Confirmation bias threatens patient safety, but can be overcome

Sometimes people see or hear what they expect, not real information

Insight confirmation bias lurking in your hospital, waiting to cause havoc for even the most skilled, well-intentioned clinicians? This mental fault allows one to see or hear what is expected or desired, rather than what actually is. It has led to adverse events in many industries, and healthcare is exceptionally vulnerable.

Tufts Medical Center in Boston is dealing with the tragic results of confirmation bias, but the institution has implemented safeguards to keep the risk at bay, says Lynn Worley, RN, JD, CPHRM, senior risk manager and assistant general counsel at Tufts Medical Center. The family of a Tufts patient is suing the hospital after a surgeon injected the wrong dye into her spine, when the surgeon mistakenly assumed it was the correct dye he had asked for. The patient died the next day from the effects of the dye. The surgeon was baffled as to how he, the nurse who handed it to him, and others along the line failed to notice that the label clearly stated it was a different dye and included a warning not to use it in the spine. (For more on the adverse event, see the article on p. 111.)

The case is a good example of confirmation bias, says Tufts Chief Medical Officer Saul Weingart, MD, MPP, PhD. The surgeon and other clinicians “saw what they expected to see” even though the label clearly said otherwise, Weingart explains.

Confirmation bias can take many forms,
Errors by employees are at the root of most data breaches, but not the most costly

The two most common sources of Health Insurance Portability and Accountability Act (HIPAA) breaches are unintended disclosure, such as misdirected emails and faxes (31%) and the physical loss of paper records (24%), which is particularly prevalent among healthcare organizations.

Those findings come from Beazley Breach Response (BBR) Services, an Atlanta company providing breach response insurance. It recently announced findings from an analysis of more than 1,500 data breaches at a meeting of the International Association of Privacy Professionals (IAPP). Breaches handled by the company have affected more than 14 million people.

These are expensive

Among the data breaches serviced by Beazley in 2013 and 2014, breaches due to malware or spyware represented only 11% by number of breaches in 2013 and 2014. However, they have been increasing, with the total number of breaches in this category growing by 20% between 2013 and 2014. Due to heavy forensics costs (money spent to find out exactly how the breach occurred), these breaches are on average 4.5 times more costly than the largest loss category, unintended disclosure, explains Katherine Keefe, JD, head of Beazley Breach Response.

“With more information being stored electronically and in the cloud, the risk of data breaches is growing,” Keefe says. “Consumers expect their privacy will be protected, and a data breach can have serious reputational and financial impact.”

Most breaches are avoidable with appropriate training and security measures, says Keefe, noting the particular need for encryption services for large-scale computer networks and mobile services. (See p. 4 for tips on avoiding a data breach.)

EXECUTIVE SUMMARY

Most HIPAA data breaches are tied to misdirected emails and faxes, but the costliest are the result of malware and spyware. The findings come from a company that offers insurance for data breaches.

• The loss of paper records accounted for 24% of the breaches.
• Malware and spyware breaches are costly because of the research necessary to unravel them.
• Breaches from computer hacking are on the rise.