Codify
BY AAPC

Health Information Compliance Alert

Enforcement News: Texting Orders? Make Sure You Have These Safeguards In Place

Plus: State negligence laws capture data breach lawsuits that fall through HIPAA's cracks.

As technology and communications evolve in the healthcare industry, there are bound to be new questions about how to keep these new methods safe and secure. Texting is one such emerging communication method that has remained under scrutiny.

On April 29, **The Joint Commission** updated its position on the use of texting for orders in the May issue of Joint Commission Perspectives. According to the update, the Joint Commission says that practitioners can use secure texting services for managing orders, but there are some caveats.

"Licensed independent practitioners or other practitioners in accordance with professional standards of practice, law and regulation, and policies and procedures may text orders as long as a secure text messaging platform is used and the required components of an order are included," the Joint Commission states.

Best bet: Specifically, the Joint Commission believes that the text messaging platform used should include:

- A secure sign-on process;
- Encrypted messaging;
- Delivery and read receipts;
- Date and time stamps;
- Customized message retention timeframes; and
- A specified contact list for individuals authorized to receive and record orders.

Also, the Joint Commission advises healthcare organizations that allow text orders to:

- Develop an attestation documenting the capabilities of their secure text messaging platform;
- Define when text orders are or are not appropriate;
- Monitor how frequently practitioners use texting for orders;
- Assess compliance with texting policies and procedures;
- Develop a risk-management strategy and perform a risk assessment; and
- Conduct training for staff, licensed independent practitioners, and other practitioners on applicable policies and procedures.

Resource: You can access the Joint Commission's updated position on texting for orders at www.jointcommission.org/assets/1/6/Update_Texting_Orders.pdf.

Keep An Eye On Your Employees: Stolen Data Leads To Class-Action Suit

Just because HIPAA doesn't allow a private right of action for breach cases doesn't mean you're safe from these types of claims in class-action lawsuits. Where you might escape such claims under federal law, you'll likely be subject to an applicable state law.

In May, the **U.S. District Court for the Southern District of Florida** accepted a dismissal from the parties involved in

Weinberg v. Advanced Data Processing, Inc. (15-CV-61598), a HIPAA data breach case. The court had previously dismissed the plaintiff's claim for breach of fiduciary duty, but the negligence and unjust enrichment claims went forward, according to a May 19 analysis by the law firm **Nixon Peabody LLP**.

Background: In 2012, the healthcare payment and data processing company **Intermedix**, owned by **Advanced Data Processing** (ADP), suffered a data breach. An employee accessed the personal information of potentially thousands of patients who used ambulances and for whom Intermedix provided billing and payment processing, Nixon Peabody reported.

The putative class-action lawsuit alleged that the employee used the stolen data to file fraudulent tax returns and obtain tax refunds using the victims' identities. The plaintiffs claimed that Intermedix failed to supervise employees' access to patient data, and failed to notify potential victims of the breach in a timely manner (notification purportedly didn't occur until late 2014).

The court ruled that although the negligence and unjust enrichment claims weren't feasible under HIPAA because the law doesn't provide a private right of action, these claims were viable under Florida's state laws. Florida's "undertaker doctrine" imposes a duty to act carefully upon someone who voluntarily provides a service to others, the law firm explained.

The parties participated in court-ordered mediation and agreed to dismiss the case under settlement terms that weren't made public. "Although the court had determined that the negligence claim could not be maintained under HIPAA, the Intermedix case serves as an important reminder that all companies which collect or maintain personal information, such as Social Security numbers, may face claims of negligence under state law for failing to ensure the privacy and security of such information."

Best practices: Nixon Peabody offers the following tips to avoid this type of breach in your organization:

- Ensure your data privacy and security policies and procedures address and limit, to the extent possible, unauthorized access by not only external sources, but also internal staff who are acting beyond the scope of their employment;
- Implement data privacy training for all employees at hire and periodically thereafter;
- Routinely monitor employee compliance with your policies and procedures;
- Include in your hiring and disciplinary policies the intentional misuse of data by employees; and
- Ensure your data privacy and security policies address timely investigations of potential breaches, as well as issuing breach notifications to state and federal authorities and impacting individuals.

Breaches In May Show Few Reported By BAs

Although the average number of reported large breaches per month is at an all-time high, breaches reported by business associates (BAs) are still few and far between. The idea that BAs are simply not experiencing as many breaches as healthcare providers and health plans seems highly unlikely, so are BAs simply not reporting breaches like they should?

Of the 22 total large-scale breaches (affecting 500 or more individuals) during the month of May, only one was reported by a BA. Most breach reports came from healthcare providers (16 reports) and health plans (five reports).

Keeping with the current trends, May's large breaches were mostly due to hacking/IT incidents (nine) and unauthorized access/disclosure (eight), with five breaches related to theft. Most incidents also involved paper/films (five), with four involving network servers, three electronic medical records (EMRs), two email, two laptops, and one desktop computer. Several other reported breaches involved a combination of desktop computer and network server, EMR and network server, EMR and paper/films, and laptop and other portable electronic device.

The largest breach in May was reported by a healthcare provider, **California Correctional Health Care Services**. The

breach affected 400,000 individuals and arose from the theft of a laptop.

Link: To view reported large-scale HIPAA breaches, visit OCR's so-called "Wall of Shame" at https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.