Guide to California's Breaches: First Year of State reporting requirement Reveals Common Privacy Violations

By Chris Dimick

Effective January 1, 2009, California healthcare providers were required to report every breach of patient information to the state. They have sent a flood of mishaps and a steady stream of malicious acts.

While some people go to great lengths to gain unauthorized access to medical records, a majority of healthcare privacy breaches in California last year were unintentional, the result of mistakes. That picture emerged over the past year as healthcare providers began reporting breach incidents under a new state law that took effect January 1, 2009.

More than three-quarter of breaches reported last year were accidental, says Kathleen Billingsley, RN, the deputy director of the California Department of Public Health, Center for Health Care Quality (CDPH). Billingsley's department is responsible for collecting and investigating privacy breach cases under the ground-breaking legislation.

Upon discovering an incident of unauthorized access or disclosure of a patient's medical information, California providers are required to submit a privacy breach notification to both CDPH and the affected patients within five business days.

Depending on the severity of the breach, providers can be fined up to $25,000 per patient for the initial breach and $17,500 for each subsequent breach. Penalties can reach up to $250,000 per incident. In addition, CDPH may refer cases to a second state office, which can conduct its own investigation of the individuals involved in the breach.

Breaches by the Numbers

CDPH was flooded with breach notifications in 2009, receiving word of 2,490 breach incidents from January 1 through December 31. The department completed investigations on 1,291 cases, with nearly all confirmed as privacy breaches and 120 either referred to other agencies or classified as a nonbreach. There were 484 cases still under investigation at the end of 2009, and 715 cases pending an investigation. (See sidebar, opposite.)

The department categorizes all breach reports upon receipt, even before an official investigation has been completed. Therefore, it can categorize the type of breach for all incidents reported in 2009.

Of the confirmed breaches, 96 cases involved malicious, intentional acts by healthcare workers and 2,290 cases were the result of unintentional actions usually involving administrative mistakes.

Of the unintentional breaches, 1,929 cases involved a patient's healthcare information accidently being sent to an outside healthcare facility or nonprovider destination-the most common type of breach incident reported in 2009, Billingsley says. This type of breach might involve a hospital employee faxing a patient's chart to the wrong Dr. Smith.

CDPH issued $437,500 in fines as the result of its investigations. However, all of those fines were assessed in two cases against the same hospital, Los Angeles-based Kaiser Permanente Bellflower Hospital, which was involved in a breach of "Octomom" Nadya Suleman's medical records early in the year.

The pace of fines will pick up in 2010, Billingsley says, with more penalty announcements pending release at press time.

CDPH was very cautious about issuing fines in the first year of the program, because they were fine-tuning processes, according to Billingsley. Cases go through a series of reviews before fines are issued, further slowing the process.

A Year of Learning

CDPH spent part of 2009 interpreting the new law and educating providers on the type of breach incidents that should be reported. This was the department's biggest challenge in implementing the landmark breach notification law, Billingsley says.

On July 29 CDPH sent a letter to all healthcare providers clarifying parts of the law. In that letter, Billingsley stated that healthcare organizations did not need to submit a breach notification if the incident involved a misdirected internal paper record, e-mail, or fax that was sent to another healthcare worker within the same facility.

For example, she says, a staff member might intend to fax information to the lab but inadvertently send it to radiology instead. "We received a multitude of those," she says.

The letter was in response to an "overwhelming" number of reports on these types of incidents. CDPH believes these mistakes present a low risk to the patient and do not warrant a state investigation under current law, according to Billingsley.

However, Billingsley says she was surprised by the high number of these incidents, and she wrote in the letter that facilities should review their internal policies and procedures to prevent similar occurrences in the future.

The 96 reported malicious breaches committed by healthcare workers came as a personal surprise to Billingsley, who has a nursing background.

"I'm surprised at the lengths people will go to try to access information that they are not authorized to access," she says. "Some individuals will actually go and get a new password and use a separate computer in order to view information."

Other malicious cases involved healthcare employees who looked at unattended records, searched patient's billing information, and even reviewed their lab results. In addition to a reminder that "we need to hold ourselves to a higher standard as healthcare workers," Billingsley says these breaches show changes to EHR systems are needed to better prevent unauthorized access to patient records.

Another common instance of unintentional breaches reported to CDPH in 2009 occurred when patients were discharged from a healthcare facility with someone else's discharge order. In a few cases, patients were even discharged with someone else's medications. A hospital can avoid these errors by installing additional system checks and balances, Billingsley says.

The First-Year Results

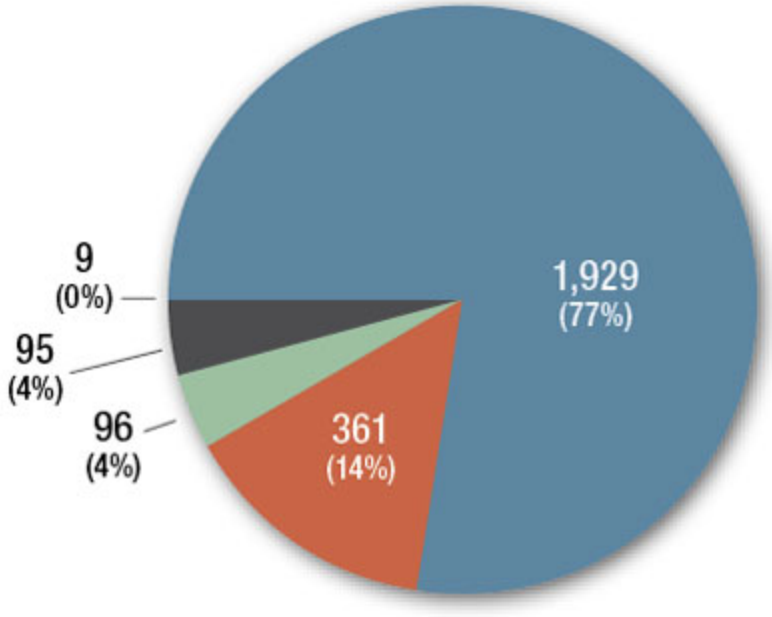
CDPH averaged nearly seven breach reports a day in the first year under the law. It spent part of the year interpreting the law and educating providers on what to report. In July the department informed providers they did not need to report a misdirected internal record or communication sent to a healthcare worker within the same facility, which many had been doing previously.

Reported Health Privacy Breaches (January 1–December 31, 2009)	
Total number of incidents reported	2,490
Completed investigations	1,291
Confirmed breaches	1,171
Unsubstantiated incidents	120

Ongoing investigations	484
Pending investigations	715

Unintentional, External Breaches Most Common

CDPH assigns each reported breach to a preliminary category during its initial review. Administrative errors, such as faxing patient information to the wrong person, represented the majority of breach reports in 2009. However, a steady stream of lost or stolen data and malicious breaches combined for 200 reported incidents over 12 months.



1,929 (77%): Unintentional breach to person outside facility/healthcare system

361 (14%): Unintentional breach by healthcare worker within the facility/healthcare system

96 (4%): Malicious breach by healthcare worker

95 (4%): Breach of IT system, theft, loss of electronic device, loss of medical records

9 (0%): Malicious breach by nonhealthcare worker

More Education to Come

During a CDPH investigation, healthcare facilities are required to submit a plan of correction within 10 days to ensure breach mistakes are not repeated.

That helps the particular hospital prevent avoidable errors, but CDPH would like to use the information it collects from the reports and subsequent investigations to educate all California providers on better protecting patient health information.

"Part of my mission is to communicate what we are seeing so that hospitals can look at their own processes and say, 'Does this happen here? Do I need to look at this process? Do I need to look at the vulnerabilities or steps that need to be taken to prevent this from happening?'" Billingsley says.

That education will likely increase in future years as the data collection and investigation processes are smoothed out. However, when CDPH assessed fines in the Bellflower Hospital cases, it publicized the breach and the steps the facility was taking to prevent future errors.

"This first year has been pretty much a massive data collection piece for us because we didn't know how many [breaches] would be reported or the types that would be reported," Billingsley says. "This is very new for us, and so we are still in the process of dissecting all this, and then we will make the decisions as to how to best communicate what we have been finding."

First Investigations of Individuals under Way

Breach cases can be subject to two investigations-one from CDPH into the facility's practices, and one from the California Office of Health Information Integrity (CalOHII) into the individuals involved in the breach.

CDPH refers breach cases to CalOHII if it determines that an individual contributed to or benefited from a breach. Fines for individuals can reach up to $250,000, and individuals can be reported to their professional licensing boards for review.

In 2009 CDPH referred 320 individuals to CalOHII for investigation. Another 24 complaints came directly from the public.

CalOHII opened 34 cases for investigation, which as of February 1 were still unresolved, and it has 310 cases pending a full investigation. The first cases were expected to be closed in March 2010, according to Alex Kam, CalOHII director.

CalOHII spent most of 2009 setting up the new breach investigation unit and developing the investigation process, Kam says. Hiring for the new department unit began in July, at the start of the state's fiscal year. The department was fully staffed by November, and full investigations were launched in early December. That extended ramp-up period explains why no cases had been fully resolved as of February, Kam says.

"It has been a building infrastructure type year, where we have been trying to build relationships [with medical and licensing boards and CDPH], establish the unit, and create procedures and processes," he says. Though 310 cases are pending a full investigation, CalOHII has evaluated nearly all referred cases.

"I don't want to give the impression to the public that it is a bottleneck, because some of the assessment [of cases] is a data collection process in and of itself," Kam says. "We are actively moving on all cases."

While Kam would not comment on open investigations, he says most of the cases referred to his organization involve staff acting against facility policies and willfully breaching patient health information. The most serious cases have been opened for investigation first, he says.

Chris Dimick (chris.dimick@ahima.org) is staff writer for the *Journal of AHIMA*.

Article citation:
Dimick, Chris. "Guide to California's Breaches: First Year of State reporting requirement Reveals Common Privacy Violations" *Journal of AHIMA* 81, no.4 (April 2010): 34-36.