The Impact of a Health Data Breach

by Deven McGraw [1]
December 9, 2011

Since the breach notification requirements applicable to entities covered by HIPAA went into effect almost two years ago, we have seen numerous reports of large health information breaches. These reports identify the entities involved in the breach, the number of patient records breached, and the type of data believed to be potentially at risk. But rarely do those reports go into much detail on the impact (both financial and psychological) of the breach on either the patients whose data was part of the breach, or the provider entities experiencing the breach.

My friend Micky Tripathi, the President and CEO of the Massachusetts eHealth Collaborative, has written a blog post [2] on a recent breach experienced by his company that provides a very complete and thoughtful account of the incident and how they handled it.

Overall, I was very impressed (and heartened) by the degree of care and concern in the Massachusetts eHealth Collaborative’s response to this incident – but two other thoughts came to mind:

- The breach occurred due to the theft of a laptop containing patient identifiable data. The company had instituted an encryption policy and was seeking an encryption technology solution when the theft occurred. Although the files were not encrypted, the laptop was password protected, as were the patient files within the laptop. Nevertheless, the company concluded that there was a significant risk of harm for those individuals whose sensitive personal information (such as a social security number) had the potential to be accessed. I wonder how many other entities covered by the HIPAA breach notification provisions would have reached the same conclusion? (Recall that under currently applicable law, notification to individuals is only required [3] when there is a significant risk of harm to the individuals whose information is involved in the breach.)

- Micky notes that the Office for Civil Rights (OCR) has proposed regulations to enable OCR to hold downstream subcontractors accountable for potential violations of HIPAA privacy and security regulations and the HITECH breach notification requirements, but these regulations are not yet final and enforceable. Had the parties not been so responsible in responding to this breach, this uncertainty regarding the ability of OCR to hold downstream actors accountable could have been a significant problem. We really, really do need [4] the final HITECH rules to be issued.

Copyright © 2013 by Center for Democracy & Technology.
The content throughout this website that originates with CDT can be freely copied and used as long as you make no substantive changes and clearly give us credit. Details.

Source URL: https://cdt.org/blogs/deven-mcgraw/912impact-health-data-breach

Links:
[1] https://cdt.org/personnel/deven-mcgraw
[2] http://www.histalkpractice.com/2011/12/03/first-hand-experience-with-a-patient-data-security-breach-12311/
[3] http://www.cdt.org/blogs/harley-geiger/hhs-new-harm-standard-breach-notification
[4] http://www.cdt.org/files/pdfs/20111110_senate_HPP_testimony.pdf