Little Breaches: OCR Releases First “Small Breach” Data

Save to myBoK

By Kevin Heubusch

The Office for Civil Rights has been publicly reporting incidents of large-scale health data breaches since early 2010, but last month it reported to Congress numbers that the industry has only guessed at to date-the reports it has received of breaches involving fewer than 500 individuals.

OCR, it turns out, was flooded with reports of small breaches, logging more than 30,500 incidents for the 15-month period ending December 31, 2010. These "small" breaches were very small, the report reveals, with the majority involving information on a single individual, typically sent to an incorrect mail or e-mail address or an incorrect fax number.

The Breach Notification Rule

The HITECH Act requires covered entities notify individuals of breaches of their personal information. It also requires them to notify the Department of Health and Human Services, of which OCR is a part. Organizations must report breaches involving 500 or more individuals to HHS within 60 days; they may report smaller breaches annually, within 60 days of the end of the calendar year in which the breaches occurred.

HITECH requires HHS, in turn, to report the numbers to Congress annually. Last month's report, a relatively brief document, was the first.

The number of individuals affected is approximate, OCR notes in the report, because some organizations were not certain of the exact number of individuals affected in a given incident. OCR also notes that it has included in the report all incidents that organizations have reported, even if the incident may have been exempted from reporting through one of three caveats included in the breach notification rule.

Only unsecured data qualifies for a breach, so the reports do not include exposed, lost, or stolen data that were encrypted. The report also does not reflect breaches that the covered entity determined posed no financial or personal risk to the individual. The notification rule does not require organizations to notify individuals or HHS of such events.

The Numbers

Reporting began for incidents occurring on or after September 23, 2009. The report covers the period from that day to the end of the 2010 calendar year.

Big Is Big

The report's information on large-scale breaches was not news, as noted, but OCR's summary is a useful overview of the data. In the approximately 15 months ending December 31, 2010, HHS received 252 reports of large-scale breaches that involved approximately 7.8 million people. Organizations reported 207 breaches in 2010 alone, which offers an annual benchmark.

Theft was the leading cause of large breaches in both reporting periods, responsible for 52 percent of reported incidents and more than half of all individuals affected. Organizations choose from four causes of breach in 2009; in 2010 OCR added a fifth category of "improper disposal."

Small Is Small

Over the 15-month period ending December 31, 2010, OCR received approximately 30,500 reports of breaches involving fewer than 500 individuals. An estimated 62,000 people were affected.

Although the raw numbers suggest an average of two individuals affected per breach, in reality most breaches involved the information of a single person.

The reason is that the leading cause of small breaches was misdirected communications, typically a clinical or claims record mailed, e-mailed, or faxed to the incorrect individual.

At the root of these incidents were poorly compiled patient data and human error. Organizations reported fixing computer errors, training staff, and revising policies and procedures to address the root cause of the problems.

Dramatic Differences Separate Large and Small Breaches

Between the start of reporting on September 23, 2009, and the end of 2010, OCR received reports of nearly 31,000 breaches as defined by the breach notification rule. Fewer than 1 percent involved large-scale breaches, but those incidents accounted for 99 percent of all breached records.

Category	No. of reports	No. of Individuals Affected	Leading cause
500 or more individuals	252	7,800,000	Theft of paper records or electronic media
Fewer than 500 individuals	30,521	62,000	Misdirected communications

Remedial Actions

HITECH also requires HHS report to Congress the actions covered entities have taken in response to breaches. (These actions do not reflect remediation resulting from an OCR investigation.) The results offer all organizations a useful checklist of actions they can take to prevent breaches in the first place.

Organizations reporting breaches involving more than 500 individuals took the following remedial steps in reponse:

- Revising policies and procedures
- Improving physical security by installing new security systems or by relocating equipment or records to a more secure area
- Training or retraining workforce members who handle protected health information
- Providing free credit monitoring to customers
- Adopting encryption technologies
- Imposing sanctions on workforce members who violated policies and procedures primarily in response to serious employee errors, removing protected health information from the facility against policy, and unauthorized access
- Changing passwords
- Performing a new risk assessment
- Revising business associate contracts to more explicitly require protection for confidential information

Approximately half of organizations that reported breaches involving the theft or loss of electronic protected health information indicated they were implementing encryption technologies to avoid future breaches.

Reference

US Department of Health and Human Services, Office for Civil Rights. "Annual Report to Congress on Breaches of Unsecured Protected Health Information for Calendar Years 2009 and 2010." September 1, 2011. www.hhs.gov/ocr/privacy/hitechrepts.html.

Kevin Heubusch (kevin.heubusch@ahima.org) is editor-in-chief at the *Journal of AHIMA*.

Article citation:
Heubusch, Kevin. "Little Breaches: OCR Releases First “Small Breach” Data" *Journal of AHIMA* 82, no.10 (October 2011): 56-57.