Healthcare and the Importance of Visual Privacy

The healthcare industry has gone through a data revolution over the past decade. A large volume of healthcare records have now been digitized, and with the passage of the Health Insurance Portability and Accountability Act (HIPAA) in 1996 and the Health Information Technology for Economic and Clinical Health Act (HITECH) in 2009, healthcare providers, their business associates (lawyers, accountants, etc.) and other custodians of protected health information (PHI) have the obligation to keep patient information safe. While significant efforts have been made to protect PHI as it is stored and transmitted, a third critical area of data protection—visual privacy—has been under-addressed by some providers.

The need for visual privacy, which is the protection of sensitive data while it is displayed on a screen, has increased even more over the past few years due to the enactment of HITECH, which includes provisions to increase the use of information technology to store, capture, transmit, appropriately share and consume health information. New ways to enter and display data means new responsibilities for healthcare organizations to protect PHI. HITECH also includes mandates to strengthen privacy and security protections for health information. It introduces new requirements for organizations that manage PHI to notify individuals if there is a breach that discloses their PHI. A breach is defined as "the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information."[1]

In medical facilities, healthcare professionals need instant access to information. Laptops and terminals are increasingly mobile and are often positioned in high-traffic public areas, which can expose a patient's PHI to unintended viewers. Additionally, many insurance agents and healthcare professionals routinely enter and process sensitive information on laptops in open environments. Over the past few years, defenses like whole-disk encryption have become standard to protect stored information if a laptop is lost or stolen. Similarly, Virtual Private Networks (VPNs) and encrypted tunnels are typically used to transmit sensitive information over secure channels back to corporate servers. While these controls are important, protecting information during storage and transmission is not sufficient to keep health information secure. When PHI is displayed on a computer screen, it is at risk of exposure to passers-by. Visual privacy controls, such as privacy filters, are a vital and an under-addressed part of data security. They fill the gap by protecting information when it is entered, displayed, and used.

[1] The American Recovery and Reinvestment Act of 2009 http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:h1enr.pdf

Privacy and Compliance in Healthcare: An Overview

Over the past few years, the digitization of medical records has created a significant burden on healthcare providers to keep information private. A wave of regulations and standards is now in place that put specific requirements on healthcare providers to protect information. Beyond storage and transmission, providers have an obligation to protect data as it is viewed. Some important laws/standards to consider are:

Health Insurance Portability and Accountability Act (HIPAA):

Enacted in 1996, HIPAA defines guidelines for managing Personal Health Information ("PHI"). The Privacy Rule requires that covered entities limit the circumstances where PHI may be used or disclosed. The Security Rule requires that covered entities maintain physical and technical safeguards to protect PHI against any reasonably anticipated risks.

Health Information Technology for Economic and Clinical Health Act (HITECH):

The HITECH Act was signed into law as a part of the America Recovery and Reinvestment Act of 2009. It introduces additional provisions that increase the use of technology in managing healthcare information. The Act also includes new breach notification requirements to inform individuals if their PHI is exposed.

In fact, HIPAA requires physical safeguards, defined as "physical measures, policies and procedures to protect a covered entity's electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorized intrusion."[2] A *defense-in-depth* approach to information security requires that data is protected while stored, transmitted and viewed. Privacy filters greatly reduce the risk of data exposure and preserve visual privacy by severely restricting the angle at which data can be seen, dramatically reducing or eliminating any potential exposure. Privacy filters can also give organizations more flexibility to place devices in locations that maximize productivity while preserving privacy instead of having to awkwardly angle monitors in public areas or completely isolate computers displaying sensitive information. 3M Privacy Filters lead the industry and come in a range of sizes and styles to protect laptops, desktops, mobile phones, and other electronic devices. For more information visit: http://www.3Mprivacyfilter.com.

[2] HIPAA Security Rule
http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf