3M
Privacy Filters

Visual Privacy in Healthcare

By Kate Borten, CISSP, CISM

In this age of electronic health records, we look to high-tech computer technology to help us implement privacy and security controls for confidential data. However, many privacy incidents and breaches occur because of human error and low-tech, rather than high-tech, shortcomings. The exposure of confidential patient information on a computer or smartphone display screen is a good example and highlights an important and often overlooked privacy and security risk – the issue of visual privacy.

HIPAA covered entities, including healthcare providers and plans, as well as HIPAA-defined business associates and their subcontractors and agents, are required to protect patient-identifiable information from unauthorized disclosure, including unauthorized snooping, and confidentiality breaches. An essential, required process for protecting this information is to perform periodic risk assessments. These risk assessments include identifying where PHI may be vulnerable to unauthorized disclosure or loss of confidentiality.

Security professionals have long recognized the value of regular physical "walk around" audits to uncover common vulnerabilities such as unattended logged-on workstations, confidential papers left on printers and fax machines, and exposed display screens on desktop workstations, rolling carts, and handheld mobile devices. This type of audit should follow a standard checklist and be performed routinely, such as monthly. In all but the smallest organizations it makes sense to assign this responsibility to department managers, with completed checklists returned to the privacy and/or security officer for ongoing analysis and documentation. In addition, the privacy and security officers should perform random audits themselves to ensure that the organization continues to protect patient-identifiable information and shore up all vulnerable areas where a visual data breach could occur. The privacy and security officers, or their designees, should review all results to identify any common weakness across the organization or any particular department with a significant number of problems.

Mitigating the privacy and security risks resulting from these physical vulnerabilities is usually straightforward. If the problem is with human behavior, such as failure to log off or failure to shred papers, then focused re-training is appropriate. If the problem is

Discussing HIPAA Privacy and Security Rules

Both the HIPAA Privacy Rule and the HIPAA Security Rule are written to ensure that patient-identifiable information stays protected. Some key highlights from each rule include:

HIPAA Privacy Rule 45 CFR 164.530(c)[1]
This portion of HIPAA's Privacy Rule states organizations "must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." Further, organizations "must reasonably safeguard protected health information [PHI] from any intentional or unintentional use or disclosure that is in violation [of the privacy rule]," and "must reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure." Limiting incidental uses and disclosures means that if there is a reasonable solution or control, it should be used.

HIPAA Security Rule 45 CFR 164.310(b)[2] – Workstation Use
HIPAA's security rule 45 CFR 164.310(b) requires that organizations "[i]mplement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information."

display screen exposure for fixed location devices, then organizations can move or reposition computer monitors. However, in many healthcare provider settings such as at a registration desk or at a nursing station, either desktop computers cannot be relocated without disrupting the workflow and employee productivity, or there is no screen angle that prevents unauthorized individuals – particularly patients, visitors, and other outsiders – from reading a screen. In that case, in addition to reminding the workforce not to leave patient data displayed when no longer needed, privacy screens or filters are the obvious reasonable and appropriate solution.

If the problem is display screen exposure for mobile devices including computers-on-wheels, handheld tablets, and smartphones, relocating or re-orienting the screen is normally not an option. Hence, the typical mitigation strategies include use of screen savers, user awareness training, and privacy filters

Regardless of whether or not display screen exposure is a problem within an organization, it is almost certainly a problem offsite. Users who access patient data at home, in other facilities or in patients' homes, and while traveling should have heightened awareness of the potential risk of unauthorized disclosure and how to reduce that risk. Once again, screen savers and use of privacy screen filters or films are invaluable privacy and security tools, as is educating mobile and other offsite workers about this risk.

Finally, the risk assessment and mitigation cycle requires monitoring for improvement. Organizations should be sure to repeat the physical audit and analyze the results to ensure both regulatory compliance and good privacy and security practice. While there are no perfect solutions, privacy screens or filters play an important role in achieving and maintaining visual privacy and security.

[1-2] The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules

HIPAA Enforcement

The 2009 American Recovery and Reinvestment Act's subset on healthcare, the HITECH Act, increases HIPAA's privacy and security rules as well as their enforcement. Here are several key points from the law.

Section *13411. Audits* requires the US Department of Health and Human Services (HHS) to provide for periodic compliance audits of both covered entities and their business associates.

Section *13410. Improved Enforcement* significantly increased civil monetary penalties for non-compliance. The civil penalties are now broken down into tiers based on whether there is willful neglect and whether or not the non-compliance is corrected. However, in each tier, including the lowest, the government is permitted to assess as much as $1.5 million for repeat violations of the same provision within a calendar year. Note that there is no overall cap on penalties for violations of multiple regulatory provisions. HHS is now required to investigate any complaint if preliminary investigation indicates possible willful neglect. Further, HHS is required to assess a monetary penalty in any case involving willful neglect. Note that penalties are now applicable to business associates as well as covered entities.

In the future individuals who are harmed by the privacy or security violation will be entitled to a percentage of any monetary penalty or settlement. Adding to the ranks of enforcers, the law permits state attorneys general to bring civil action on behalf of residents who have been threatened or adversely affected by HIPAA and HITECH Act privacy or security violations. These changes mean that individuals and their lawyers will be more likely in the future to take a legal stand when the privacy and security of their protected health information is violated.