Health Information Compliance Alert

HIPAA Compliance: HIPAA In 2015: Prepare Yourself For 5 Big Trends

Prediction: State law claims will continue to facilitate breach lawsuits.

What does 2015 have in store for HIPAA compliance requirements and pitfalls? The experts have wasted no time weighing in, and they've identified the following major trends for the coming year:

1. Get Ready for Tougher OCR Audits

One of the biggest trends for HIPAA compliance in the year ahead will be the **HHS Office for Civil Rights**' (OCR) stepped-up audit program. Also look for increased penalties against entities that violate HIPAA, warned attorneys **Bruce Platt** and **Robert Slavkin** in a Jan. 8 blog posting for the law firm **Akerman LLP**. The Affordable Care Act (ACA) and Meaningful Use programs also both pose unique security challenges to the healthcare industry.

Beware: "The attention and enforcement actions from OCR are likely to be on an order that U.S. providers and other covered entities [CEs] simply haven't seen before, and it's going to take many by surprise," cautioned **Mark Fulford** in a Jan. 14 blog posting for **LBMC Security & Risk Services**. If OCR finds you not in compliance with HIPAA requirements, the consequences may be serious.

"We expect OCR to exercise new levels of scrutiny and enforcement in order to identify healthcare organizations' particular risks," Fulford said. Further, OCR will take steps to ensure that you mitigate risks and respond to rising threats.

Also, use of the OCR online complaint system will continue to increase this year, thanks to a $2-million budget increase for OCR in fiscal year 2015, noted attorney Elizabeth Litten in a Dec. 30, 2014 blog posting for the law firm **Fox Rothschild LLP**. This will result in increased OCR compliance investigations, audits, and enforcement actions.

2. Watch for Lawsuits Based on State Law Claims

Despite HIPAA's lack of private right of action, plaintiffs haven't shied away from bringing lawsuits following breaches in state courts and plaintiffs have won several of these cases.

Last year, individual plaintiffs prevailed in several cases with settlements and jury verdicts for alleged HIPAA violations, pointed out attorney Linn Foster Freedman in a Jan. 8 analysis for the law firm Nixon Peabody LLP. These cases were "presumably based on state law claims."

Watch out: "These were cases of first impression and will no doubt gain speed in 2015," Freedman predicted. "Therefore, medical providers should be aware of this precedent and continue to focus on HIPAA compliance."

3. Protect Against Cybercriminals

"We anticipate that [2015] will be another year of damaging and costly cyber-attacks," Fulford warned.

After a multitude of cyber-attacks and hacking incidents last year across many industries, "there will likely be more persistent threats to healthcare data in 2015," Platt and Slavkin agreed. Accidental data leaks are not uncommon in healthcare, and "hackers will take full advantage of those opportunities."

Pitfall: "And with more data storage on 'cloud' based servers, healthcare data makes for an attractive target for cybercriminals," Platt and Slavkin cautioned. As a result, enforcement efforts will likely increasingly focus on employee training, review of systems security, and third-party review to verify that you are as protected from cyber threats as you can be.

You and your BAs must prepare for these risks to mitigate or avoid them altogether, Fulford stressed. Ultimately, all parties involved with PHI "must work together to protect sensitive data, especially as electronic records are expected to grow more and more common in 2015."

4. Beef Up Your BAAs

With so many CEs getting into hot water lately due to their BAs' mistakes, BA Agreements (BAAs) will likely become more sophisticated, detailed and frequently negotiated, Litten predicted.

For example: CEs may require their BAs to implement very specific security controls, perhaps relating to particular circumstances, or comply with a specific state law's privacy and security requirements, Litten posited. BAAs may limit the creation or use of de-identified data derived from the CE's PHI or require the BA to purchase cybersecurity insurance.

"In short, the BAA will increasingly be seen as the net (holes, tangles, snags and all) through which the underlying business deal must flow," Litten noted. "As a matter of fact, the financial risks that can flow from a HIPAA breach can easily dwarf the value of the deal itself."

5. Comply with the TCPA

Hidden trap: Yet another concern for the healthcare industry in terms of privacy and security is compliance with yet another federal law: the Telephone Consumer Protection Act (TCPA). Due to the rising trend of using technology like text messaging to patients' mobile phones for appointment or prescription refill reminders, providers need to be wary of their compliance with the TCPA, Freedman said.

"TCPA continues to be a minefield for compliance," Freedman noted. In fact, a case was filed in late 2014 against a pharmacy for texting patients with refill reminders.

"TCPA requires that the express written consent of the patient must be obtained prior to texting a patient," Freedman instructed. "If you plan to text patients at all, take the time now to update your patient intake form to include 'express written consent' to text the patient on their cellphone."