Applying technology to improve the U.S. health care system has been a goal for over two generations. Beginning with paper punch cards and giant computers, health care IT has steadily progressed to powerful web-based tools. Today’s technologies enable individuals to access, use and disclose personal health information with the click of a mouse. As a result, there is greater exchange of electronic health information (ePHI) and collaboration of hospitals, physicians, patients and payers than ever before. There is, however, greater potential that individuals – intentionally or unintentionally – may improperly disclose sensitive health information in a manner that is not authorized under HIPAA.²

Privacy and Security are Imperatives

Effective management of ePHI and other sensitive personal information requires a consistent and proactive approach – and one that takes into account the reality that privacy and security cannot depend upon the user alone. Health care professionals and executives, together with their organizations, must establish a culture of privacy and security in order to protect against reasonably anticipated threats. Experience has shown that this is best accomplished with a holistic approach that includes administrative, physical and technical safeguards.

The problem for many health care organizations is that their IT systems are complex and simply were not designed for the protection of ePHI, which is required in today’s regulatory environment. A typical organization may have numerous applications, distributed across the organization, using an array of protocols that reach across the entity’s perimeter. In most health care organizations, physicians, health care

3 For a complete listing of privacy breaches over the last several years, see the listing maintained by Privacy Rights.org located at http://www.privacyrights.org/ar/ChronDataBreaches.htm.
professionals and employees can easily disclose ePHI in e-mails or other electronic communications channels, such as instant messaging (IM) or file transfers (FTP). As a result, each of these communication channels can potentially leak ePHI and, in fact, have been proven to do so.5

“Covered entities” are mandated by HIPAA and implementing regulations to maintain reasonable and appropriate administrative, physical and technical safeguards to protect the confidentiality, integrity, and availability of electronic protected health information against any reasonably anticipated threat. Covered entities that do not comply with the requirements are subject to a number of penalties. Civil penalties are $100 per violation, up to $25,000 per year for each requirement violated. Criminal penalties range from $50,000 in fines and one year in prison up to $250,000 in fines and 10 years in jail for knowingly violating the requirements. In June 2005, the U.S. Department of Justice (DOJ) issued a memorandum clarifying who can be held criminally liable under HIPAA.6 Covered entities – including health plans, health care clearinghouses, health care providers who transmit claims in electronic form, and Medicare prescription card sponsors - are subject to these criminal penalties. Individuals such as directors, employees, or officers of the covered entities, where the covered entity is not an individual, may also be directly criminally liable under HIPAA in accordance with principles of “corporate criminal liability.” The DOJ interpreted the “knowingly” element of HIPAA for criminal liability as requiring only knowledge of the actions that constitute an offense. Specific knowledge of an action being in violation of the HIPAA statute is not required.

Powerful Technology – Cost Effective Solution

The challenge is to limit the exposure of ePHI and other sensitive consumer data by preventing it from leaving your organization’s network unprotected. Intrusion’s Compliance Commander is powerful technology that provides a cost-effective tool to locate and to prevent such security lapses – before they occur. Compliance Commander stops ePHI data with 100% accuracy before it can leave your network unprotected. Compliance Commander’s Dynamic Application Detection™ technology protects all applications, ports and protocols against intentional and unintentional leaks of ePHI.

This enables your IT team to mitigate areas of risk that frequently include common business processes involving:
- Business associates7
- Patient or customer support
- Mobile health care staff
- Other IT applications and services

Compliance Commanders Dynamic Application Detection™ technology protects all applications, ports and protocols. It also protects against targeted attacks, which are becoming more widespread as the value of consumer and health care data grows.

Intrusion’s integrated Ticket Manager Workflow tool provides a simple, yet powerful, process for fixing data leaks before they can cause damage. Advanced reporting and management capabilities quickly summarize your risks, enabling you to focus your resources on the areas of highest risk to your organization and your patients.

You and your team have spent years building a successful business – working hard to develop trust with your patients and customers and value for your stakeholders. Don’t risk your hard work by failing to implement effective tools such as Intrusion’s Compliance commander. The Department of Health and Human Services, Federal Trade Commission and other regulatory enforcement agencies expect you to protect ePHI like you would your company’s cash. Your patients and customers demand it.

---

5 The 2006 Survey reveals the numerous incidents of patient privacy and security breaches that occur for most organizations. Privacy Breaches: Sixty percent (60%) of compliant providers indicated that they had experienced privacy breaches between July 2005 and January 2006. Forty-one percent (41%) experienced between one and five privacy breaches, and another 19% had six or more breaches. Sixty-six percent (66%) of payers reported privacy breaches; 54% indicated that they had between one and five privacy breaches, 3% had six or more breaches, and 9% had an unknown number. Security Breaches: Twenty-four percent (24%) of providers experienced between one and five security incidents, and 13% reported 6 to 11 incident. Among payers, 28% experienced between one and five security incidents, though another 7 percent experienced between 6 to 11 breaches.


7 Under HIPAA, a “business associate” is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.