COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 19, Number 4. April 10, 2019 Atrium Health's Response Plan Helps Health System Get Through Breach

By Jane Anderson

Several years ago, Atrium Health, based in Charlotte, North Carolina, brought together a team that included personnel from departments throughout the organization, ranging from privacy to legal and corporate communications. The team, which also included information systems security, audit services and risk management representatives, was tasked with creating a new, comprehensive breach response plan.

That plan sprung into action last fall when Atrium Health learned that hackers had accessed two databases containing protected health information (PHI) for more than two million people ("Vendor Hack Results in 2.65M Records Breached for Atrium Health, Baylor," *RPP* 18, no. 12). The hack occurred in Atrium Health's business associate, AccuDoc Solutions Inc., a billing provider.

Atrium Health won praise at the time for moving quickly and professionally to deal with the incident. Alicia Bowers, Atrium Health vice president and chief privacy officer, tells *RPP* that the breach response plan created by the Atrium Health team helped quite a bit.

"We triggered the breach response plan almost immediately upon notification of the incident by our vendor," Bowers says. "The chief privacy officer and, if the breach involves security, the chief information security officer make the decision to trigger the breach response plan."

The plan itself serves as a road map and as a repository of lists, regulatory requirements, communications and tracking tools, plus reminders for a breach, she says. Following its development, Atrium Health has continued to update it over the years.