



Bob's Pharmacy and the HIPAA Breach Protocol

BY NED MILENKOVICH, PHARM.D, JD



AUTHOR BIO

Ned Milenkovich, PharmD, JD, is chairman of the health care law practice at Much Shelist PC in Chicago and former vice chairman of the Illinois State Board of Pharmacy.

Editor's note: The characters in this article are a work of fiction. Names, characters, businesses, places, events, locales, and incidents are either the products of the author's imagination or used in a fictitious manner. Any resemblance to actual persons, living or dead, or actual events is purely coincidental.

BOB, A CONSCIENTIOUS NEIGHBORHOOD PHARMACIST, runs Bob's Pharmacy in Smalltown, USA. He and his wife Sally, also a pharmacist, have worked tirelessly for many years to serve their community with good health care advice. Bob called his attorney last week because he was concerned about a patient who alleged that someone in his pharmacy leaked protected health information (PHI) when the patient's prescription was electronically transmitted to the local community library by mistake.

Bob recalls that 9 years ago, the American Recovery and Reinvestment Act of 2009 became law. The Recovery Act, as it is commonly known, is a stimulus package that also enacted the Health Information Technology for Economic and Clinical Health Act (HITECH) to promote the adoption and meaningful use of health information technology.

HITECH addresses the treatment of electronic health records and increases the compliance requirements for a "covered entity" as it is defined under the Health Insurance Portability and Accountability Act (HIPAA) of 1996. HITECH also introduces additional requirements for a business associate engaged by a covered entity to assist it in carrying out its health care activities and functions.

Bob's Pharmacy likely falls under HIPAA's definition of a covered entity. If so, Bob's Pharmacy will be subject to HIPAA and HITECH regulations. This means that Bob's Pharmacy must provide breach notification to the Office of Civil Rights and affected patients if a data breach occurs. Therefore, as soon as a breach of PHI is evident, Bob's Pharmacy must determine whether the incident necessitates notifying of the compromised individuals to the Department of Health & Human Services and, in certain instances, to media outlets.

The regulations establish a 3-phase standard oper-

ating procedure. Phase 1 determines whether an impermissible disclosure or use has occurred under HIPAA guidelines. Phase 2 requires a documented risk assessment analysis to determine whether, and to what extent, the privacy or security of PHI has been breached. Phase 3 requires an assessment of whether the breach meets 1 of 3 regulatory exceptions that do not trigger obligatory notification. Bob's Pharmacy should go through each of these steps with its legal counsel to determine whether a breach of PHI occurred.

If a breach concerns 500 or more residents of any state, Bob's Pharmacy must, in the form of a press release, notify major broadcast or print media where the affected people likely reside. Notification must be made within 60 days of the breach, and it must be provided without unreasonable delay.

If a business associate working on behalf of Bob's Pharmacy discovers a breach, they must notify the pharmacy. It must be stressed that the discovery of a breach by a business associate may be attributable to the pharmacy if that business associate is determined to be an agent of the pharmacy. In such an instance, this results in Bob's Pharmacy notice period commencing with the date that the business associate discovers the breach instead of the date that the business associate notifies the pharmacy of such a breach.

However, if the business associate is deemed to be an independent contractor instead of an agent, then the notice period for Bob's Pharmacy to report a breach discovered by the business associate begins on the date that the business associate notifies the pharmacy of the breach, unless Bob's had previously discovered the breach. Given this, it behooves pharmacies to incorporate specific security breach provisions into their business associate contracts. ♦