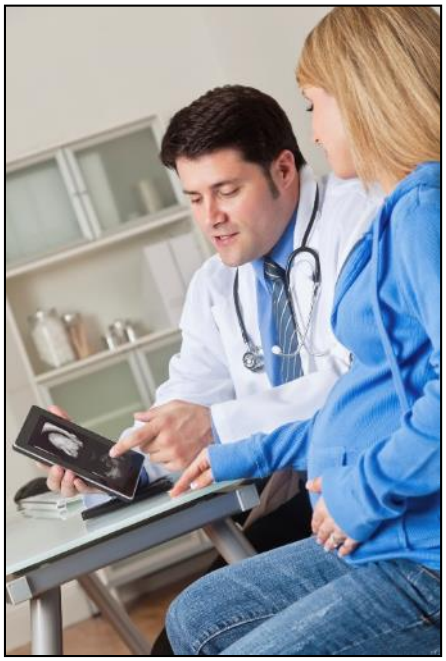
Chapter 1
Why Do Privacy and Security Matter?

Increasing Patient Trust and Information Integrity Through Privacy and Security



To reap the promise of digital health information to achieve better health outcomes, smarter spending, and healthier people, providers and individuals alike must trust that an individual's health information is private and secure. If your patients lack trust in Electronic Health Records (EHRs) and Health Information Exchanges (HIEs), feeling that the confidentiality and accuracy of their electronic health information is at risk, they may not want to disclose health information to you.[6] Withholding their health information could have life-threatening consequences.

This is one reason why it's so important for you to ensure the privacy and security of health information. When patients trust you and health information technology (health IT) enough to share their health information, you will have a more complete picture of patients' overall health and together, you and your patient can make more-informed decisions.

In addition, when breaches of health information occur, they can have serious consequences for your organization, including reputational and financial harm or harm to your patients. Poor privacy and security practices heighten the vulnerability of patient information in your health information system, increasing the risk of successful cyber-attack.

To help cultivate patients' trust, you should:

- Maintain accurate information in patients' records
- Make sure patients have a way to request electronic access to their medical record and know how to do so

[6] http://www.healthit.gov/sites/default/files/022414_hit_attitudesaboutprivacydatabrief.pdf. See also Agaku, I.T., Adisa, A.O., Ayo-Yusuf, O.A., & Connolly, G.N. (2014, March-April). Concern about security and privacy, and perceived control over collection and use of health information are related to withholding of health information from healthcare providers. *Journal of the American Medical Informatics Association, 21*(2), 374-8. Abstract available at http://www.ncbi.nlm.nih.gov/pubmed/23975624.

- Carefully handle patients' health information to protect their privacy
- Ensure patients' health information is accessible to authorized representatives when needed

Protecting patients' privacy and securing their health information stored in an EHR is a core requirement of the Medicare and Medicaid EHR Incentive Programs.[7] (The EHR Incentive Programs are also referred to as the "Meaningful Use" Programs throughout this Guide.) **Your practice — not your EHR developer — is responsible for taking the steps needed to protect the confidentiality, integrity, and availability of health information in your EHR.**

Effective privacy and security measures help you meet Meaningful Use requirements while also helping your clinical practice meet requirements of the HIPAA Rules and avoid costly civil money penalties for violations,[8] as discussed in Chapter 7.

[7] http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/index.html
[8] http://www.hhs.gov/ocr/privacy/hipaa/enforcement/