COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 19, Number 3. March 06, 2019 Columbia Email Breach Shows Need for Research Safeguards

By Theresa Defino

Compared to privacy breaches that routinely affect millions, the one suffered by Columbia University Medical Center in 2016 was tiny, but the information exposed was among the most sensitive. In November of that year, a Columbia researcher notified an internal board overseeing her study that email addresses of 145 individuals involved in HIV/AIDS research were visible in a recruitment pitch. A study coordinator had included individuals' addresses in the CC portion of an email inviting participation in a related upcoming study.

Because only breaches affecting 500 or more individuals are required to be made public under federal law, smaller incidents like this one may remain secret. But in Columbia's case, the breach, which also appears to be reportable under HIPAA, came to light because a U.S. agency found that the medical center violated U.S. regulations governing research by failing to report what had happened.

Last month, the HHS Office for Human Research Protections (OHRP) published a determination letter that it sent to Columbia University indicating that the email disclosure was considered a "breach in confidentiality" that qualified as an "unanticipated problem involving risks to subjects or others." Such problems are to be "promptly" reported to OHRP; this one wasn't until months later and only after the agency, acting on a complaint, contacted Columbia.

OHRP said Columbia had delayed its report to the agency because its "investigation was still pending," but this is not an allowable reason for lack of a prompt notification.

The email breach, which a former OHRP regulator calls "shocking," offers reminders that maintaining privacy is just as important in studies as it is in treatment settings and that when the protected health information (PHI) is research-based, an organization may face actions by an agency other than the Office of Civil Rights (OCR). Additionally, organizations will want to review the corrective actions Columbia took in the wake of the email breach, including terminating the study coordinator.

Privacy Protections Subject to IRB Review

In addition to HIPAA, organizations conducting applicable research must comply with specific regulations at 45 CFR part 46, also known as the Common Rule, meant to protect study subjects. These regulations apply to federally funded studies (Columbia's had NIH support) and when drugs or devices are developed for potential approval by the Food and Drug Administration, and address the privacy of research participants.

Research is generally reviewed and approved by a hospital or other organization's institutional review board (IRB). Among the criteria for IRB approval is ensuring "there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data," when appropriate to a particular trial.

Further, the Common Rule requires organizations to review and report to OHRP "unanticipated problems involving risks to subjects or others" and adverse events. The former was one of the issues in Columbia's situation.

RPP attempted to learn more about the privacy breach and contacted the investigator on the study, as well as several other Columbia officials. After no response for nearly two weeks, a spokeswoman who *RPP* had not contacted emailed the following. "Thanks for your recent request about OHRP's determination letter. Unfortunately, we do not have any additional information to share at this time." Among *RPP*'s unanswered questions are whether Columbia considered the breach reportable under HIPAA or not, and if it has been reported.

It is unusual to learn about breaches involving research studies because OHRP rarely makes compliance findings at all, and even fewer involve privacy issues. OHRP's letter to Columbia is only the third it has issued since October 2016. In previous years, OHRP had issued dozens of such letters, which address concerns ranging from lack of informed consent to failures to follow IRB procedures.

The determination letter that OHRP sent to Columbia closing the investigation was the only document that has been released; it did not post correspondence from Columbia but referred to information it had provided. Although the letter was issued this year, the events described in the letter took place in 2016 and 2017.

OHRP: Breach Presented Risks

According to the letter, OCR received a complaint in February 2017 apparently from someone who had either seen an email or received one that Columbia sent to people currently enrolled in a study testing a web application providing "self-care strategies" for people living with HIV/AIDS. The email was asking "them to participate in a new study" for underserved people with HIV. "The carbon copy (cc) section of the email contained 145 email addresses for the subjects in the current study (some of whom were recognized by the complainant)," OHRP said.

The investigator learned of the breach in November 2016 and, as required, brought it to the attention of the IRB "as an unanticipated problem involving risks to subjects or others." When OHRP contacted Columbia in the same month it received the complaint, Columbia officials said they had not reported it to OHRP because their "investigation was still pending."

But as OHRP wrote to Columbia, "HHS regulations at 45 CFR 46.103(a) and (b)(5) require, among other things, that unanticipated problems involving risks to subjects or others and serious or continuing noncompliance be reported promptly to OHRP. We determine that the recruitment email sent with other study subjects' email addresses, albeit inadvertent, constituted a breach of subject confidentiality that represented an unanticipated problem involving risks to subjects or others."

OHRP did not receive the required report from Columbia until April, six months after the investigator first learned of the breach and reported it to the IRB. The letter does not indicate when the email itself was actually sent.

The agency did not take any enforcement action against Columbia as a result of the breach or the failure to report it. When noncompliance is found, OHRP may take a number of actions, ranging from suspending a study to requiring specific corrective measures. In this instance, OHRP identified a number of steps Columbia had taken and said these were adequate to address the issues.

In addition to the report to OHRP, Columbia:

- Voluntarily halted "email recruitment procedures…until a secure process for sending recruitment emails to potential participants was fully developed and implemented."
- Terminated the "employment of the study coordinator who sent the recruitment email."
- Had "all members of the study team…re-take" Columbia's HIPAA "privacy and information security

training."

- Asked the study team to "review" a manual developed by the investigator, "Best Practices for Maintaining Privacy and Confidentiality for Study Participants," and posted the manual "inside of each study team member's workspace."
- Required study team members to "participate in the university's research compliance foundations course."
- Sent an "apology letter…to the study subjects to notify them of the breach of confidentiality and to apologize for any for any for the inconvenience that it caused (sic)."

The regulations do not define "prompt" in terms of reporting, but in 2007 guidance, OHRP recommended that an investigator should alert the IRB within one week of learning about a serious adverse event and within two weeks of "any other anticipated problem." Subsequently, the institution should inform OHRP of any type of unanticipated problem to OHRP within a month of receiving the investigator's report.

Reporting Obligations Are Clear

While OHRP's issue with Columbia seemed to rest on the timing of the notification, Lisa Rooney, a former compliance oversight coordinator for OHRP and now a consultant, says some institutions may fail to appreciate that a data breach is a risk to a study participant that must be reported.

"A lot of people think 'physical risk,' but it's much more than that" among the types of problems that must be reported to OHRP, says Rooney.

She notes that OHRP's guidance included this example of a reportable event:

"An investigator conducting behavioral research collects individually identifiable sensitive information about illicit drug use and other illegal behaviors by surveying college students. The data are stored on a laptop computer without encryption, and the laptop computer is stolen from the investigator's car on the way home from work." OHRP explains that this "is an unanticipated problem that must be reported because the incident was (a) unexpected (i.e., the investigators did not anticipate the theft); (b) related to participation in the research; and (c) placed the subjects at a greater risk of psychological and social harm from the breach in confidentiality of the study data than was previously known or recognized." (For more information, see http://bit.ly/2XwK23r.)

Researchers and IRBs need to ensure that safeguards are "protocol-specific," based on the type of information being collected and how it will be used and stored, Rooney says.

In this particular situation, sending an email with the other names visible was "totally out of line," Rooney says. "I was shocked by it. It was just so sloppy." The fact that the information concerned HIV/AIDS made the situation "even worse." If it was a high cholesterol study, the exposure of the email addresses might not have been so potentially damaging, she says.

Was OCR Notified?

Researchers and hospitals may actually need to beef up their safeguards for PHI used in studies in the near future, although it is not clear yet just how. That's because the revised Common Rule directs the HHS secretary to work with the privacy office of the Office of Management and Budget and other agencies that follow the Common Rule to "issue guidance to assist IRBs in assessing what provisions are adequate to protect the privacy of subjects and

to maintain the confidentiality of data."

Under OHRP policies, the agency would typically refer issues it encounters that are not within its jurisdiction, or that overlap, to other related parts of the government, Rooney tells *RPP*.

A case like this, for example, could have been referred to OCR for possible action, given OHRP deemed it a breach of confidentiality. OHRP's correspondence with Columbia does not indicate whether officials made any such referral nor whether Columbia reported the exposure of the HIV information and emails to OCR.

As noted earlier, Columbia officials would not answer any questions from *RPP*, including whether they reported the email exposure to OCR.

HIPAA applies to research when the institution conducting the study is a covered entity, business associate or a hybrid entity; the responsibility also flows to subcontractors and others who are sharing PHI. The only exception is when data are de-identified using strict HIPAA guidelines.

HIV Data Breaches Have Brought Sanctions

OCR does not comment on reports of small breaches nor on incidents that may be the subject of ongoing investigations.

There's no question that OCR can bring enforcement actions against provider organizations, but that authority also extends to research institutions as well. In March 2016, the Feinstein Institute for Medical Research was the first, and to date the only, purely research organization to feel OCR's wrath. It paid a $3.9 million penalty—a record at the time—and agreed to a three-year corrective action plan ("Research Institution Shares Lessons From Breach, Path to $4 Million OCR Settlement," *RPP* 16, no. 4).

More recently, OCR won a $4.3 million judgment last year against MD Anderson Cancer Center for a series of small breaches resulting from the theft or loss of PHI for 33,500 individuals. Among the cancer center's unsuccessful arguments was that research data is exempt from HIPAA ("MD Anderson Cancer Center's Travails Show Struggle to Encrypt, OCR 'Impatience,'" *RPP* 18, no. 8).

OCR's cases have also stressed that, regardless of research issues, the agency is willing to take enforcement action even when the PHI of just one or two people is compromised, and especially so when HIV/AIDS information is inappropriately used or disclosed.

In May 2017, St. Luke's-Roosevelt Hospital Center Inc., part of the Mount Sinai Health System, resolved allegations of HIPAA violations by paying $387,000 and agreeing to follow a three-year corrective action plan.

The agency said that twice within a nine-month period in 2014, an employee with a program that "provides comprehensive health services to persons living with HIV or AIDS and other chronic diseases" inappropriately faxed medical records to a patient's employer and to the office where a different patient was a volunteer ("In Break from Trend, OCR Cracks Down On Organizations for Media Release, Faxes," *RPP* 17, no. 6). ✧