Tackling Non-Acute Care's Unique Privacy and Security Challenges

By Mary Butler

Patient privacy is at a true premium in retail pharmacies. Patients can choose to present at a drive-thru window, a desk that shares space with a cash register or two, a consultation window, or a script drop-off area where the only privacy barrier is behind the counter. Often, the only real nod to privacy is a sign saying "the line forms here" three or four feet away from the counter.

Pharmacists frequently dispense medications with minimal verification of identity as patients often send friends, spouses, relatives, or caregivers to pick up their prescriptions. Patients who don't want a line full of other customers to overhear their personal questions about side effects or interactions might wait until they get home to call a pharmacist with questions, and conscientious pharmacists might call patients about concerns themselves since the retail setting isn't always conducive to private discussions.

While chain retail pharmacies usually have corporate privacy officers, compliance with HIPAA is usually left in the hands of the pharmacist, who must do their best while juggling competing priorities. It's true that identification verification is less stringent in pharmacies, but that doesn't mean they get a pass on HIPAA. In 2009, CVS paid a $2.25 million fine to the Department of Health and Human Services' Office for Civil Rights (OCR) and instituted a corrective action plan to ensure that it will appropriately dispose of protected health information (PHI), such as labels on prescription bottles and old prescriptions.[1] This came after OCR learned that several CVS pharmacies exposed the PHI of hundreds of patients when it disposed of pill bottles in unsecured dumpsters.

Like other non-acute HIPAA-covered entities—such as long-term care facilities, ambulatory clinics, rehabilitation settings, mental health facilities, telehealth providers, and home health providers—pharmacies are left to comply with privacy and security regulations without the staff and other resources that hospitals and other acute providers enjoy. And that's not because privacy and security are any less important.

Non-acute care areas face unique privacy and security challenges. For example, many hospice patients are too ill when they arrive to provide proper consent for privacy authorizations. Also, non-acute care can face special regulations—substance abuse and behavioral health facilities are covered by special privacy regulations (42 CFR Part 2), which pose additional privacy and security challenges. And in February 2018 OCR announced that Fresenius Medical Care North America, which owns a chain of dialysis infusion centers that offer services for individuals with kidney failure, agreed to pay $3.5 million in fines and adopt a corrective action plan as a result of five separate privacy breach events.[2]

As the provision of healthcare increasingly moves beyond acute care settings, it's become even more important that health information management (HIM) professionals understand the nuances of safeguarding PHI wherever it resides and understand the unique challenges in non-acute settings.

Maintaining Privacy in Mental Health and Telemental Health

The state of Missouri is in a unique position thanks to a Centers for Medicare and Medicaid Services (CMS) pilot project focused on delivering quality mental health services in rural areas. The Excellence in Mental Health Act demonstration program is a two-year eight-state initiative to expand Americans' access to mental health and addiction care in community-based settings. Brenda Fuller, RHIA, CHPS, vice president of HIM and data reporting for Compass Health, which provides behavioral health services, dental health services, and primary care in federally qualified health centers, is working to implement the pilot project in Compass Health's 14 locations.

Fuller helps oversee all of the HIM functions in Compass's network, from electronic record implementations to release of information (ROI), but the behavioral health component is one of the most challenging.

"Most behavioral health clinics such as ours—formally called Community Behavioral Health Clinics—have typically not had enough funding or providers to serve everyone who presents with mental illness, thus creating the need for individuals in management to wear many hats. Time has improved the 'many hats' situation but we often still struggle with hiring enough providers to meet the needs of those we serve," Fuller says.

Still, it's part of Compass's mission to be a one-stop shop for its population's healthcare needs, providing primary care, dental care, and behavioral health services all in one location. Fuller's first challenge when she started working for Compass was to implement an electronic health record (EHR) system that could reliably protect the sensitive mental health details of those patients that also seek dental and primary care at the clinics. This is particularly tricky because all of the clinic's prescribers need to see a given patient's medication list so that they don't unknowingly prescribe opioids to a patient who isn't supposed to have them, or who is already getting them from another doctor.

"Because we focus on behavioral health and that's who we serve the most of, we had to make sure our particular [EHR] vendor was able to do all of it—whether it was primary care or adding that dental software. That was a long vetting process. You have to have a vendor that can do all, but so far so good," Fuller says.

In her role, Fuller also helps the clinic facilitate telemental health visits and coordinate in-home behavioral healthcare, where caseworkers see patients in their homes. Individuals needing care can come into a Compass clinic and be set up in a room with a video link to a therapist working remotely. A nurse is usually present throughout the encounter and assists the therapist in checking vital signs and taking notes. Fuller makes sure the visits are HIPAA-compliant and that the video link is encrypted and secure.

Providing behavioral health in the home presents additional challenges, however, because the patients often don't have reliable Wi-Fi or broadband internet connections.

"One of the biggest fears is losing that documentation. You type, thinking it's saving what you're typing, only to find out it's not," Fuller says, noting that this is part of the CMS pilot project they're still perfecting. "There was a pilot started a few years ago where they did get disconnected. We're being extra careful to make sure we haven't lost information. We initially had login connectivity issues in getting our own staff into it, but we've gotten beyond that."

The caseworkers sent to patients' homes do their documentation on an iPad and upload patient data into the EHR when they get back to the office. In-home behavioral healthcare can be unpredictable, and clients can occasionally become violent. That's why, Fuller says, the iPads used for documentation are equipped with protective cases to minimize damage if they are thrown.

One thing Compass clinics have that other comparable community health clinics don't is a robust clinical documentation improvement (CDI) department, even though the clinic doesn't have coding professionals due to the limited number of codes they use. "We are fortunate here to have a strong CDI department and they work hand-in-hand with compliance creating a strong audit/compliance plan," Fuller says.

Privacy Challenges in Long-Term Care

The need for HIM professionals in long-term care (LTC) is as vital as it is in acute care, but due to funding issues in that setting and the fact that college HIM programs place less focus on it, HIM professionals with LTC experience are harder to find. To correct this, some states have tried to pass legislation requiring LTC facilities to have credentialed HIM individuals on staff. AHIMA supported proposed legislation to this effect in the state of Missouri, but the bill stalled. In most cases, the required position of privacy officer in LTC is filled by a facility's administrator. Many LTC centers hire HIM consultants who visit on a quarterly basis to review business associate agreements and monitor compliance in other areas.

That's a responsibility that Deanna Peterson, MHA, RHIA, CHPS, vice president of health information consulting at First Class Solutions, fulfills for many LTC facilities. Peterson visits LTC providers in Missouri and Illinois on a quarterly basis. She helps these providers with oversight of electronic devices; reviewing release of information policies; and conducting documentation audits, which includes verifying that facility residents have set up a power of attorney, and making sure facilities

have a good system in place so that when patients leave the facility for outside doctor's appointments their visit notes get integrated into their chart.

One difference between acute care and LTC is the matter of the Notice of Privacy Practices, which Peterson says are updated less frequently in LTC. "There was so much more awareness in acute care settings in 2013 when HITECH came through. That wasn't so prominent in LTC, so every now and then, if I get a new client, I'll still see outdated Notice of Privacy Practices," Peterson says.

There's a similar gap when it comes to ROI. "That basic knowledge of ROI requirements and [understanding of] what you can and can't do is typically not there," Peterson says. "So maybe they got a crash course in their HIPAA orientation on treatment, payment, and operation. But the really in-depth knowledge of ROI—researching state regulations as far as the chain of custody when a resident expires, some of that knowledge is not there. The access clarification that HHS made in 2016, just clarifying what you can and can't charge for copies of medical records—there's not an awareness in LTC."

Debbie Johnson Hewgley, RHIT, CHP, director of HIM and privacy officer for Lifecare Centers of America, oversees privacy policies for the company's 200-plus skilled nursing facilities (SNFs). A constant struggle she sees stems from the fact that SNFs are still very much in a hybrid environment with paper records and electronic records both in use. They are also more reliant on fax machines than other provider types for getting records from one provider to another—and this can lead, on occasion, to records being faxed to the wrong number, resulting in a breach.

HIPAA-compliant record retention and ROI has an extra layer of complexity in LTC due to the average length of stay for patients. Many providers are continuing care retirement communities offering independent living, assisted living, and skilled nursing care, which means patients could have records going back 20 years or more. Despite this, Hewgley says her company has a policy that it must make a patient's records available within two days upon request—even when records need to be retrieved from its off-site storage facility.

Additionally, LTC facilities aren't immune to the cybersecurity events that hit hospitals or insurers. "We get phishing emails and calls from people saying they're the Microsoft help desk—all of that social engineering—we get that too," Hewgley says. "My advice to HIM professionals in LTC is to be as prudent watching your privacy and security as if you worked in a large hospital."

Privacy and Security in the Federal Aviation Administration

At first glance, the Federal Aviation Administration (FAA) doesn't appear to be a covered entity in a HIPAA sense, but dedicated HIM professionals do work there to help ensure the privacy of its records are protected. According to Christy Hileman, MBA, RHIA, CCS, team coordinator, autopsy records administrator at the FAA's Civil Aerospace Medical Institute, the FAA is considered a public health authority under HIPAA like other government health agencies such as the Centers for Disease Control and Prevention. This means that the FAA has to follow HIPAA regulations when it obtains medical records for research initiatives. However, when Hileman's division works with pilot medical evaluations and autopsy records, it is subject to the Privacy Act of 1974.

Every year the FAA investigates between 280 and 300 fatal aircraft accidents—including commercial aircrafts, hot air balloons, helicopters, gliders, private planes, and jets. The Civil Aerospace Medical Institute is a research division that, among other tasks, manages autopsy records for pilots killed in aircraft accidents. Autopsy records are used for two purposes: to help determine the reason an accident occurred, and for research.

Hileman also must be familiar with retention rules that apply to government documents, including guidelines set forth by the National Archives. Other records kept by the FAA, such as pilot toxicology records, can be accessed under the Freedom of Information Act (FOIA). The conflicting privacy laws can create a difficult challenge in her work. For example, under HIPAA, a deceased individual's records are kept private for 50 years, whereas under the Privacy Act of 1974, a deceased person's records can be obtained through a FOIA request any time after they die.

One of the most significant privacy and security challenges at the FAA is the fact that US government agencies are a huge target for hackers from rogue nations. "At the FAA, we have privacy and security rules set by the government, which sets

standards. We have to use encryption—it's the same for HIPAA as for us. Being a government entity, we're constantly inundated by foreign countries trying to get our information. We have to protect our assets," Hileman says.

Notes

1. Department of Health and Human Services. "Resolution Agreement: CVS Pays $2.25 Million & Toughens Disposal Practices to Settle HIPAA Privacy Case." February 18, 2009. www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/cvs/index.html.
2. Department of Health and Human Services. "Five breaches add up to millions in settlement costs for entity that failed to heed HIPAA's risk analysis and risk management rules." February 1, 2018. www.hhs.gov/about/news/2018/02/01/five-breaches-add-millions-settlement-costs-entity-failed-heed-hipaa-s-risk-analysis-and-risk.html.

Mary Butler (mary.butler@ahima.org) is associate editor at the *Journal of AHIMA*.

Article citation:
Butler, Mary. "Tackling Non-Acute Care's Unique Privacy and Security Challenges." *Journal of AHIMA* 90, no. 2 (February 2019): 14-17.