COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 20, Number 7. July 09, 2020 Big Breaches, Down in First Half of 2020, Show Role of BAs; Increase May Be Coming

By Theresa Defino

During the first six months of this year, 228 breaches affecting 500 or more individuals were reported to the HHS Office for Civil Rights (OCR), and of the top 20, five involved business associates (BAs), including the largest.[1]

If the second half of the year is like the first, the 2020 breach total could fall short of 2019's record high of 511 breaches of this size posted on OCR's so-called "Wall of Shame" website.

But whether the numbers truly reflect fewer breaches or are temporarily down, perhaps due to delayed reporting or the impact of the COVID-19 pandemic, is just a guess at this point.

If anything, some are predicting that the number of breaches may climb in the second half of the year. Covered entities (CEs) have 60 days from when a breach occurs to notify the agency, so the OCR website is always somewhat behind.

Experts have been warning for months that the "bad guys" are seizing on the chaos of the moment to strike, particularly through email hacks.[2] Indeed, of the top 20 breaches reported this year, based on number of affected individuals, all of them were the result of hacking/IT incident involving email, except three.

Still, the trend in recent years has been for smaller breaches, a somewhat relative term, and that has so far continued in 2020. It wasn't unusual four or five years ago for a health plan, for example, to report a breach involving more than one million people. The big spike from 2014 to 2017 included Anthem and Premera Blue Cross, with 79 million and 11 million affected, respectively.

Last year saw a breach affecting 22 million individuals, partly attributed to Quest Diagnostics and LabCorp, due to a breach at their collection agency. That organization itself is a subcontractor and wasn't responsible for reporting the breach to OCR. On OCR's website, Quest's BA Optum360 reported 11.5 million affected individuals related to this breach.

As of the end of June, however, there have been no breaches of this magnitude reported. The largest breach reported thus far in 2020 was Health Share of Oregon, and it also set the pace for the issue of BAs as a cause.

On Jan. 2, the health plan learned that a laptop containing the protected health information (PHI) of 654,362 individuals was stolen from GridWorks, which the plan described as its "non-emergent medical transportation" vendor. The laptop disappeared after a burglary in November 2019.

For Marti Arvin, executive advisor for Austin, Texas-based cybersecurity consulting firm CynergisTek, the recent OCR data continue to send the message that breaches involving BAs are most likely underreported.

Breaches May Be Going Undiscovered

Arvin also told *RPP* the pandemic is "one likely reason" for fewer breach reports—but that doesn't mean breaches aren't happening.

"Health care organizations have shifted their focus to responding to the pandemic and are potentially not identifying the data compromises to their organization," she said. "Some of the processes they had in place to identify a data compromise might have been changed to accommodate their remote workforce."

She doubted that the numbers reflect "the result of better information security hygiene," saying that the health care community "has seen an increased volume of phishing attacks, including ransomware, since the start of the pandemic."

Are the days of million-person breaches really over? Such a statement, according to Chris Apgar, CEO and president of Apgar & Associates, "would be conjecture."

The lack of supersized breaches "may be associated with COVID-19 in the sense that nation states are dealing with the pandemic and have cut back on nation state cyberattacks," Apgar speculated.

Security Threats from Telework

By the end of this year, however, there may be a jump, if the increased security risk posed by sometimes hastily implemented telework and remote employment is exploited and actual breaches occur, he said.

"All CEs and BAs scrambled to make the move to telehealth and telework," Apgar said. "In doing so, I've found several clients who didn't think things through and examine the risks associated with telework and telehealth, opening the door for more breaches and security incidents."

Apgar added that there "may have been a significant number of breaches over the past few months that have yet to be reported because of the focus on day-to-day patient care and getting business done at the expense of managing risk in a way to prevent breaches."

Similarly, this pandemic period, as Arvin noted, has also been associated with ransomeware attacks.

"Ransomware attacks have increased during the pandemic, and there have been news stories about CEs that have paid the ransom," said Apgar. "That's not a lot different than ransomware attacks in the past, but I think the number of entities paying the ransom [has] increased (not based on anything but observation). What has changed is ransomware appears to be moving more toward 'I'll hold your data for ransom, and I'll also steal the data without letting you know.'"

OCR's data also show fewer thefts over time, with 8% of breach reports as of the end of May attributed to theft.

"This shift might be because organizations are more commonly encrypting devices," said Arvin. "But it could also be because the devices have been at less risk of theft, because the devices are staying at home. They are not in the car while an employee grabs dinner, and fewer employees are commuting or traveling with their devices."

Arvin does offer praise for CEs and BAs in bringing down the number of individuals affected by breaches, saying they may have implemented better processes, particularly to guard against attacks via email.

"More and more organizations are putting in place technology solutions that warn users when an email is from an outside party," she said. "They are also doing more white hat phishing campaigns to help users learn what to look for in a phishing email. If a breach is caught earlier, the number of impacted individuals will likely also be lower."

A 'Hidden Risk' for CEs

But one area that remains a problem is BAs.

"I have always felt that data compromises and, thus, breaches" by BAs are underreported, said Arvin, a frequent public speaker at industry events.

She said she regularly asks audience members "how many data compromises their BAs reported to them in the past year," and the response is "very seldom more than five, unless it's a large organization, and most organizations report they have 200-plus BAs."

Said Arvin: "Given the state of data compromises in health care provider organizations, it does not seem feasible that the number for BAs is so low."

Some CEs likely just don't know what's really going on with their BAs, especially if they let them make the call as to what is a reportable breach, she said.

Most CEs, said Arvin, lack "the resources to do better due diligence with their BAs to confirm that all security incidents or breaches have been reported back to the covered entity. Allowing a BA to determine what is a breach, which is the language of most business associate agreements, means the covered entity is relying on the risk tolerance of the business associate. That risk tolerance may not be consistent with the risk tolerance of the covered entity, thus what the covered entity would say is a reportable breach, the BA might not."

Arvin pointed out that, because the "ultimate responsibility for breach reporting remains with the covered entity, [an unreported breach] is a hidden risk that many covered entities have not considered."

Hacking, Email Attacks Are Up

According to an OCR analysis of breaches from January to May 31 of this year, the types of breaches are as follows. For comparison, the second percentage shown in parenthesis reflects OCR data from Sept. 23, 2009—when the breach notification rule went into effect—through May 31, 2020.

- Hacking/IT: 62% (31%)
- Unauthorized access/disclosure: 25% (28%)
- Theft: 8% (29%)
- Improper disposal: 3% (3%)
- Loss: 3% (6%)

Regarding locations of breached data, email made up almost half the reports this year, while portable electronic devices were at the bottom at just 2% from January to the end of May, as follows (as before, the cumulative total from 2009 to the end of May is shown in parenthesis):

- Email: 43% (20%)
- Network server: 24% (18%)
- Paper records: 17% (20%)
- Laptop: 3% (12%)
- Electronic medical record: 3% (6%)
- Desktop: 3% (10%)

- Other: 3% (10%)
- Portable electronic device: 2% (5%)

As noted earlier, Health Share of Oregon had the biggest breach reported this year. The following are the 19 largest breaches reported as of June 26, in order of size of affected patients, with breach report submission date, type of breach, location of the lost PHI and whether a BA was involved.

1. Elkhart Emergency Physicians Inc. of Indiana; 550,000; May 28; improper disposal; paper/films
2. BJC Health System of Missouri; 287,876; May 5; hacking/IT incident; email; BA involved
3. Ambry Genetics Corporation of California; 232,772; March 3; hacking/IT incident; email
4. PIH Health of California; 199,548; Jan. 10; hacking/IT incident; email
5. BST & Co. CPAs LLP of New York; 170,000; Feb. 16; hacking/IT incident; network server; BA involved
6. Aveanna Healthcare of Georgia; 166,077; Feb. 14; hacking/IT incident; email
7. Tandem Diabetes Care Inc. of California; 140,781; March 17; hacking/IT incident; email
8. Brandywine Urology Consultants PA of Delaware; 131,825; March 27; hacking/IT incident; desktop computer, email, laptop, network server
9. Beaumont Health of Michigan; 112,211; April 17; hacking/IT incident; email
10. Meridian Health Services Corp. of Indiana; 111,372; April 27; hacking/IT incident; email
11. Overlake Medical Center & Clinics of Washington; 109,000; Feb. 7; hacking/IT incident; email
12. Merit Health Insurance Company of Illinois; 102,748; June 12; hacking/IT incident; email, network server
13. Tennessee Orthopaedic Alliance; 81,146; Feb. 14; hacking/IT incident; email
14. Magellan Complete Care of Florida; 76,236; June 12; hacking/IT incident; email, network server
15. Munson Healthcare of Michigan; 75,202; Feb. 26; hacking/IT incident; email
16. Arizona Endocrinology Center; 74,122; April 10; unauthorized access/disclosure; electronic medical record
17. Stephan C. Dean of California; 70,000; March 4; hacking/IT incident; desktop computer, electronic medical record, email; BA involved
18. NCH Healthcare System Inc. of Florida; 63,581; Feb. 17; hacking/IT incident; email
19. Solo Laboratories of Pennsylvania; 60,000; Feb. 18; hacking/IT incident; network server; BA involved

Contact Arvin at marti.arvin@cynergistek.com and Apgar at capgar@apgarandassoc.com.

1 "Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information," Office for Civil Rights, U.S. Department of Health and Human Services, last accessed July 6, 2020, http://bit.ly/2rk0XdW.
2 Jane Anderson, "Health Care Organizations Struggle to Fight Evolving Threats Stemming From Pandemic," *Report on Patient Privacy* 20, no. 6 (June 2020), https://bit.ly/38AuwJF.