By reviewing this information, you agree to understand that this training is:

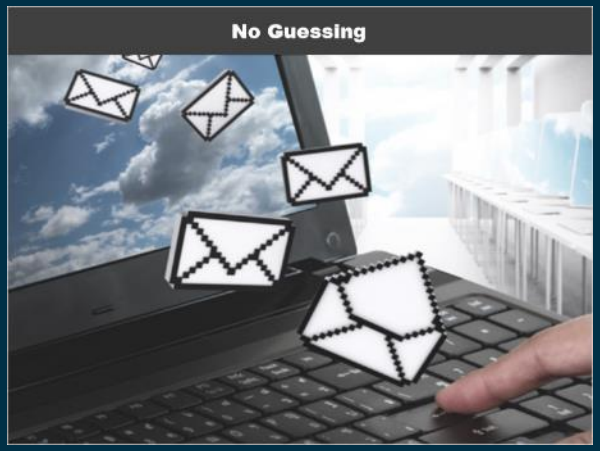
Classified: Restricted

Only VSP® Employees or other persons specifically authorized by VSP may access this information.

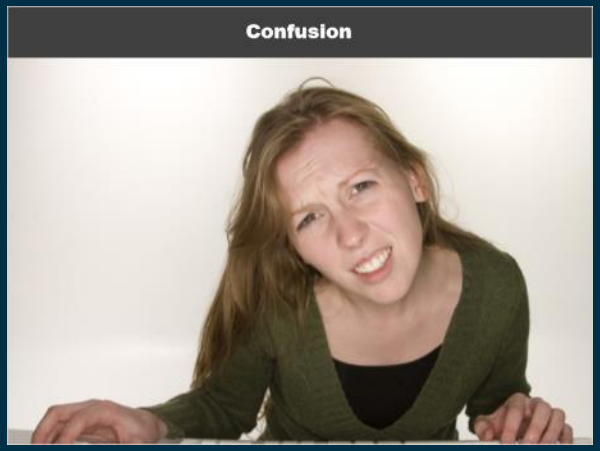
HIPAA TRAINING

Who This Course is For

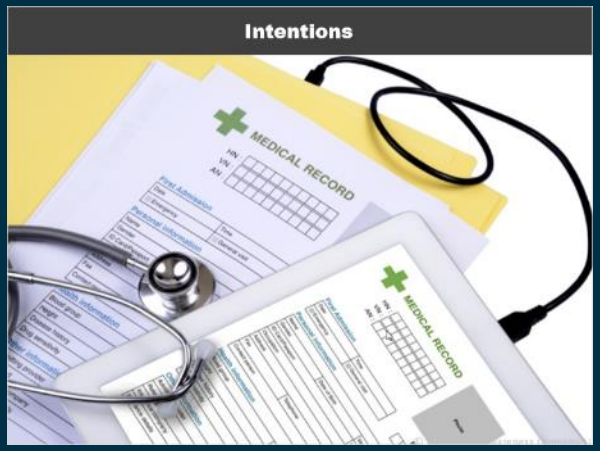
This course is designed specifically for the needs of individuals or entities covered by the provisions of the Health Insurance Portability and Accountability Act-better known as HIPAA. This course focuses on familiarizing end users with the basic provisions of HIPAA with respect to protecting patient privacy and the security of patient records.



It is not intended to be a substitute for your company's internal policies on HIPAA compliance. Whenever you have a question about your company's policies or practices, or what you should do in any specific situation, don't guess. Contact your HIPAA compliance office immediately.



There is a lot of confusion about what HIPAA does and does not require. While the 1996 law and its regulations are long and complicated, the basic principles are simple.



HIPAA is designed to make sure that medical information is kept confidential and private and only used in the way for which it is intended.

This means that medical information can only be collected, shared, stored and used for legitimate purposes and must be properly protected.

The HITECH Act in 2009 made sure that the HIPAA privacy and security regulations, including the data breach notification requirements, apply not only to healthcare entities but to those business associates with whom they share health data.

This awareness course outlines specific ways to accomplish this requirement.

The law talks about different HIPAA “covered entities.”

These include healthcare providers (like doctors, hospitals and labs), healthcare plans (like HMOs and PPOs) and healthcare clearing houses that collect and process heath care data. While not all entities that have any connection to health information may be “covered” by HIPAA, if you collect or use health information, even if it came from a third party, you must use it properly and protect it.

Many people and organizations associated with the healthcare profession collect or use health information. While it is clear that hospitals and doctors collect this information, so do their lawyers, accountants, managers, licensors, and even IT specialists.

These entities are generally called “business associates”, and they must also take care to use and protect the healthcare information properly. A good way to look at business associates is anyone who has access to unencrypted health data. This can include data processors, storage facilitators, or other people or entities who can see health data.

A key term under HIPAA is called “PHI” or Protected Health Information. This is any health information which is about, or can be linked to, a particular person, such as information about a diagnosis, treatment or lab result.

PHI is protected no matter how or where it is collected or stored, such as on a computer, in an email, on a patient's chart, on a post-it note, stored on a telephone, or even in a voicemail. If it relates to an identifiable person's health, it is probably PHI.

The kinds of health information protected by HIPAA include anything about the patient's medical condition: what was done for or advised to the patient, information about payment and insurance or anything that can be used to identify the individual. Interestingly enough, merely the fact that a person is a patient or has received treatment, or simply made an inquiry about treatment, can be PHI.

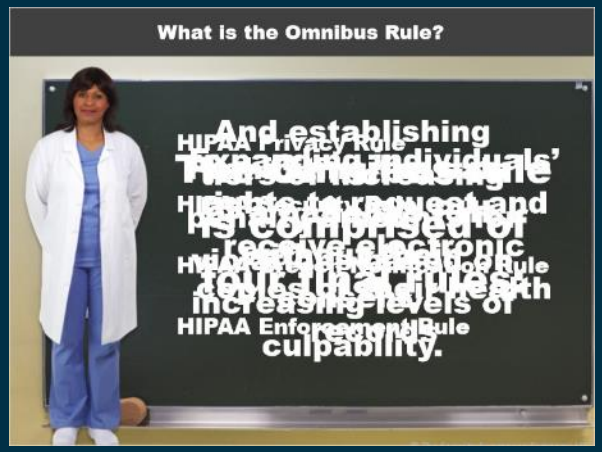
There are many permitted uses of PHI. In fact, there are probably many more permitted uses of PHI than prohibited ones.

You can, of course, tell the patient about his or her medical condition, or disclose PHI where the patient has made an informed consent. You can also make any disclosures that are necessary to or even incidental to, patient treatment, payment or healthcare operations. This means you can tell other healthcare providers, labs, insurance companies, consultants or otherwise share the data in order to treat the patient or obtain payment.

In fact, a good starting point is that PHI can be used anytime for health related reasons, including diagnosis, treatment, healthcare administration or any payment for these services.

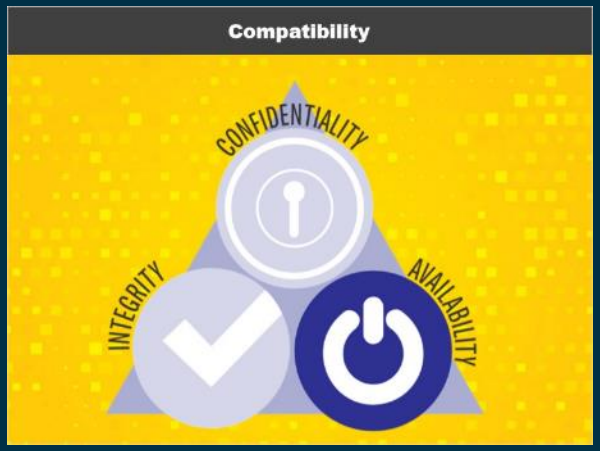
The most important rule is to use common sense.

In January of 2013, the Department of Health and Human Services modified HIPAA with a new set of regulations known as the HIPAA Omnibus Rule. This final rule includes many complex changes - over 500 pages worth - to further improve the protection of sensitive data and provide patients with additional rights regarding their health information.



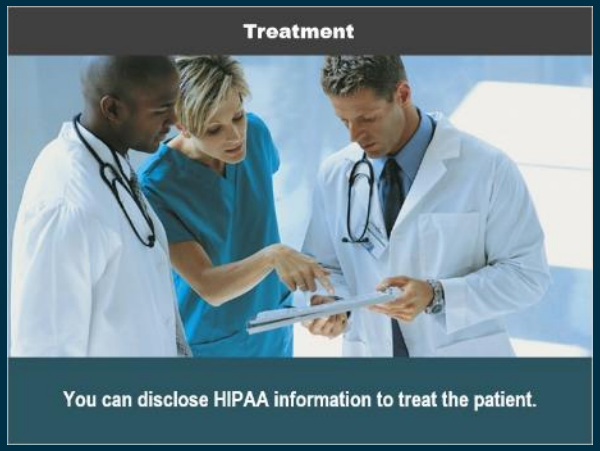
The Omnibus Rule is comprised of four final rules: the HIPAA Privacy Rule, HIPAA Security Rule, HIPAA Breach Notification Rule, and HIPAA Enforcement Rule.

Some example modifications include: expanding individuals' rights to request and receive electronic copies of their health records; prohibiting the sale of a patient's PHI without their consent, and establishing tiers of increasing penalty amounts for violations based on increasing levels of culpability.



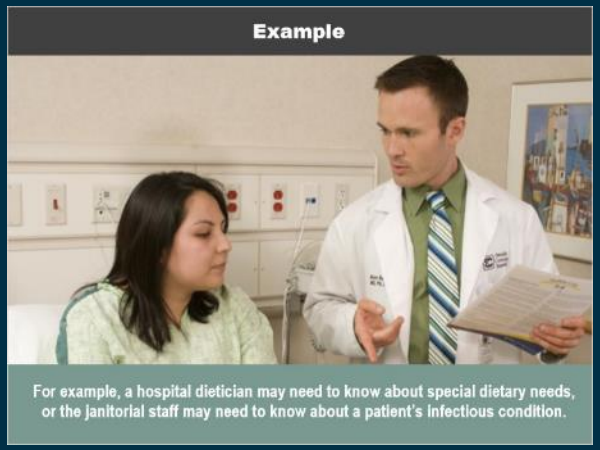
As complicated as this all sounds, the main goal of the Omnibus Rule is to ensure patient's rights, to update HIPAA with language that not only makes it forward compatible with future technology but also clarifies terms and definitions - making them more objective, and to improve workability and flexibility for regulated entities- ultimately decreasing their burden.

The bottom line is that anyone who ever handles patient data or health information of any kind works together to abide by all provisions to ensure the confidentiality, integrity and availability of that data.



Obviously, you can disclose HIPAA information to treat the patient. This means to find out what is medically wrong and provide medical and related services.

Lots of things are covered under the “treatment rule” including consultations, referrals and even telling non-medical staff about the patient’s condition where it relates to treatment.



For example, a hospital dietician may need to know about special dietary needs, or the janitorial staff may need to know about a patient's infectious condition.

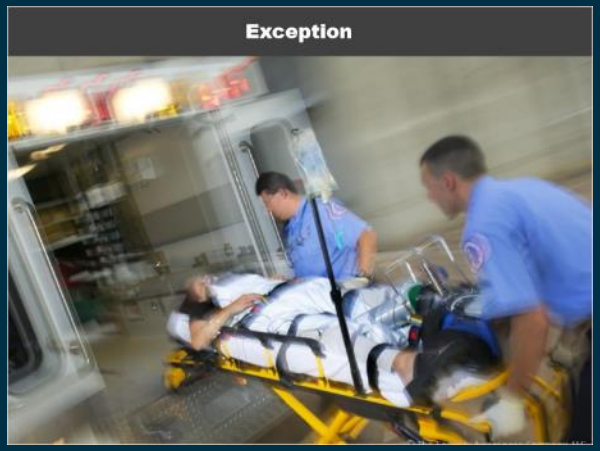
These "disclosures" would be permitted under the "treatment rule."

In order to be reimbursed for services, covered entities may have to disclose information about the patient's treatment to third party payers.

This is also permitted under HIPAA, provided that the disclosure is reasonable and is to the minimum extent necessary to obtain payment.

There are many other activities a covered entity takes, which do not relate directly to patient treatment. Quality assurance, licensing, regulatory compliance, auditing, legal reviews, underwriting and insurance, business planning and other administrative activities may require the use or disclosure of PHI. This too is permitted under HIPAA, as long as the information remains protected and is used only for the proper purpose.

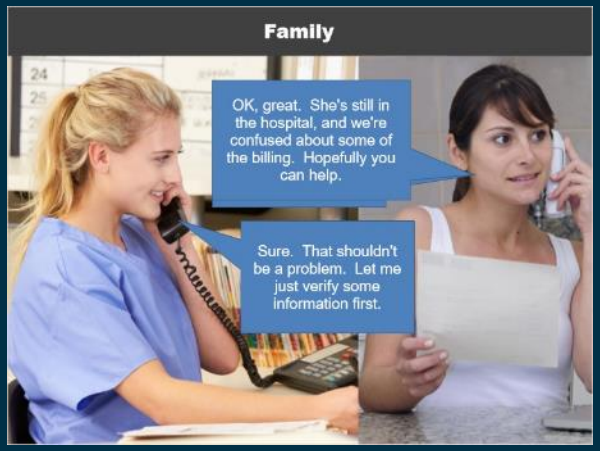
As a general rule, patients should be given the opportunity to consent or object, to the disclosure of PHI.



The only exception is in the case where an emergency exists which requires such disclosure.

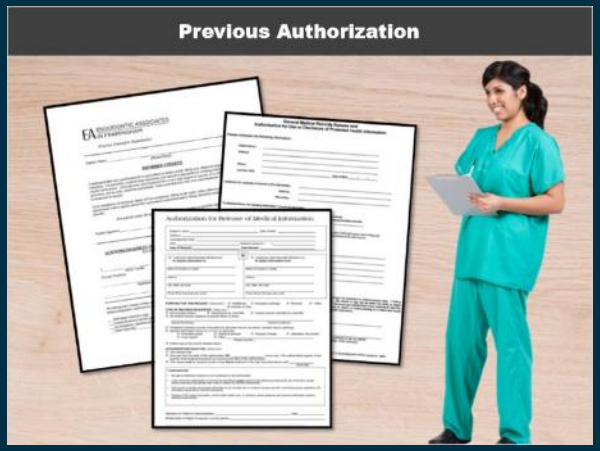
The goal of HIPAA is to balance patient's need for privacy and security against the needs of the provider, insurer or other covered entities to collect and use health information. In some circumstances, such as the need to protect the public health from an epidemic, disclosures are permitted.

As a general rule, if the disclosure or use is not for treatment, payment or healthcare operations, the patient's written authorization is required.

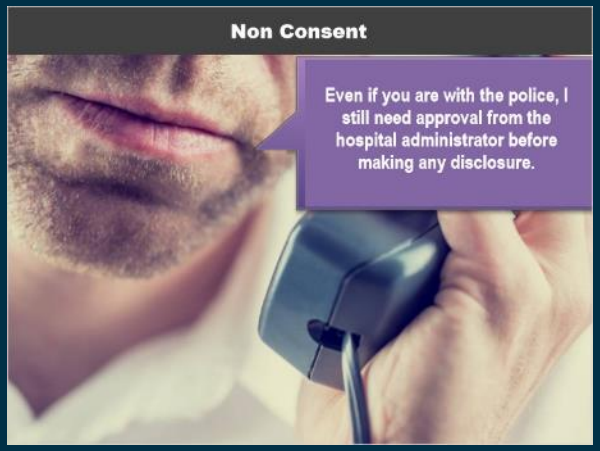


Frequently, a family member or close friend may make an inquiry about whether a relative or friend is receiving treatment, or about the status of a bill. It is important to know that HIPAA has no “hard and fast rule” regarding this situation. Thus, you should use common sense in deciding not only when, but how to make such a disclosure.

Of course, if the patient is awake, alert, and able to consent, the patient may authorize the disclosure, provided that you have reasonably authenticated that the potential recipient is in fact the relative or other person the patient has consented to give access to the information.

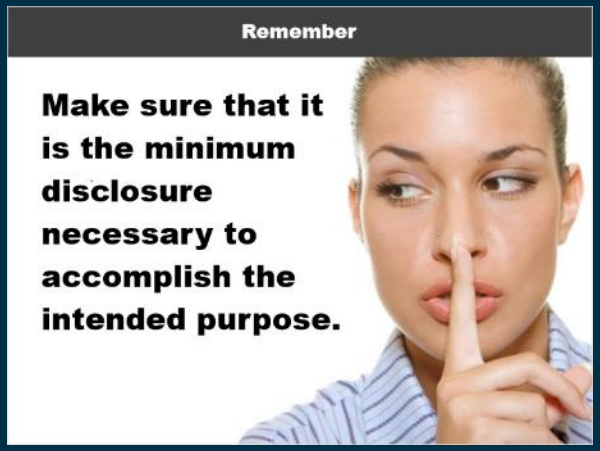


If the patient has previously authorized disclosure through a written consent form, like a health care proxy or HIPAA disclosure form, then you can also make the disclosure as authorized by the patient.



If a patient specifically does not consent (he or she says no) then, generally, you may not release the information unless there are extenuating circumstances (such as the patient's mental status, a medical emergency, the need to protect the public, a law enforcement demand or a subpoena). In these cases, it is best to obtain legal advice, when possible, before making a disclosure.

If the patient is unable to consent to the disclosure, you should use your best professional judgment about whether the disclosure is in the best interests of the patient, and use reasonable means to validate the identity of the person to whom the disclosure is being made.



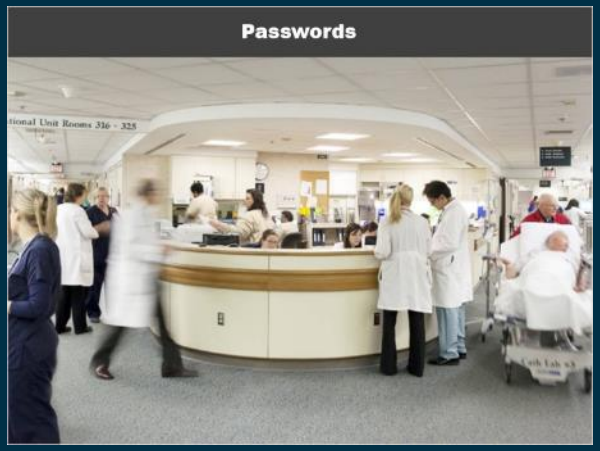
Remember, whenever you make any disclosure of PHI, ensure that it is the minimum disclosure necessary to accomplish the intended purpose.

In addition to protecting privacy, HIPAA requires covered entities to provide security for PHI.

While you are aware of basic security practices, like not sharing passwords or downloading viruses, the HIPAA rules focus on protecting PHI from threats and misuse. It requires appropriate technical, administrative and physical security, including assessments and evaluations, along with training and awareness.

But, HIPAA does not require specific technologies. It requires you to do what is reasonable, considering how big and complex your organization is, what kind of infrastructure you have, how much the security will cost and what the risk is to the PHI.

What a large hospital may need to do is not the same as what a small doctor's office may require. The key here is to be reasonable.



Of course, you should never share your password, and you must ensure it is properly protected. In hectic healthcare environments, this may present a challenge, particularly where patient treatment is concerned. Unlike an ordinary office, a hospital or other medical provider may have many patients, family members, staff and others, milling about.

Therefore, you should take reasonable precautions to make sure that PHI is not exposed, like turning computer screens so that they can't be seen by unauthorized individuals, ensuring that systems "time out" after a period of non-use, that users must authenticate themselves and even things like keeping patient records behind the desk so they can't be seen by unauthorized individuals. Remember, the goal is to protect PHI.

PHI is very sensitive information. Therefore, you should take extra steps to make sure that it is protected, no matter where it is.

Don’t store this information on thumb drives, portable media or any place where it might be lost or stolen.

In fact, the information should be stored in an encrypted or scrambled manner so that even if the device is lost or stolen, the data cannot be compromised.

Keep PHI out of sight and locked up when not in use.

PHI is also in danger when it is being transmitted. If you talk over the phone about PHI, make sure you know who you are talking to.

You should never send PHI over the Internet, whether by email or other electronic means, unless it is reasonably protected, preferably by encryption.

Only send PHI for proper purposes to people who have a need to possess it and in a way that ensures that it is protected.

The rules about protecting PHI also apply to disposing of it, no matter how the PHI was collected. Therefore, make sure that any PHI discarded is properly shredded or otherwise destroyed.

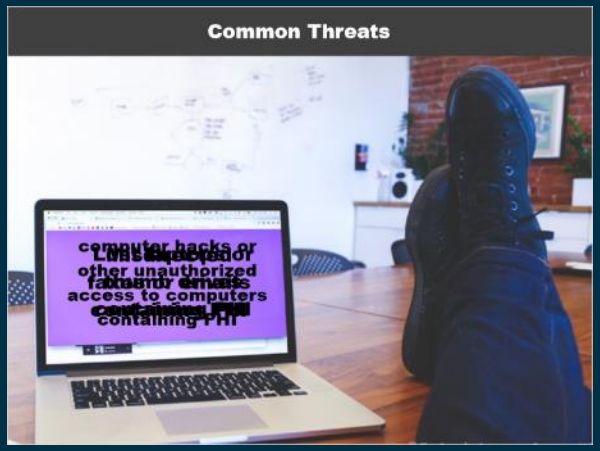
If you dispose of computers or electronic media that contain PHI (and this might include cell phones that store emails containing PHI), make sure that these files are not merely deleted, but wiped clean using appropriate software for that purpose.

HIPAA also requires reasonable physical security. This means locking doors, windows, drawers, closets, and file cabinets to limit PHI access only to authorized individuals.

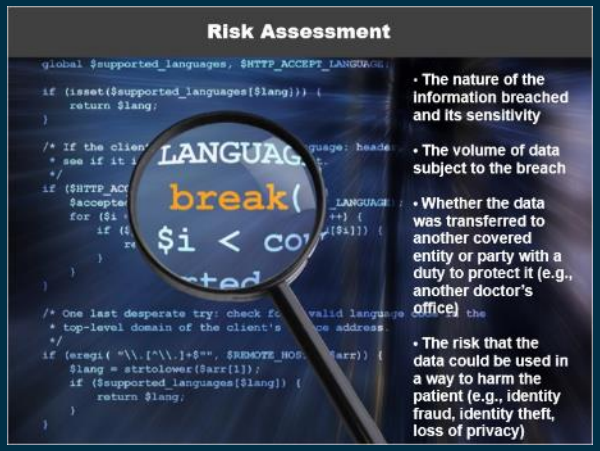
Challenge people who don’t belong.

Make sure there is a reasonable level of access control to any media that contains PHI. HIPAA does not mandate a particular level of physical security, just that which is reasonable.

The HIPAA and HITECH laws require both covered entities and business associates to disclose whenever they have had an unauthorized access to or loss of unencrypted or unsecured PHI.



The most common threats include lost laptops or thumb drives containing PHI, misdirected faxes or emails containing PHI, as well as computer hacks or other unauthorized access to computers containing PHI.



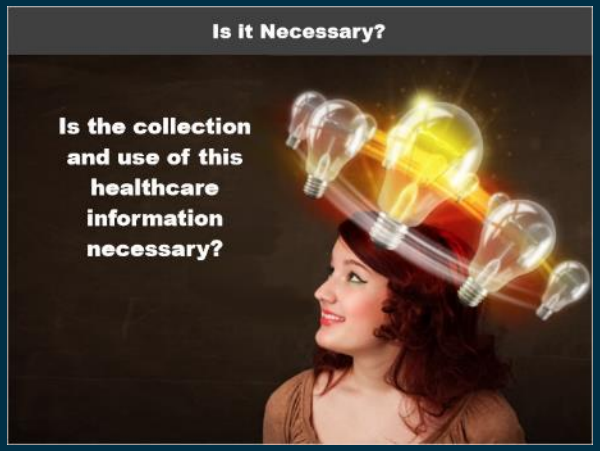
Such data breaches must be reported promptly to management, and where appropriate, to the patient or the government. In deciding whether notification should be made, management will conduct a "risk assessment" which will look at factors like:

- The nature of the information breached and its sensitivity
- The volume of data subject to the breach
- Whether the data was transferred to another covered entity or party with a duty to protect it (e.g., another doctor's office)
- The risk that the data could be used in a way to harm the patient (e.g., identity fraud, identity theft, loss of privacy)

Finally, HIPAA grants patients certain rights.

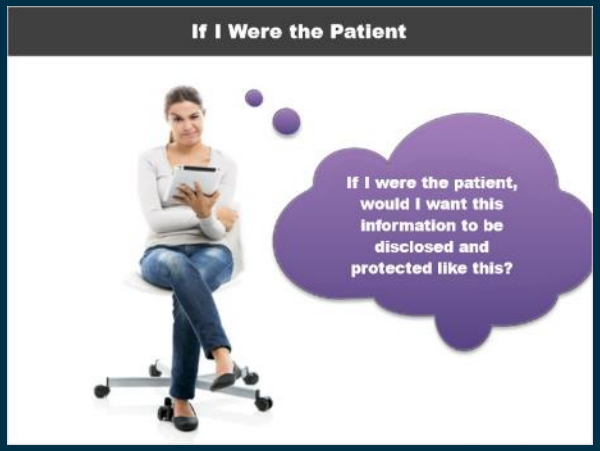
- They have a right to know about data collection and privacy practices.
- They can generally (but not always) see their own health information, and make sure it is accurate.
- They can opt out of the patient directory so other people won't know they are a patient.
- They can communicate confidentially with providers. For example, saying "Don't email my medical records." or "Only call me at a particular number."
- They generally have the right to know why their health information has been disclosed, and to whom.
- And, they have a right to complain, both internally and to regulators.

Substantial fines may be imposed for violations of HIPAA regulations.



The most important thing to ask is whether the collection and use of the healthcare information is necessary.

Do I need it? Do I need all of it? Do I need to disclose it? Am I protecting this information using reasonable practices?



Ask yourself, if I were the patient, would I want this information to be disclosed and protected like this?

Can this data be encrypted or otherwise protected from unauthorized access or use?

Remember, if you have questions about what to do or see anything suspicious or unusual, make sure you ask the appropriate management personnel.

For more information regarding HIPAA requirements, please visit www.hhs.gov.

THANK YOU