MINTZ

Bah, Humbug! HIPAA Compliance Isn’t Getting Any Easier

December 21, 2017 | Blog | By **Dianne J. Bourque**, **Ellen L. Janos**

VIEWPOINT TOPICS

- Health Care

RELATED PRACTICES

RELATED INDUSTRIES

As we look back on 2017, one message is clear: don't be a Scrooge when it comes to HIPAA compliance. With ever-evolving security threats and unrelenting enforcement, regulated entities must maintain a spirit of compliance that lasts the whole year through. It is in that spirit – and with apologies to Charles Dickens – that our HIPAA year in review is brought to you by the ghosts of HIPAA Past, HIPAA Present and HIPAA Yet to Come.

The Ghost of HIPAA Past

2017 continued to be haunted by large-scale data breaches. **As reported by our Privacy & Security colleagues**, Equifax announced one of the largest breaches in US history in September, which involved highly sensitive information such as social security numbers and birth dates. The Equifax breach didn't involve health information, but in July, OCR sent a clear message regarding the importance of health information security and **ratcheted up the fear factor** associated with its HIPAA Breach Reporting Tool (HBRT), commonly referred to as the HIPAA "Wall of Shame." The updates make it easier to search and view information about data breaches and make it harder for offenders to hide in the aftermath of a

breach.

It was similarly terrifying that 2017 required guidance on HIPAA and natural disasters, but in the aftermath of several large-scale natural disasters, OCR **issued guidance** to remind health care providers of how health information may be used and shared in a crisis, consistent with HIPAA standards.

The Ghost of HIPAA Present

Aggressive HIPAA enforcement remained an ever-present reality in 2017 and there were a number of notable settlements imposed on regulated entities large and small:

- OCR **settled its first enforcement action** for a health care provider's failure to timely report a breach to OCR, affected individuals, and the media. It cost the health care company $475,000.
- In April, **OCR announced** a tiny $31,000 settlement with a small health care provider for failing to produce a BAA with one of its business associates, and, just four days later, a separate $2.5 million settlement with a larger healthcare company for failing to implement sufficient HIPAA policies and procedures.
- Memorial Hermann, a large health system, **settled potential HIPAA violations** with OCR for $2.4 million after publicly disclosing a patient's name in the title of a press release regarding an incident at one of its clinics.

The Ghost of HIPAA Yet to Come

Of course, the Ghost of HIPAA Yet to Come is the scariest one of all. Iliana Peters, formerly OCR's Senior Advisor for HIPAA Compliance and Enforcement, and presently OCR's Acting Deputy Director for Health Information Privacy, provided **insight into HIPAA enforcement trends** and OCR's current and future agenda at the 2017 Health Care Compliance Association's annual "Compliance Institute." One of the highlights of Ms. Peters' presentation was the anticipated implementation of HITECH Act provisions requiring a percentage of civil monetary penalties or settlements collected by OCR to be shared with individuals affected by a HIPAA violation. Given OCR's willingness to impose seven-figure fines, it is likely that this development will incentivize data breach victims and others aggrieved by the privacy or security failures of a covered entity or business associate, and increase the stakes for non-compliance. Ms. Peters' presentation also referenced implementation of controversial updates to the HIPAA accounting rules which were passed as part of HITECH, but have yet to be implemented.

It's not all doom and gloom on the horizon, however. Earlier this week, OCR **released a new set of tools and initiatives** to help fight the nation's current opioid crisis and implement the 21st Century Cures Act. These tools support critical federal policy goals with the potential to have a significant, positive impact on health care. OCR has promised additional guidance in the coming months. So as 2017 winds down, there is reason to be hopeful for regulated entities that are willing to take advantage of available guidance and to learn from the mistakes of the past. Everything that we learned in 2017 can be used to support HIPAA compliance in the months and years ahead. So on that positive note, we wish everyone happy holidays and a 2018 that is free from the specter of non-compliance.

Authors

Dianne Bourque

Ellen L. Janos, Member Emerita

Ellen was previously a Member in Mintz's Health Law Practice and retired in 2024.