Ten Activities to Safeguard Patient Privacy in Urgent Care

Alan A. Ayers, MBA, MAcc
Content Advisor, Urgent Care Association of America
Vice President of Strategy and Execution, Concentra Urgent Care

According to the FTC, medical identity theft is the nation's fastest growing crime—fueled by growing numbers of uninsured, organized fraud rings, and prescription drug seekers. Consumers are increasingly concerned about the security of their health and financial data and consider how well a medical provider safeguards their privacy an integral part of a quality patient experience. Moreover, obtaining and disclosing protected health information (PHI) in violation of HIPAA can result in stiff civil and criminal penalties for an urgent care operator.

The following ten activities can help your center reduce the risk of unauthorized disclosure of protected health information:

1. CONDUCT A PRIVACY AUDIT
A privacy audit starts by identifying the ways PHI is collected, stored, and transmitted at your facility. Walk through every process from registration to discharge from the perspective of employees and patients, observing every verbal exchange, paper form, and computer entry. Scrutinize existing processes for ways that privacy could be breached and correct any deficiencies. Verify that a Notice of Privacy (NOP) is provided every patient and is posted in plain sight near the front desk. Patients should also sign an acknowledgement that they read and understand the NOP and authorize the use of PHI for activities not directly related to treatment.

2. TRAIN YOUR STAFF ON HIPAA
Every provider and staff member should be able to articulate the scope of HIPAA regulations, describe examples of PHI, and differentiate between authorized and unauthorized disclosures. In addition to training every new hire on HIPAA compliance, veteran staff should complete "refresher" privacy training every year. Role playing involving common disclosure scenarios makes training more relevant and memorable. A well-trained staff will be able to anticipate and prevent unauthorized disclosures and offer process improvements to reduce the risk of a HIPAA violation.

3. CONSIDER THE PATIENT SIGN-IN SHEET
The front desk should monitor who enters the facility and passes from the waiting room to the clinical treatment areas. Many urgent care centers have patients "sign in" upon arrival. The sign-in sheet provides an important operational record but many urgent care patients consider the fact they even presented at the center to be a disclosure. Although some centers use a black magic marker to conceal the names of patients who have been checked in, the best solution is either to keep the list behind the front desk (with a staff member writing patient names) or to use "peel off" sticker kits available through medical supply houses. All visitors—including vendors—should be identified before receiving access to areas containing PHI and non-staff members should not be permitted to walk the facility without a staff escort.

4. DESIGNATE STAFF-ESCORT AND STAFF-ONLY AREAS
Areas where patients are treated—and thus PHI may be present—should require a staff escort at all times. Signage on the door from the waiting room to the clinical treatment area should indicate that for patient privacy, patients and visitors should be escorted beyond this point. Areas where PHI is processed and stored—including clinical workstations, the front office, and file rooms—should be off-limits to everyone except for authorized staff. Computers, fax machines, and copiers should be placed only in these areas, which should be segregated by doors, walls, and other physical barriers. Signage should indicate that for patient privacy, only staff members may enter the restricted area.

5. KEEP PATIENT RECORDS, PAPERS AND COMPUTER MONITORS OUT OF VIEW
Patients and visitors should not be able to read or reach for paperwork in the work areas where it's processed. In addition to a physical barrier—such as an elevated countertop—computer monitors should face away from view and contain peripheral "privacy shields." Patient charts not being worked on should be closed or flipped over, charts should never be left in exam rooms, and if it's necessary for staff to step away from a task, the chart should never be left unattended. File rooms and doctors offices should be locked at night.

6. HAVE ELECTRIC SHREDER OR LOCKED SHRED BINS AVAILABLE

Documents containing PHI that are no longer needed should be shred or disposed of in proper containers—never in the trash where they may be recovered by "dumpster divers." Electronic paper shredders should be HIPAA compliant "cross-" or "confetti-shredders." If shred bins are used, they should be locked and a reputable mobile shredding service—specializing in medical practices—should empty bins on a regularly scheduled basis.

7. LIMIT CONVERSATIONS ABOUT PATIENT HEALTH INFORMATION

Staff should always be aware of who is around them and what information could be overheard. If it's necessary to discuss a patient's health information, defer such communications to areas where patients and visitors cannot overhear and then speak in a controlled volume. Common indiscretions include discharging or counseling patients in the hallway, discussing cases in work areas or at the front desk, and telephone calls to ancillary providers. Health information must be strictly on a "need to know" basis for doing one's job—staff should never peruse patient charts out of curiosity or gossip about a patient's health or service encounter.

8. VERIFY TELEPHONE AND FAX NUMBERS; MAIL AND EMAIL ADDRESSES

Utmost care should be taken to assure that external communications get to the intended recipient. One of the most common privacy breaches is sending patient information to an incorrect fax number. Dialing errors may be prevented by pre-programming the fax machine with frequently used numbers or calling recipients to verify the correct fax number prior to sending. A further precaution is to call after sending to assure the fax was received by the intended party. To assure correct contact information is on file, the front office should ask patients to verify their demographics prior to every visit—a practice that also improves billing accuracy and collections success.

9. REQUIRE INDIVIDUAL PASSWORDS AND ACTIVATE SCREEN SAVERS

Staff members should have unique and confidential individual password access to the applications they are authorized to use and staff should never be permitted to share passwords. Placing a password on a Post-it Note adjacent to the monitor is an invitation for unauthorized use that makes it impossible to track indiscretions to specific individuals. Similarly, several minutes of computer inactivity should activate a "screen saver" to conceal any PHI and once inactive, users should have to re-enter their passwords to resume work.

10. CONSIDER AND ACT UPON PATIENT COMMENTS

Although patients may not know the intracacies of HIPAA and what constitutes an unauthorized disclosure, they are sensitive and will often make comments about activities and processes they feel compromise their privacy. Patient perceptions should always be taken seriously, evaluated, and if appropriate—acted upon. If, for example, a patient comments that others in the waiting room can hear his interactions with the front desk, then a solution may be to construct a privacy barrier or ask patients to step into an office to discuss their concerns. Patients should also be informed—beyond the requisite NOP—of the center's special efforts to protect their privacy.