

HIPAA FAQs

By [Simone Handler-Hutchinson](#)

Below are several frequently asked questions and answers addressing the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its accompanying privacy and security regulations.

Q: Is the government really going to enforce the HIPAA privacy and security regulations?

A: Yes. HIPAA is already being enforced, even though the HIPAA enforcement provisions aren't yet final. To date, thousands of privacy complaints have been filed with and investigated by the Office for Civil Rights (OCR). One man has been sentenced to jail time for a HIPAA privacy violation. The Centers for Medicare & Medicaid (CMS) has also established a separate complaint process to receive and investigate all non-privacy complaints—those related to HIPAA security and transaction and code set compliance. In addition to the threat of a HIPAA violation and possible civil and criminal penalties, there are other serious risks when a patient's health information has been improperly disclosed. For example, a patient might sue a health care provider for breach of patient confidentiality in state court, or file a complaint with the state professional licensing board or agency, or with the patient's health insurer. There is also the risk of bad public relations when a privacy or security breach becomes public.

Q: Do I need to renegotiate ALL my business associate agreements to comply with the HIPAA security regulations?

A: No. To comply with the HIPAA security regulations (compliance date: April 20, 2005) you must add certain security provisions to only those business associate agreements that involve the exchange of "electronic protected health information" or EPHI. For example, a business associate agreement with a company that recycles or destroys a nursing home's outdated computers, monitors and other electronic devices would require HIPAA's security provisions. To comply with the security requirements without having to renegotiate all your business associate agreements that involve EPHI, create a separate HIPAA security addendum that can be signed and attached to your existing business associate agreements.

Q: How should an organization respond when it receives a call or letter from OCR or CMS informing it that a privacy or security complaint has been filed against it?

A: There are a number of steps you can take to protect yourself. For starters you will need to cooperate with the government agency and gather any and all information relating to the complaint. You will also have to show them: 1) whether you had reasonable policies and procedures in place, 2) whether your staff was fully trained on them, 3) whether the policies and procedures were followed (and if not, why not), and 4) what steps you took to mitigate the harm caused by the HIPAA violation, if applicable.

Q: How can a small health care provider comply with the HIPAA security standards?

A: While the HIPAA security standards are complex, they do allow providers needed flexibility. For instance, the security standards don't mandate the use of any specific type of technology. They also allow a provider, regardless of size, to use security measures that allow the provider to "reasonably" and "appropriately" comply with the standards. Further, in determining what security measures to implement, a provider may take into consideration its size and capabilities, as well as the costs of compliance.

More HIPAA questions? Please contact Schenck, Price, Smith & King's Health Care Practice Group at: (973)539-1000 or email Simone Handler-Hutchinson directly at: shh@spsk.com