar slogan or other phrase.

Example phrases: I love my new Xbox One

Example passwords: Ilove!mynewxbox1

Variety. Don’t use the same password for everything. Cybercriminals steal passwords on websites that have very little security, and then they use that same password and user name in more secure environments, such as banking websites. There are many ways to create a long, complex password. Here are some suggestions that might help you remember it easily:

Avoid creating passwords that use:
• Dictionary words in any language.
• Words spelled backwards, common misspellings, and abbreviations.
• Sequences or repeated characters. Examples: 12345678, 222222, abcddefg, or adjacent letters on your keyboard (qwerty).
• Personal information. Your name, birthday, driver’s license, passport number, or similar information.
• Avoid reusing passwords.

Most Common Passwords of 2016

123456    passw0rd    1234567
password   123456789  baseball
12345678   football   welcome
qwerty     starwars   letmein

Use Rules that apply to all passwords you create.
Example: Capitalize every 4th letter and turn every "e" into a "?".

Check password strength
http://www.passwordmeter.com/ or https://howsecureismypassword.net/
HIPAA Quick Reference Guide

Accounting of Disclosures
The Privacy Rule requires covered entities and business associates to make available, upon written
request, an **Accounting of Disclosures** of the individual’s PHI made in the six years prior to the request
(45 C.F.R. § 164.528). An accounting must include all disclosures of PHI, except for certain specifically
excluded disclosures (including disclosures to carry out treatment, payment and health care operations
(TPO) under 45 C.F.R. § 164.506). The Accounting of Disclosures provision applies to disclosures of
paper and electronic PHI, regardless of whether the information is contained in the designated record set.

**The following types of disclosures must be tracked:**
- Reports of child abuse, neglect, or domestic violence;
- Any disclosure required by law (state encounter data, infectious disease reporting, etc.);
- Disclosures to funeral directors, coroners, and medical examiners;
- Disclosures in accordance with a judicial subpoena;
- Public health activities (births, deaths, public health investigations, adverse events, work related injuries, FDA required reporting, etc.);
- Health oversight activities (audits and investigations by Government);
- Specialized government functions (law enforcement custodial situations);
- Disclosure for certain law enforcement purposes (identification of a suspect or missing person, identification of a crime victim, suspected crime, etc.);
- Disclosures to organ procurement and banking organizations;
- Disclosures to a third party when the safety of an individual is at risk;
- Workers’ compensation disclosures;
- “Breaches” of patient information such as Disclosures made in error.

**Standard accountings must include:**
1. Date of disclosure;
2. Name of the recipient, and address if known;
3. Brief description of the PHI disclosed;
4. Brief statement of the purpose of the disclosure that reasonably informs the individual of
   the basis for disclosure, or a copy of the request for the disclosure.

There can be no charge for the first Accounting of Disclosures requested. You can charge reasonable
fees for Accountings requested within 12 months of the initial request.

**Employees Should Know That All Covered Entities Must:**
- Encrypt all email containing PHI. Exemption is sending email to patients after they are given a "light warning" as to confidentiality risks of unsecured email.
- Have policies & procedures limiting the use of the internet to work purposes only.
- Have a Sanctions Policy and Document All HIPAA Violations.
  - Abide By The Minimum Necessary Standard.
  - Restrict Your Access Based On Job Function.
  - Document all “Breaches” of PHI. (See Pages 22 & 23)
  - Train Staff Yearly on HIPAA.
  - Provide Security Reminders Throughout Year.
  - Enforce Strong Password Policies.
  - Review and Report on All Access to Patient Information (audit logs) by Individual User ID.
  - Develop a “Culture of Compliance” for the office.
This Is A Ransomware Email That Has Made Cybercriminals Millions of Dollars

Think Before You Click!

Problem with parcel shipping, ID:00000102090
FedEx Ground <arnold.montgomery@giani-media.com>
Sent: Wed 10/5/2016 3:49 AM
To: mm@hpacompliancekit.com

Message 1 FedEx_00000102090.zip (5 KB)

Also beware .exe and .bat. Remember, bad things can be attached to .pdf and Word documents.

Dear Customer,

We could not deliver your item. Shipment Label is attached to email.

Yours sincerely,
Arnold Montgomery,
FedEx Operation Manager.

Beware emails with hyperlinks in the body of the email. They most likely will send you to a web site that will download malicious software without your knowledge.

Review All Emails Containing Attachments

1. Look at the return email address, does it match the Business Name?
2. How did the sender get my email address?
3. Never open a .zip file contained as an attachment in an email. Other extensions you should not open: .exe, .bat.
4. They have my email address, but do not know my name or Company Name?
5. This is a common greeting on phishing attacks coming from outside the U.S.
6. A comma after the name is not how most of us sign an email.
7. Note Operation, not Operations Manager and the period at the end.

Also look for misspelled words.
HIPAA Quick Reference Guide

**Reasonable Safeguards to Protect Protected Health Information**

…Lower your voice when discussing patient information.

…Do not discuss patient information in public areas including hall ways.

…Do not view your own medical record or those of family and friends without proper authorization.

…Dispose of protected health information in designated shredding bins.

…Verify fax numbers and requestor before sending PHI.

…Do not remove PHI from the facility without written authorization.

…Report suspicious activity, never click on suspicious links.

…Do not install software (screen savers, etc...) without written approval.

…Avoid connecting to untrusted or unknown wireless networks and never access or transmit PHI through unsecured public WiFi locations.

…Never go on Facebook or other social networks at the office and do not disclose patient information over the internet.

…Never attach a thumb drive or cell phone to your workstation’s USB port without authorization from the HIPAA Compliance Officer.

…Always use a fax cover sheet containing a confidentiality statement and the office telephone number when faxing patient information.

…Never release information over the phone without performing due diligence to ensure you are talking to the correct person and they are authorized to receive the patient’s information. (Ask for identifiers, call the patient back on the phone number listed in their file, etc.)

…Do not store documents with PHI on your workstation or mobile device.

…Do not text or email sensitive patient information over unencrypted networks.

…Use the Win Key/L to lock your computer when you leave your station.

…If something makes you suspicious, report it immediately.

…Be on the lookout for Medicare Fraud and Abuse, report to Compliance Officer.

…Take care of the patient information you are entrusted with in the same manner as you would want your own private medical records handled.

…Never access your personal email from the office network/computer.
AWARENESS TRAINING - RANSOMWARE

Ransomware locks up data files with encryption, a method of making our access to data impossible without having for the encryption key. Cybercriminals demand a “ransom” for the key. Our practice suffers downtime, loss of financial resources and patients’ trust that our office is properly securing medical records.

Training and Awareness are keys to our practice preventing a successful ransomware attack. Even with security measures such as our firewall, anti-virus and other network protections, your actions can expose our systems to ransomware and other malicious software. It is the policy of our practice to ensure all workforce members are properly trained on how to avoid malicious software. It is the policy of our practice, to help insure the protection of patient records, that all workforce members will adhere to the following procedures:

If you do not understand any of these procedures ask our HIPAA Compliance Officer about its proper implementation in our office. Violation of any of the above will lead to Sanctions per the HIPAA Security Rule.

1. Never click on an update link that pops up on your computer. Common pop-ups are Adobe, Java, Windows and Anti-Virus updates. Inform IT or your supervisor. Other common pop-ups are from the US Department of Justice or Cybercrime Division. Do not click on these screens, contact IT or your supervisor.
2. Never disable the anti-virus on your computer.
3. Do not install software, such as a screensaver, on your computer without written authorization from the HIPAA Compliance Officer.
4. Never disable the Windows firewall on a workstation.
5. Never unplug or otherwise disable any of the networking devices in the equipment room such as the router or firewall.
6. Do not connect your cell phone or other personal device to your computer using the USB port. (Do not charge your mobile device using a USB cable.
7. Never surf the internet or use the internet for non-work purposes.
8. Never check your personal email from your office computer.
9. Do not connect your personal mobile device to the organization’s wireless network without written approval from the HIPAA Compliance Officer.
10. Do not give out/share your User ID & Password.
11. Always use Complex Passwords, eight characters using upper and lower case to include at least two numbers and one special character (!, ? or $).
12. Change all passwords at least every 90 days.

EMAIL is the most common method of Ransomware Attacks; it is the policy of our practice to implement the following precautions when using email:

13. Verify return email address by putting the cursor over the email address and check to make sure it is the same address showing on the email.
14. Check the return address to the letter. Example: localhospital.com is not localhospital.com
15. Do Not click on a hyper link or download an attachment unless you were expecting the attachment or you have verified with the sender that they sent the attachment. **Think Twice Before Clicking.**
16. Do not download attachments with extensions such as .zip, .exe or .bat .
17. If you do download a file, immediately check the file to ensure it has the proper extension. Example, for a PDF the extension is .pdf.

**Social Engineering attacks play on your emotions and trick you into breaking our policies and procedures to gain access to the network. Use the following procedures to guard against these attacks:**
18. Avoid clicking on links for “free” stuff or that may entice you with fear, urgency, curiosity or sympathy. Examples would be photos of a natural disaster, fund raising after a terrorist attack or free lunch for filling out a survey.
19. Do not follow requests for actions that require you to call a number where they ask for your User Name and Password. Criminals can make the caller ID look as though the caller is from your IT company or any other vendor. Never give out practice information or Passwords over the phone.
20. Use Common Sense, if it looks too good to be true, it probability is.
21. Stop and think what is being asked of you. How did they get my phone number, email address? Would the IRS call me or send me a letter? (The IRS will always send you notification of any action by mail.)

**Signs that your computer/network has been infected include the following:**
- a. You can no longer find or access files on your computer;
- b. A noticeable slowdown of your computer;
- c. Realization that a link or file attachment opened or website visited may have been malicious in nature.

**Immediately upon realization that your computer is infected or you suspect your computer to be infected perform the following in order:**
1. Unplug the power cable of your computer;
2. Unplug the network cable of the computer;
3. Inform your supervisor or IT department/vendor;
4. All staff will need to change passwords immediately.
Sensitive Protected Health Information (sPHI) includes:

- Psychotherapy Notes (which are not part of the official medical record)
- Information about a Mental Illness or Developmental Disability
- Information about HIV/AIDS Testing or Treatment (including the fact that an HIV test was ordered, performed or reported, regardless of whether the results of such tests were positive or negative)
- Information about Communicable Diseases
- Information about Venereal Disease(s)
- Information about Substance (i.e., alcohol or drug) Abuse
- Information about Genetic Testing
- Information about Child Abuse and Neglect
- Information about Abuse of an Adult with a Disability
- Domestic Abuse/Violence
- Information about Sexual Assault
- Information about Artificial Insemination

Additional Protections for sPHI:
Even though a patient may have agreed to have a family member present when you are discussing the patient’s general health, you should always check with the patient before discussing highly confidential information in the presence of family and/or friends.

While a patient may have given you permission to leave messages on an answering machine, you should never leave a message asking the patient to return a call concerning sPHI.

Never Respond to a Subpoena Request without Notifying the Patient if the Subpoena Does Not Have A Valid Authorization, Notice of Production (NOP) or Judge’s Signature.

Subpoena with Authorization Form: You must verify that the Authorization Form has all nine required elements. These records are on behalf of the patient so the new fee schedule applies. See Page 21.

Subpoena with Notice of Production. Clearly stated within the Subpoena will be a statement that the attorney has given the patient notice that they would be requesting their medical records and that within the legally allowed time frame no objection has been filed by the patient. You are then allowed to release the records without a Valid Authorization Form. (It is good practice to verify any Subpoena request with the patient before releasing records.)

Court Order. How will you know it is a Court Order to release a patient’s medical records, it will have a Judge’s signature or stamp. Follow the instructions to the letter or you may be called before the Judge.
Authorization forms must contain the Nine Authorization Elements required by the Privacy Rule.

_These elements are:_

1. description of the information to be used or disclosed.

2. a description of each purpose of the requested use or disclosure. The statement “at the request of the individual” is a sufficient description of the purpose when an individual initiates the authorization.

3. name or other specific identification of the persons or class of person(s) authorized to make the requested use or disclosure.

4. name or other specific identification of the person(s) or class of persons to whom the covered entity may make the requested use or disclosure.

5. an expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure.

6. state that the information used or disclosed pursuant to the authorization may be subject to re-disclosure by the recipient and no longer be protected by the Privacy Rule.

7. the signature of the individual and a date.

8. notify the individual of the right to revoke the authorization and the process for so doing. Notify the individual that a revocation will not effect action already taken in reliance on the authorization form.

9. notify the patient that a provider may not condition treatment on the patient signing the authorization form. (Please note: different rules apply if the use or disclosure is for research-related treatment or PHI created for use by a third party).

**REMEMBER:** Sensitive Protected Health Information requires an additional action by the patient before disclosing the information, even if the patient authorizes the entire file be sent to another office or third party.
Breach Notification Requirements

At the recent HIPAA Security Conference it was said that “if you sneeze it’s a breach and you have to report it to everybody.” That sounds accurate and the best advice in today’s security breach environment.

Identifying a Breach.
If you think it’s a breach, it is a breach. Really, HIPAA defines a suspected breach as an actual breach until your organization performs a Breach Security Risk Assessment and determines that no breach occurred.

HIPAA Omnibus Definition of a Breach
A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information. An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised.

As a workforce member it is your responsibility to ensure that any disclosure of patient information that is not allowed by the HIPAA Omnibus regulations is documented and reported to your HIPAA Compliance Officer. Unless there is a patient emergency, reporting a breach is your top priority. Immediate response can help your organization mitigate any harm the breach could cause and may reduce the number of patient records disclosed.

Common Breaches That Must Be Reported
Faxing PHI to the incorrect fax number or doctor’s office.
Giving an Encounter Summary or other patient records to the wrong patient.
Mailing PHI to the incorrect address & it is returned with evidence it was opened.

3 HIPAA Exceptions To Reporting (May not be allowed by State Law)
1. The first exception applies to the unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or business associate, if such acquisition, access, or use was made in good faith and within the scope of authority.
2. The second exception applies to the inadvertent disclosure of protected health information by a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the covered entity or business associate, or organized health care arrangement in which the covered entity participates. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule.
3. The final exception applies if the covered entity or business associate has a good faith belief that the unauthorized person to whom the impermissible disclosure was made, would not have been able to retain the information.

Report, Report, REPORT.

REMEMBER: Check Your State Law for Breach Notification Requirements.
HIPAA Quick Reference Guide

Breach Documentation Requirements

**Medical Practice**

**BREACH Security Risk Assessment & LoProCo Determination**

**Person Making Report:** Click here to enter text.

**Breach Reported By:** Workforce Member of Organization

**Date Breach Known or Suspected:** Click here to enter a date.

**Date the Breach Occurred (If Known):** Click here to enter a date.

**Case Number Assigned (Optional):** Click here to enter text.

Under the final rule, breach is defined as “an acquisition, access, use, or disclosure of protected health information in a manner not permitted...[and] is presumed to be a breach, unless the covered entity can demonstrate that there is a low probability that the PHI has been compromised (emphases added).” According to HHS, “breach notification is necessary in all situations except those in which the covered entity or business associate, as applicable, demonstrates that there is a low probability that PHI has been compromised.”

Mark all types of PHI involved: □ Paper PHI □ Electronic PHI □ Sensitive PHI □ Verbal PHI

**Number of records involved in breach:** Click here to enter text.

**RISK ASSESSMENT**

1. What was the nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification? (Could this information be used by an unauthorized recipient to further his own interests? Could it be re-identified relatively easily? Would it facilitate Identity Theft (SSN, credit card #, etc.?)?

**Identifiers:**

- Account Numbers
- Date of birth
- Fax Numbers
- Email Address
- Social Security Number
- SSN – Last #
- Health Plan Numbers
- Account Numbers
- Certifications/License #
- Vehicle Identifiers
- URLs
- IP Address
- Biometric identifiers
- Full Face Photos
- Unique identifying #
- Geographical (Address)
- Dates
- Medical Record #
- Other: Click here to enter text.

**Payment or Treatment Information:**

<table>
<thead>
<tr>
<th>Treatment</th>
<th>Click here to enter text.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payment</td>
<td>Click here to enter text.</td>
</tr>
<tr>
<td>Healthcare Operations</td>
<td>Click here to enter text.</td>
</tr>
</tbody>
</table>

2. Who was unauthorized person who used the protected health information or to whom the disclosure was made? (is the recipient already obligated to protect PHI? Is recipient trustworthy? Identification also helps as mitigation—the recipient is already on the radar if the data is later misused.)

**Organization/Person/Staff Member Involved:** Choose an item.

**Name of Person:** Click here to enter text.  

**HIPAA Covered Entity? ---**

3. Was the protected health information actually acquired or viewed? Recovery of a lost laptop with PHI would present potential compromise. If forensic analysis shows the laptop was not accessed since prior to its loss, there is no actual compromise. PHI fixed to an individual would present an actual compromise. If recipient claims “I didn’t read it,” the weight that is given in consideration will depend on the trustworthiness of the individual (42).

**Answer: Yes**

**Describe nature of review:** Choose an item.

4. To what extent has the risk to the protected health information been mitigated? Recipient returns document and states he did not view it. A letter of attestation and/or a Non-Disclosure Agreement may prove useful as mitigating factors. Encryption as mitigation—YES! Must meet encryption standards. There is no “encryption-equivalent” available for paper documents.

**List:** Choose an item.

**List Additional Mitigation:** Click here to enter text.

List any attachments: (copy of PHI data, letters, depositions, attestations)

Click here to enter text.
REMEMBER
“HIPAA should not get in the way of the best interests of the patient.”
Office for Civil Rights

HIPAA Training Checklist

Our HIPAA Compliance Officer is: ____________________________________________.

I understand I am not allowed to access my own/family friends chart without prior approval from the HIPAA Compliance Officer.

I understand that if a Breach occurs that I must complete the Breach Security Risk Assessment and immediately give it to the HIPAA Compliance Officer.

I will apply the “Minimum Necessary Standard” to all uses and disclosures of patient information.

I have read this edition of HIPAA Essentials and understand the information contained.

Signature: ________________________________________________________________

Name Printed: _____________________________________ Date: ______________