HIPAA :
Health Insurance Portability and Accountability Act

Health Insurance Portability and Accountability Act (HIPAA) of 1996

This Act was established in 1996, to insure privacy and protection of personal information to the healthcare consumer. The HIPAA privacy rule protects from unauthorized disclosure of any personal-identifiable health information that pertains to a consumer of healthcare services.

PHI-Protected Health Information is considered to be any personally identifiable information in a health care environment, this includes electronic or paper or oral formats.

Five HIPAA Rules

HIPAA Security Rule
Standards to safeguard ePHI.

HIPAA Enforcement Rule
How investigations are completed

Breach Notification Rule
60 days to notify HHA

HIPAA Omnibus Rule
Mereges Hightech rules with HIPAA rules.

HIPAA Privacy Rule
PHI Disclosure Rule

HIPAA Privacy Rule:

The Privacy Rule dictates how, when and under what circumstances PHI can be used and disclosed. Enacted for the first time in 2003, it applies to all healthcare organizations, clearinghouses and entities that provide health plans. Since 2013, it has been extended to include Business Associates.

The Privacy Rule sets limits regarding the use of patient information when no prior authorization has been given by the patient. Additionally, it mandates patients and their representatives have the right to obtain a copy of their health records and request corrections to errors. CEs have a 30-day deadline to respond to such requests.

HIPAA Security Rule:

The Security Rule sets the minimum standards to safeguard ePHI. Anybody within a covered entity or business associate who can access, create, alter or transfer ePHI must follow these standards. Technical safeguards include encryption to NIST standards if the data goes outside the company's firewall. Physical safeguards may relate to the layout of workstations (e.g. screens cannot be seen from a public area), whereas administrative safeguards unite the Privacy Rule and the Security Rule. They require a Security Officer and Privacy Officer to conduct regular risk assessments and audits. These assessments aim to identify any ways in which the integrity of PHI is threatened and build a risk management policy off the back of this.

Breach Notification Rule:

The Department of Health and Human Services must be notified if a data breach has been discovered. This must be within 60 days of the breach's discovery for incidents involving 500 or more individuals, and within 60 days of the end of the calendar year in which the breach was experienced for breaches of fewer than 500 records. Individuals whose personal information has been compromised must also be informed within 60 days, and if more than five hundred patients are affected in a particular jurisdiction, a media notice must be issued to a prominent news outlet serving that area.

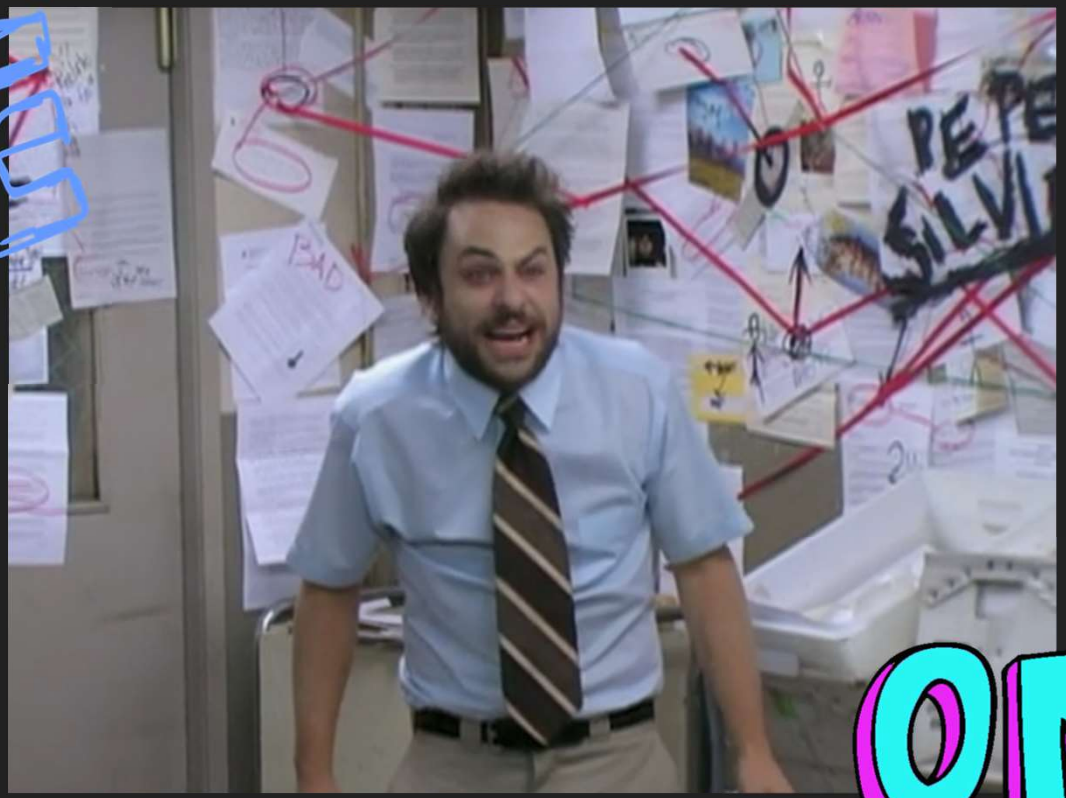
Omnibus Rule:

The Omnibus Rule activated HIPAA-related changes that had been part of the HITECH Act. These included the extension of HIPAA coverage to BAs, the prohibition of using PHI for marketing or fundraising purposes without authorization and new penalty tiers for violations of HIPAA. Part of those penalties can be retained by OCR to fund more stringent investigations of data breaches and complaints of noncompliance.

Enforcement Rule:

Should a breach of PHI occur, this rule lays out how any resulting investigations are carried out. Once the level of negligence has been determined, appropriate fines can be issued. For example, if it is determined that the violation was due to ignorance, a fine of up to $50,000 can be levied against the negligent party per violation with an annual maximum of $25,000 for violations of an identical provision. If the violation was because of willful neglect and was not rectified within 30 days, a fine of $50,000 per offence is possible up to an annual maximum of $1,500,000 for violations of an identical provision.

Trying to understand HIPAA



To make a LOOOOOOOONG story SHORT……


It is the
LAW!!

HIPAA Compliance

The main takeaway for HIPAA compliance is that any company or individual that comes into contact with PHI must enact and enforce appropriate policies, procedures and safeguards to protect data. HIPAA violations occur when there has been a failure to enact and enforce appropriate policies, procedures and safeguards, even when PHI has not been disclosed to or accessed by an unauthorized individual.

If you work in healthcare or are considering doing business with healthcare clients that requires access to health data, you will need to know what is considered protected health information under HIPAA law. The HIPAA Security Rule demands that safeguards be implemented to ensure the confidentiality, integrity, and availability of PHI, while the HIPAA Privacy Rule places limits the uses and disclosures of PHI.

PHI (Protected Health Information)

PHI-Protected Health Information is considered to be any personally identifiable information in a health care environment, this includes electronic or paper or oral formats.

1. Names (Full or last name and initial)
2. All geographical identifiers smaller than a state, except for the initial three digits of a zip code if, according to the current publicly available data from the U.S. Bureau of the Census: the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000
3. Dates (other than year) directly related to an individual
4. Phone Numbers
5. Fax numbers
6. Email addresses
7. Social Security numbers
8. Medical record numbers
9. Health insurance beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers (including serial numbers and license plate numbers)
13. Device identifiers and serial numbers;
14. Web Uniform Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger, retinal and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code except the unique code assigned by the investigator to code the data

PHI is any health information that can be tied to an individual, which under HIPAA means protected health information includes one or more of the following 18 identifiers. If these identifiers are removed the information is considered de-identified protected health information, which is not subject to the restrictions of the HIPAA Privacy Rule.

Simply PHI is any personal information that can identify or potentially identify any individual.

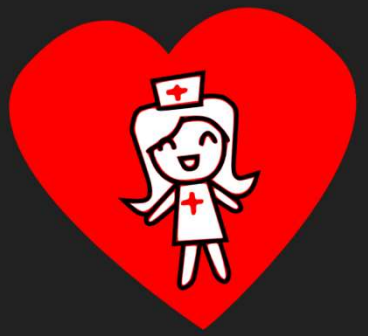
Essentially everything is PHI in our clinics, we will protect the patient's health information and corresponding items to the fullest of our ability.

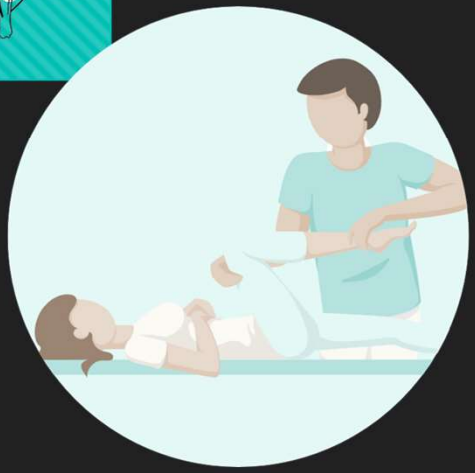
Treat PHI like we treat gold at Fort Knox

FORT KNOX

Who is a covered entity?

A Covered Entity is anyone who provides treatment, payment and operations in healthcare. According to the U.S. Department of Health & Human Services (HHS) Healthcare Providers, Health Plans, and Healthcare Clearinghouses are all Covered Entities. Healthcare Providers include hospitals, doctors, clinics, psychologists, dentists, chiropractors, nursing homes, and pharmacies. As well as any business associate that may have access to PHI.





HIPAA Law & Violations

We may violate HIPAA without even knowing so……..

It is IMPORTANT we are aware of the letter **and** the spirit of the law.

Here is precautions we as a company take to ensure our Clinics are safe:

Maintain a high level of cyber security::

- All clinic servers are secured to prevent Hackers exposing any PHI.
- We have an IT company who has set up our servers to be HIPAA compliant.
- They monitor 24/7 to ensure our patients PHI is secure at all times.

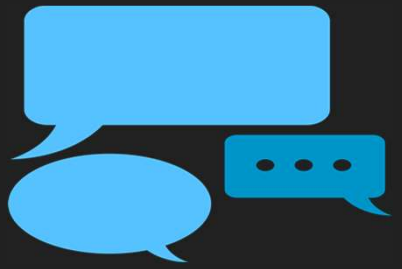
Annually conduct HIPAA trainings for all staff and providers.

We have established protocol for any HIPAA breach, or violation.

Unauthorized search for PHI

Using Names on unsecure platforms Sending a text, a Slack or any communication means:

- Texting the FOC about Big Foot's issue with his bunion on his right foot.



- Looking up a person because you think you know them or curious to see what they are coming in.

Example: Henry saw The Dalai Lama being admitted in the ER. He is wondering why he came in so he looks up him in the hospitals EHR and reads the chart notes.

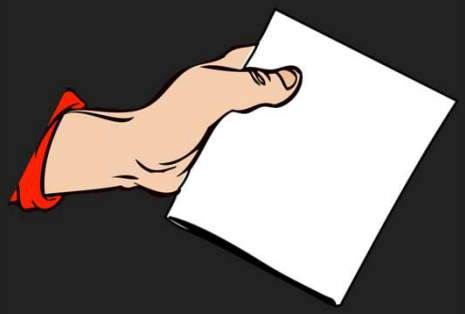
- Going into a family or friend's chart to look up any information.

Example: Sally an employee at Creaking Door Chiropractic's looks in her husband Jack's account to see if he paid his balance.

Employees & Providers disclosing information

- Staff or Providers talking about a patient's PHI out loud so everyone can hear.

Example: Dr. George brings back Samuel L Jackson back for a consult and starts to go over his symptoms and issues in the lobby where it is full of patient's waiting to be seen.



- Accidentally sending / emailing / facing / handing paperwork for a patient and it is the wrong patient,

Example: Dr. Wil hands Jimmy John an Rx for a back brace BUT he handed him Mr. McAlister's Rx for an MRI.

- Employees' having documents or computer screen with visible PHI.

Example: Processing a fee sheet for Deadpool and Wolverine walks up and sees Deadpool's name and knows he is in the clinic.

Employees & Providers disclosing information

- Staff or Provider talking about a friend or family member to another patient.

Example: The front desk is checking in Jane Doe and mentioning to her we just saw her daughter earlier this morning.

- Employees' gossiping about patients to friends or coworkers.

Example: Talking to your spouse about how you treated Jennifer Lopez today.

- Employees' giving out patient information to non-authorized persons.

Example: Jane's husband calls to verify her appointment, but is not listed as an authorized person to release information to. We cannot provide that information to him.

Social Media

- Looking up Patients online via, social media, internet searches, and other platforms for personal use.

Example: A super cute patient comes in, and a staff member looks him up on Facebook to see if he is married.

- Looking up Patients family / spouse / friends, because you think you know them.

Example: Luke thinks he sees his baby mama's sister-in-law in the lobby he looks to see if the patent in the lobby is the sister-in-law.

- Googling a patient, or searching on any internet search for PHI.

Example: Penny Goggles her patient patient because she thought she saw his mug shot in the news.

Proper Disposal of PHI:

Improper disposal of PHI, Any and all papers with patient information must be disposed separately from trash and be shredded for PHI.

Including but not limited to:

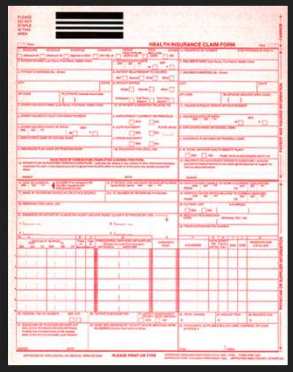
- Claim
- Statement
- Rx
- Intake
- Labs
- Receipts
- Phone message
- Fee Sheet
- Chart
- Travel card

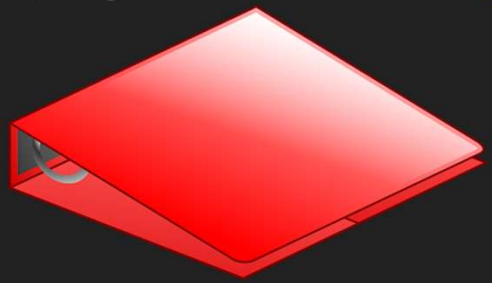
Empty personal shred bin at the end of your shift.

We employ a company that shreds our PHI on site.

Shred a Box
CONFIDENTIAL DESTRUCTION

What goes into the Shred Bin?





HIPAA and Medical Records:

How to be in compliance with medical records and medical requests.

- Patients are entitled to obtain a copy of their medical records at their request.
- Patients must fill out a medical records request, or we cannot process the request.
- Requests must be processed within 30 days. It is our policy to have 5-7 business days to process the medical records request.
- Request MUST be reviewed by the provider before we give a copy out.
- Patients may delegate a personal representative with written authorization to obtain records or inquire about PHI.
- As a provider we are allowed to send over a patient's record to another provider, as coordination of benefits.
- When we receive a fax request for a request: If it is from a CE we are can send out the notes. If it is from any other source, a signed release from the patient must accompany the request.
- Request MUST be reviewed by the provider before we give a copy out to ANYONE.

HIPAA:

Questions, Comments or Concerns?