



eHI Explains: 6 HIPAA MYTHS

Though HIPAA has been around since before the iPhone, there is still a lot of confusion about what HIPAA does and does not cover.

#1: Doctors can't talk to your loved ones

HIPAA allows doctors to give loved ones a report on a patient's health, unless a patient is conscious and clearheaded, and opposes this information to be shared. The doctor has the authority to use their professional judgement about what is shared and with who. The only time a patient's wishes are denied if is the doctor believes the patient is a serious threat to themselves or others.

#2: Doctors need written authorization to share your health information

If the doctor is sharing your information with another physician or medical professional to aid in an individual's care, then they do not need any authorization. To share your information with one's family or trusted friend, then the doctor can receive a verbal, written, or electronically sent authorization to share.

#3: Doctors can't email patients

Doctors have the option to engage in communications with their patients through both encrypted and unencrypted emails. Once a patient is given information about the risks, they can decide which email platform to use with their doctor. Regardless, a doctor must ensure all of the patient's data is secure, and that nothing is ever edited, false or deleted.

#4: HIPAA protects all health data

HIPAA protects data that is shared with one's doctor or their medical practice. However, once data is shared with someone or something not covered by HIPAA (think: 3rd Party Apps like My FitnessPal) then the data is no longer legally protected.

#5: If an organization is HIPAA-certified, it is okay to share information with them

There is no such thing as a "HIPAA-certified" organization or device. An individual can become "HIPAA-certified", but this does not mean that they are complying with HIPAA. Instead, this solely means that they have undergone a course on HIPAA and know the rules.

#6: If you download a health app, your information will be protected

There is no such thing as a "HIPAA-certified" health app. If a company offers a direct-to-consumer version of an app that is not provided on behalf of a covered entity (like a provider or hospital), it is not subject to HIPAA. If a consumer downloads data from his or her doctor's EHR through a patient portal and then uploads the data into a health app that the provider has no role in developing, there is no business associate relationship between the organization offering the app and the provider.