HIPAA in 30

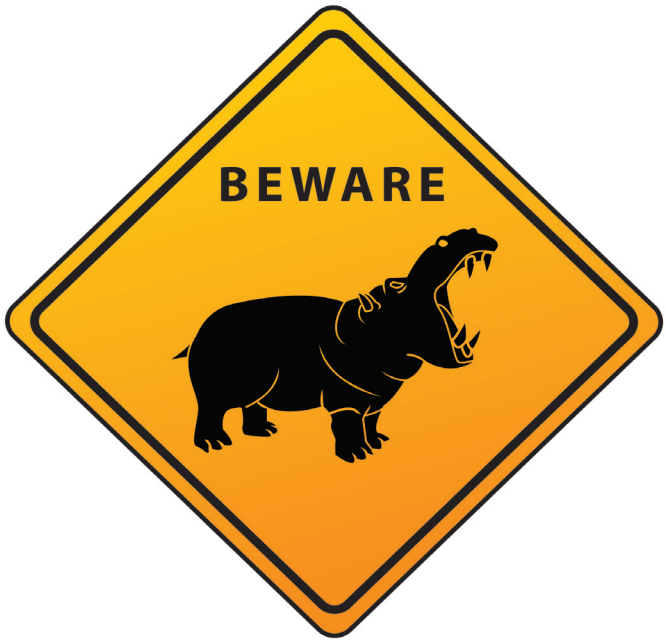
1 HIPAA is Federal Law
composed of the:
HIPAA Privacy Rule
HIPAA Security Rule
Breach Notification Rule
These rules and regulations carry significant fines and penalties for practices & individual staff members.

2 HIPAA Protects PHI
Protected Health Information. PHI is any oral, written or electronic individually-identifiable health information collected or stored by a HIPAA covered entity. PHI consists of at least one identifier matched with TPO. (Treatment, Payment or Health Care)

3 Minimum Necessary
The Minimum Necessary Standard, a key protection of the HIPAA Privacy Rule. It is based on sound, current practice that protected health information should not be used or disclosed when it is not necessary to satisfy a particular purpose or carry out a function.

4 Permitted Disclosures
A covered entity is permitted, but not required, to use and disclose protected health information, without an individual's authorization for purposes of Continuity of Care.

5 Right of Access
Patients have a right to access their entire designated record set, pay lower fees for records, get records in digital format, be verified over the phone for medical records requests and to access directly upon request.



6 Medical Records
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.

7 Medical Records Pricing
Patients can be charged a flat fee, up to $6.50 or the Practice needs to use a worksheet showing how the price was calculated using the HIPAA allowable charges.

8 Digital Format
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 or as otherwise agreed to by the covered entity and individual.

9 Emailing Required
Email is a digital format that can be requested by patients. Mail and e-mail are generally considered readily producible by all covered entities. It is expected that all covered entities have the capability to transmit PHI by mail or e-mail.

10 Verification
The Privacy Rule requires a covered entity to take reasonable steps to verify the identity of an individual making a request for access. Verification may be done orally. You need to document the request.

11 Direct Access
Patients have a right to see their medical records directly as you see them in the EHR. They can take photos of the screen. No charge can be applied for this access and you must accommodate within 30 days.

12 Denial of Access
Patients do not have a right to access their psychotherapy notes. Other denial can be applied for harm and other exemptions. Denials are divided into denial without review and denial with review.

13 Request to Amend
Individuals have the right to have covered entities amend their protected health information in a designated record set when that information is inaccurate or incomplete. If you agree, make the amendment, if you disagree, send a letter why you disagree.

14 Confidential Contact
Health care providers must permit individuals to request an alternative means or location for receiving communications of protected health information by means other than those that the covered entity typically employs.

15 Restrictions of PHI
A covered entity must agree to a request to restrict disclosure of PHI about the individual to a health plan if the individual has paid the covered entity in full."

16 Disclosures to Family
friends and caregivers. HIPAA allows health care professionals to disclose some health information without a patient's permission under certain circumstances.
Ask Permission
Give Opportunity to Object

17 Accting of Disclosures

Individuals have a right to an accounting of the disclosures of their PHI by a covered entity or the covered entity's business associates. All disclosures outside of TPO must be disclosed from the past 6 years. No charge is allowed.

18 Notice Privacy Practices

CE's must provide a Notice of its Privacy Practices. The notice must describe the ways the CE may use & disclose PHI. The notice must state the CE's duties to protect privacy, provide a notice of privacy practices, & abide by it's terms.

19 HIPAA Security Rule

The Security Rule sets the standards of security controls all CEs and BAs must follow. The rule is flexible to allow different size entities to enact security that is reasonable and appropriate. It all starts with your Risk Analysis and Risk Management Plan.

20 Healthcare Cybersecurity

Awareness is the key to protecting your valuable data. All staff members need to be trained on common cybersecurity tatics such as phishing email and other social engineering techniques.

21 Phishing Email

Cybercriminals target your practice with email that has malicious links and/or attachments. Learn to check the return email address to make sure it matches the sender's address. Do not multi task when reviewing email. Pay attention to what you click.

22 Social Engineering

Taking advantage of human behavior is the social engineer's tool. Trust but verify. When talking to anyone over the phone, know who you are talking to. Be limited with the information you give out and never give out your password over the phone.

23 Complex Passwords

Weak, non-complex passwords allow cybercriminals to guess your password with super fast computers. Make sure your password is 10 characters in length, uses upper and lower case letters, at least two numbers and a symbol. Example: w1tty@pPl71eAxe

24 Password Protections

Change your passwords every 90 days. Make sure you are using complex passwords to 1) log into your computer, 2) to log into software containing PHI and 3)do not forget email. Cybercriminals go after email to learn what attacks will work against your practice.

25 Limit Internet Usage

The Internet is infected with malicious web sites. Land on one of these sites and your practice is compromised within a 1/2 second. Use the internet for work purposes only. Never access your personal email from a work computer, it's too dangerous.

26 Sending Email

Email must be encrypted if it contains any PHI. The only exception is when it is sent directly to the patient after the patient has been warned of the danger and the warning is documented in the email. No patient signature required.

27 HIPAA Breach

Any impermissible acquisition, access, use or disclosure of unsecured PHI is presumed to be a breach. Sending PHI to the incorrect physician's office or giving a patient another patient's discharge summary. Both must be documented with a Breach Risk Assessment.

28 Breach Risk Assessment

4 Questions Required by Federal Law. 1. What were the identifiers and TPO involved? 2) Who was the unauthorized disclosure made to? 3) Was the PHI actually viewed or acquired? 4) To what extent has the risk been mitigated?

29 Incidental Use

HIPAA does not require every risk of an incidental use or disclosure of PHI be eliminated. A use or disclosure that occurs as a result of, or as "incident to," a permitted use or disclosure is permitted. Reasonable safeguards & Minimum Necessary required.

30 Privacy vs. Care

HIPAA is a balance, providing good health care while maintaining the patient's privacy is your responsibility. Use your professional judgment, common sense and error towards providing the best patient care. Always document HIPAA concerns for your HCO.