Codify
BY AAPC

Health Information Compliance Alert

Enforcement News: Watch Out: Upcoming HIPAA Audits Will Be 'Aggressive'

Plus: FBI knows how much money your patient's PHI is worth.

Keep your eyes peeled this autumn for a notification and data request from the **HHS Office for Civil Rights** (OCR). If you receive these communications, your practice is one of the selected entities that will face a more vigorous HIPAA audit.

OCR plans to audit 350 covered entities (CEs) and 50 business associates (BAs) during the first round of audits. For those who receive the notification and data request in Fall 2014, "the lucky recipients will be the first participants in the OCR's effort to adopt a more aggressive approach to investigating compliance with HIPAA standards for privacy, security and breach notification," wrote Tampa, FL-based **Akerman LLP** associate attorney **A. Crosby Crane** in a May 1 posting for the firm's Health Law Rx Blog.

Why? The more aggressive approach stems from the December 2013 **HHS Office of Inspector General** (OIG) report that slammed the OCR for falling behind on HIPAA enforcement, Crane said. OCR has been making headway in implementing a permanent audit program, instead of relying on complaints as a way to assess compliance.

And the looming permanent audit program "could translate into open season" on CEs and BAs, Crane warned. That's because OCR is no longer favoring voluntary compliance or corrective actions as opposed to monetary settlements as it has in the past. "Many privacy and security experts believe large settlements will become increasingly common as a result of the OCR's increased enforcement efforts," he cautioned.

Protect yourself: You can get a leg up on preparing your practice for the upcoming HIPAA audits by taking a close look at your risk assessment. Crane recommended using the security risk assessment tool that HHS released in March (www.healthit.gov/providers-professionals/security-risk-assessment).

Although using the tool won't guarantee that you'll survive an audit unscathed, "its use very likely will be a factor in how the government views a provider's overall compliance efforts," Crane explained. "Just how much of a factor remains to be seen, but a prudent HIPAA compliance program would be well served to use the tools provided by HHS."

What The FBI Has To Say About PHI Security

How valuable is your patients' PHI? Can you quantify each patient's record in a dollar amount? Well, the **FBI's** Cyber Division apparently can.

On April 8, the agency issued a Private Industry Notification entitled, "Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain." The Notification generally classifies the state of information security in healthcare, according to **Jim Sheldon-Dean**, founder and director of compliance services for **Lewis Creek System, LLC** in Charlotte, VT.

So what did the FBI conclude? First, healthcare entities are implementing security measures insufficiently, breaches are widespread, and the rapid increase in electronic health record (EHR) implementation is leaving the healthcare industry vulnerable, Sheldon-Dean reported.

Another interesting tidbit from the FBI was that the agency believes PHI is far more valuable than financial data PHI is worth $50 per record, while financial information is valued at just $1 per record. You can read the Notification at www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.

CPT® 2023 American Medical Association. All rights reserved.

Avoid The Top 5 Investigated HIPAA-Compliance Issues

With all of the breaches, enforcement actions and audits swirling around the HIPAA stratosphere, you'd better prepare yourself with some basic information. For example, do you know what types of covered entities (CEs) are most likely to face corrective action?

As of March 31, the **HHS Office for Civil Rights** (OCR) has compiled and analyzed enforcement data to reveal the most common compliance issues investigated and the most common types of CEs who've faced corrective action. According to OCR, the most common compliance issues investigated are (in order of frequency):

1. Impermissible uses and disclosures of protected health information (PHI);
2. Lack of safeguards of PHI;
3. Lack of patient access to their PHI;
4. Uses or disclosures of more than the minimum necessary PHI; and
5. Lack of administrative safeguards of electronic PHI (ePHI).

And the most common types of providers required to take corrective action for voluntary compliance are (in order of frequency):

1. Private practices;
2. General hospitals;
3. Outpatient facilities;
4. Health plans (group health plans and health insurance issuers); and
5. Pharmacies.

Resource: To stay abreast of these HIPAA enforcement statistics, visit OCR's Enforcement Highlights webpage at www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/index.html.

Heads Up: Your Practice's Own Info Is Now On Display

You know how the **U.S. Department of Health & Human Services** (HHS) feels about protecting patients' information, but protecting providers' data doesn't seem to rank very high on the department's agenda.

Case in point: On April 9, HHS announced the unprecedented release of data on providers who receive Medicare payments. The privacy-protected data on services and procedures provided to Medicare beneficiaries by healthcare professionals also shows payment and billing information by each provider.

The newly released data exposes such information on more than 880,000 providers who received a total of $77 billion in Medicare payments in 2012 under the Part B Fee-For-Service (FFS) program. The data set also allows comparisons by physician, specialty, location, types of services and procedures, Medicare payment, and submitted charges, HHS reports.

"Data transparency is a key aspect of transformation of the healthcare delivery system," **Centers for Medicare & Medicaid Services** (CMS) Administrator **Marilyn Tavenner** noted in the HHS press release. "While there's more work ahead, this data release will help beneficiaries and consumers better understand how care is delivered through the Medicare program."

And the data should provide researchers, policymakers, and the public a new insight into healthcare spending and physician practice patterns, HHS Secretary Kathleen Sebelius said in the April 9 statement. You can view the data set at www.cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/Medicare-Provider-Charge-Data/Physician-and-Other-Supplier.html.

Check Out These Free Compliance Tools

If you're thinking about redecorating your facility with some HIPAA-focused adornments, the website HealthIT.gov offers a treasure trove of posters, factsheets, brochures, and much more.

CPT® 2023 American Medical Association. All rights reserved.

All the downloadable materials are free and include banners and badges for your website, as well as educational presentations. The downloadable materials focus on privacy and security issues relating to mobile devices. To view the materials, go to www.healthit.gov/providers-professionals/downloadable-materials.

Example: To give you a sense of what the materials have to offer, here are the tips from HealthIT.gov's postcard, "10 Tips to Protect and Secure Health Information When Using a Mobile Device:"

1. Use a password or other user authentication.
2. Install and enable encryption.
3. Install and activate remote wiping or remote disabling.
4. Do not install or use file sharing applications.
5. Install and enable a firewall.
6. Install security software and keep it up to date.
7. Research mobile applications before downloading.
8. Always keep your device in your possession.
9. Use adequate security to send or receive health information over public Wi-Fi networks.
10. Delete all stored health information before discarding the mobile device.

CPT® 2023 American Medical Association. All rights reserved.