



Managing Information Privacy & Security in Healthcare

HIPAA Privacy and Security Resources for Solo Practitioners and Small Group Practices

By Melanie Schattauer, MA, RHIA

The HIPAA Privacy and Security Standards can be challenging for healthcare organizations regardless of size. Solo practitioners and small group practices may also face the additional challenge of finding reliable sources of information on what is required and then addressing the requirements within their limited resources. A wide variety of resources on the HIPAA Standards are available on the Internet. Particularly relevant are those published by the Department of Health and Human Services (HHS) as well as those sponsored by national, specialty, state, or county medical or dental associations.

The Department of Health and Human Services Resources

The Department of Health and Human Services (HHS) Office for Civil Rights (OCR) has published several resources providing information for both consumers and covered entities on the HIPAA Privacy and Security Rules. This guidance includes items such as a patient's right to an electronic copy of their electronic health record, use and limitations of their protected health information for marketing and/or fundraising, and when a healthcare provider may share a patient's health information with the patient's family, friends, or others involved in the patient's care. These resources answer common questions about HIPAA that are often misunderstood by healthcare providers and patients alike, and can be located using the following links:

- For consumers: <http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/index.html>
- For providers: <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html>
- Additional Resources for small providers, small health plans and other small businesses: <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/smallbusiness.html>

Additionally, the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act (ARRA) of 2009, contained several provisions aimed at strengthening the privacy and security protections for health information established under HIPAA. On January 25, 2013, the Department of Health and Human Services published the Final Rule modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules (the Final Rule also contained modifications to the Genetic Information

Non Discrimination Act (GINA)). This Final Rule, also known as the HIPAA Omnibus Rule, can be located using the following link:

<http://www.hhs.gov/ocr/privacy/hipaa/administrative/omnibus/index.html>

Another important part of the HITECH Act is the HIPAA Privacy, Security and Breach Notification Audit Program. The purpose of the program is to evaluate a provider's or hospital's compliance with the HIPAA Privacy, Security and Breach Notification Rules. The Audit protocol is available on-line and is an excellent resource/tool to determine if the necessary policies, procedures and processes are in place to protect a patient's protected health information (PHI).

- To learn more about the program, visit:
<http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html>
- For a direct link to the Audit Program Protocol:
<http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html>

National Associations HIPAA Resources

State and national medical associations as well as national specialty associations often provide guidance for their members. Some of these include:

[American Health Information Management Association](#)

[American Hospital Association](#)

[American Medical Association](#)

[Healthcare Information and Management Systems Society](#)