Navigating the Waters of HIPAA Regulations and Resources: the Basics

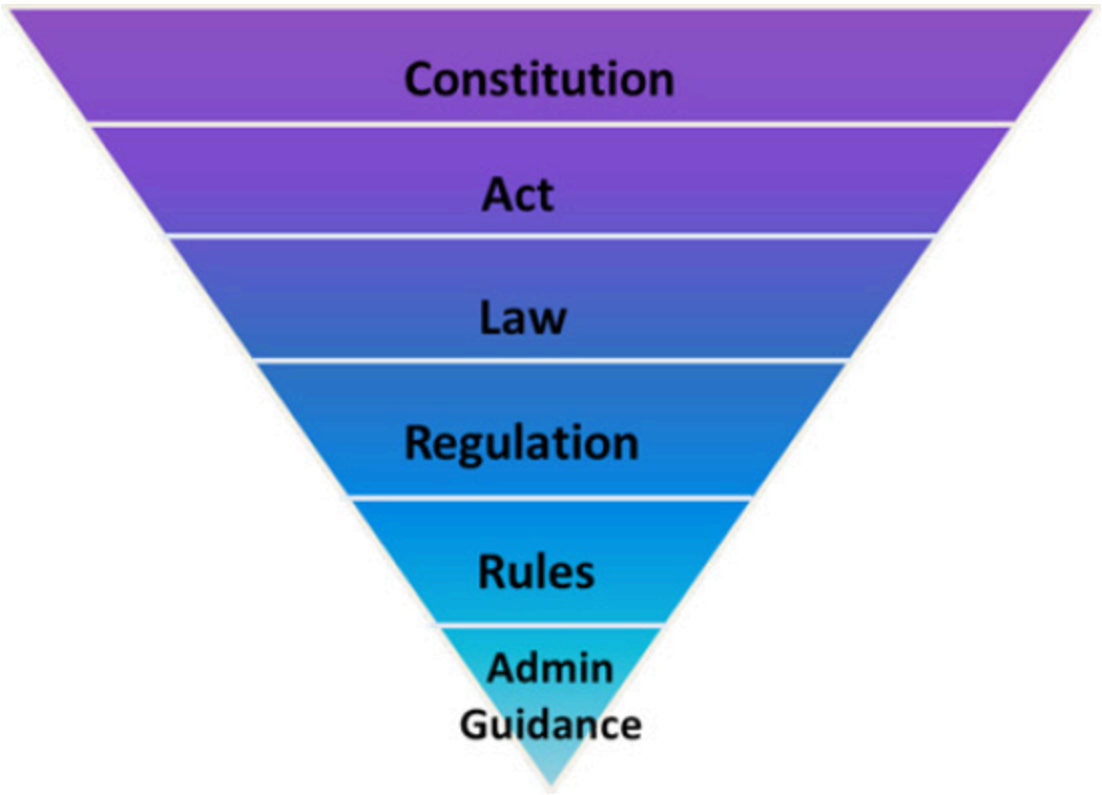
Save to myBoK

By Richelle Marting, JD, MHSA, RHIA, CPC, and Dana DeMasters, MN, RN, CHPS

Despite its codification under the administrative simplification provisions of the Health Insurance Portability and Accountability Act (HIPAA), those responsible for compliance often agree HIPAA is anything but administratively simple. Even the plethora of resources offering HIPAA guidance can easily become overwhelming. Online guidance may offer answers to questions, but may not hold up against the reality of administrative enforcement. Binding legal authority is preferred over anecdotal references, but which legal sources should be given priority over others? This article explains some of the legal resources available on HIPAA and how they can help solve several common privacy and security issues.

Figure 1

The following diagram illustrates the hierarchy of legal authority.



The sources of legal authority illustrated in Figure 1 above are listed below in chronological order of creation and illustrate how each relates to HIPAA authority. See the notes listed after some of the areas for the HIPAA equivalent of this type of legal authority.

1. **Act.** First, an act is passed by Congress. Acts are plans to implement a law, such as HIPAA.
2. **Law.** After an act is passed, a law (statute) is created. Statutes are often broad, such as 42 U.S.C § 1320d-6, which makes it unlawful to wrongfully use or disclose individually identifiable health information. This broad law does not describe these terms, however.

3. **Proposed Rule.** Once laws are created, a government department or agency such as the US Department of Health and Human Services (HHS) may be tasked with developing regulations to implement the law. Regulations are then proposed and published in the *Federal Register*. The public can review and comment on the proposed rule before it becomes a final rule or regulation.[1]
4. **Final Rule.** The responsible department will review comments to its proposed rule and decide what aspects will be implemented, modified, or removed. After making these decisions, a final rule is published in the *Federal Register*.[2] A final rule addresses public comments received and explains the department's decision making in creating the final rule. The regulatory language in the final rule is published on the US Government Publishing Office website. Note that while these rules are issued before a regulation, the regulation is the more authoritative source.
5. **Regulation.** A regulation is implemented once a final rule is published and has the force of law. Unofficial copies of the Code of Federal Regulations are published at www.ecfr.gov.

Government agencies such as the HHS Office for Civil Rights (OCR) may interpret laws and regulations by issuing guidance and answers to frequently asked questions or publish their opinions on specific cases enforced. If addressed in court, courts will give deference to the interpretations by the agency charged with the laws' administration.[3]

Examples of HIPAA Guidance in Practice

The following are examples of tricky HIPAA questions and some guidance on answers, along with where these scenarios fit into the hierarchy of legal authority.

Question: A hospital employee has gossiped about a patient's protected health information (PHI) to coworkers not involved in the patient's care. Would this constitute a HIPAA violation?

Answer: Yes. Section 264 of HIPAA required HHS to submit recommendations for standards on the privacy of health information.[4] The federal law broadly addressing this requirement makes it an offense to knowingly use a unique health identifier improperly (42 U.S.C. § 1320d-6(a)(1)). Federal law also defines individually identifiable health information (42 U.S.C. § 1320d). The federal laws do not, however, detail what constitutes an impermissible use of PHI.

HHS initially proposed a regulation defining "use" of PHI as "the employment, application, utilization, examination, or analysis of health information within an entity that holds the information."[5] The HIPAA Final Rule added "sharing" of information to the list of activities constituting a use within a covered entity.[6] The definition published in the final rule became binding federal regulation (45 C.F.R. § 160.103). Similar regulations prohibit using PHI unless certain requirements are met, such as using information for legitimate treatment, payment, or operations purposes. Even then, regulations require use of only the minimum information necessary (45 C.F.R. § 164.502(a), (b)). OCR has issued administrative guidance on point for this issue. For example, OCR discusses incidental uses and disclosures at www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/incidentalu%26d.pdf.

Because the information above was shared within the entity holding the PHI, the gossip is a "use" of PHI. Gossiping about a patient does not serve a legitimate treatment, payment, or healthcare operations purpose, and is therefore an impermissible use.

Question: A clinic manager contacts the privacy officer with an urgent request. The spouse of a patient is calling the clinic and threatening to harm staff. What legal sources allow for release of patient information to law enforcement and what information may be released?

Answer: The same provisions of HIPAA and federal law in the first scenario apply here as well. In 1999, HHS proposed to permit use and disclosure of PHI in emergency situations upon a reasonable belief that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of any person or the public.[7] The proposed rule explained such information may be needed by law enforcement, first responders, or others, including the target of a threat, that are able to prevent or lessen the threat of harm. Any uses and disclosures for these purposes must also be consistent with healthcare providers' standards of ethical conduct.

The proposed rule also explained this permissible use and disclosure must be limited to situations of imminent and serious threats, not merely in response to hypothetical scenarios or potential emergencies that are not imminent and serious, stating

"this permitted disclosure would be narrow."

Additionally, the proposed rule provides examples of what constitutes standards of ethical conduct, such as the American Medical Association's Principles of Medical Ethics on Confidentiality, which provide that safeguarding information is subject to certain exceptions because of overriding social consideration.

When a patient threatens to inflict serious bodily harm to another person or to themselves and there is a reasonable probability the patient may carry out the threat, the physician should take reasonable precautions for the protection of the intended victim, including notification of these activities to law enforcement. The proposed rule also noted it was not intended to create a duty to warn, but rather would make it permissible under HIPAA's regulations.

When the rule was finalized, HHS removed language referencing emergency circumstances. They said circumstances that would warrant these permissible disclosures are not intended to apply to emergency care treatment, and that there may be situations other than "emergency circumstances" that could warrant disclosure in order to prevent or lessen an imminent threat.

According to the final rule (codified at 45 C.F.R. § 164.512(j)), disclosures in these cases should meet the minimum necessary standard (45 C.F.R. § 164.502(b)). OCR published guidance that these disclosures are permissible when a covered entity has a good faith belief that the disclosure is necessary to prevent or lessen the threat. Beyond the individuals and entities described in the proposed and final rules, OCR explains this could include disclosures to family members or others who could mitigate the threat. Again, the guidance emphasized that the threat must be "serious and imminent," although there may be other provisions permitting disclosure in situations where the threat is not serious and imminent.

If the provider reasonably believes the threat is credible and presents a serious and imminent risk to the health and safety of its staff, and if the disclosure is consistent with the provider's professional standards of ethical conduct, the clinic could report the threat to law enforcement or others who may be in a position to lessen or mitigate the threat.

Access to Knowledge Lessens Risk

The waters of legal authority on privacy and security may seem choppy and uncharted at times. Knowing the most authoritative sources to reference and having a comprehensive list of statutes, rules, regulations, and administrative guidance helps smooth the sailing.

[1] Department of Health and Human Services (HHS). "Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act—A Proposed Rule." *Federal Register* 75, no. 40,867. July 14, 2010.

[2] HHS. "Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules—A Final Rule." *Federal Register* 78, no. 5,566. January 25, 2013.

[3] HHS. "Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules." *Federal Register* 78, no. 5,565. January 25, 2013.

[4] HHS. "Health Insurance Portability and Accountability Act of 1996." Government Publishing Office. Public Law 104-191. August 21, 1996.

[5] HHS. "Standards for Privacy of Individually Identifiable Health Information—A Proposed Rule." *Federal Register* 64, no. 69,918. November 3, 1999.

[6] HHS. "Standards for Privacy of Individually Identifiable Health Information—A Rule." *Federal Register* 65, no. 82,461. December 28, 2000.

[7] HHS. "Standards for Privacy of Individually Identifiable Health Information—A Proposed Rule." *Federal Register* 64, no. 59,971. November 3, 1999.

Richelle Marting (rmarting@forbeslawgroup.com) is an attorney with the Forbes Law Group in Overland Park, KS. Dana DeMasters (dana.demasters@libertyhospital.org) is a privacy/security officer at Liberty Hospital in Liberty, MO.

Article citation:
Marting, Richelle; DeMasters, Dana. "Navigating the Waters of HIPAA Regulations and Resources: the Basics" *Journal of AHIMA* 88, no.1 (January 2017): 28-31.