Patients entrust healthcare organizations with their confidential information. Any loss of this data can have a substantial financial impact on the individual patients whose data is compromised. It is our duty and responsibility to earn and maintain the trust of patients. Part of that responsibility is complying with federal and state laws, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (the “Act”). Despite the absence of the words “patient,” “privacy,” and “information,” this Act directly impacts the way physician offices must maintain patient privacy and provide security for a patient’s protected health information.

The regulatory requirements, captured in the Privacy Rule and the Security Rule, spell out what information is protected and the requirements for protecting it. It is critical to recognize that the task of complying with HIPAA is never “done.” Maintaining patients’ privacy and safeguarding their information is something that needs to be incorporated into our work everyday. HIPAA compliance is an ongoing process. The HIPAA section of the HIMSS Privacy and Security Toolkit for Small Provider Organizations provides a number of resources for small provider organizations to use to improve their compliance with the Privacy and Security Rules.

The HIPAA legislation has been in place for some time now. Since its enactment, HIPAA has been amended, most recently by the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009 (ARRA). These changes include (but are not limited to) extending the HIPAA requirements to Business Associates, restricting disclosures to health plans for patients who pay in full, prohibiting the selling of patient information, and breach notification requirements (discussed below). These requirements are discussed in more detail in the ARRA/HITECH portion of the Toolkit.

4 The Health Information Technology for Economic and Clinical Health (HITECH) Act Pub.L. 111-5, Title XIII http://www.thomas.gov/home/approp/app09.html#h1
It is important to recognize the impact of other recent developments from the ARRA/HITECH which are now forcing many to re-evaluate the HIPAA compliance. A key provision is the move to digital health records, e.g., Electronic Health Records (EHR) or Electronic Medical Records (EMR). These changes are requiring new ways to do business and new challenges to protect the privacy and security of the digital information. Couple this with the new fines that can be levied by Health and Human Services for HIPAA violations and this is placing pressure on small providers to put the changes into place.

Another element of the legislation is the applicability to small providers. ARRA/HITECH has stipulated that any loss of unprotected personal health information (PHI) must be reported as a breach. Additionally, if the number of records is above 500 individuals, then it must also be publicly reported. According to an annual study conducted by the Ponemon Institute, the average cost per compromised record is $144—$204 of indirect costs and $60 of direct costs. As information systems are converted to digital format it is important to review the HIPAA and ARRA/HITECH regulations and determine four things.

1. Where will PHI be stored and accessed?
2. How will the information be protected when it is either stored or exchanged?
3. Who has authorized access to the information?
4. How will the paper records be handled (HIPAA has regulations concerning the disposal of PHI)?

The HIMSS Privacy and Security Toolkit for Small Provider Organizations provides a wealth of information regarding HIPAA Privacy and Security.