Privacy Breaches and Invasions

Peter J. Martin, Esq.

Peter J. Martin, Esq.

Health care practitioners have for years known that, under HIPAA, if there is a "breach" of unsecured, protected health information, there may be an obligation to notify the affected patients or regulatory agencies or both. Likewise, under Massachusetts data privacy laws, there are well-known notification obligations in the event of a breach of security with respect to personal information. Regulatory guidance exists to help practitioners understand when a "breach" has occurred – under HIPAA, the breach has to compromise the security or privacy of the information; and under state law, the breach must create a substantial risk of identity theft or fraud.

A recent Massachusetts Superior Court case has highlighted another legal avenue for those aggrieved by an unauthorized disclosure of confidential information, this time under the state right of privacy statute: Massachusetts General Laws, chapter 214, section 1B. That statute says, "A person shall have a right against unreasonable, substantial or serious interference with his privacy." In a decision handed down in November of 2015, the court permitted a claim to proceed under that statute, brought by a group of hospital patients whose medical records were inadvertently posted on a website, denying a hospital's motion to dismiss the case. The decision is based on the Massachusetts law of "standing" – basically, the rule that a plaintiff must allege at least a real and immediate risk of injury in order to bring a claim. Here, the court ruled that since plaintiffs alleged facts that, if true, "suggest a real risk of harm from the data breach," the case should not be dismissed but should proceed so as to allow the development of further evidence regarding whether the data was accessed and, if so, the nature and extent of that access.

The dispute began when the hospital sent notices to the affected patients that their patient records "were inadvertently made accessible to the public through an independent medical record transcription service's online site." The hospital also advised those patients that the medical records "could potentially be accessed by non-authorized individuals," though the hospital did not know how long the information was available or whether any of it was misused. In so doing, the hospital appears to have met its HIPAA obligation of providing affected patients a description of the breach incident itself and the types of information affected by it.

The patient-plaintiffs read this notice and inferred that their records were accessed or were likely to be accessed by unauthorized persons. They sought damages against the hospital and the medical transcription company for the unauthorized exposure of their medical records. The first count in their complaint was for "invasion of privacy" under the Massachusetts privacy statute. The court ruled that the plaintiffs' allegation of a risk of harm was sufficient to survive the defendants' motion to dismiss the case. The defendants claimed that without an allegation that the records were actually accessed or used by an unauthorized person, the plaintiffs had failed to state a claim. The court disagreed. The plaintiffs thus were not required to allege that unauthorized persons actually accessed or misused their information to proceed with their case.

There are a couple of comments to be made about this matter. First, note that the standing threshold in this case is that the plaintiffs allege facts that support an inference of there being a "real risk of harm from the data breach." The level of risk does not need to be quantified, though the alleged injury may not be speculative, remote or indirect. While the plaintiffs may, at a later stage in the trial, be unable to show actual harm, the court's reasoning suggests they might still recover damages if, for example, they can prove mental distress or harm to their interest in privacy arising from the information being made accessible, perhaps even in the absence of actual misuse of the information. In contrast, under HIPAA, an "acquisition, access, use or disclosure of protected health information" is only a "breach" giving rise to notice obligations if the breach "poses a *significant* risk of financial, reputational or other harm to the individual" (emphasis added). Further proceedings in the case may lead to the result that access to redress under Massachusetts' privacy statute is easier to come by than under HIPAA.

Second, it appears the court found it significant that the hospital was unable to say how long the information was publicly accessible through the website. The court said that the plaintiffs reasonably inferred both that this accessibility lead to a serious risk of disclosure and that the records either were accessed or were likely to be accessed by an unauthorized person. It appears the court felt that the longer the period of such accessibility, the stronger those inferences could be drawn. Consequently, practitioners and health care institutions are well advised to seek to identify and rectify an unauthorized disclosure of information as soon as possible so as to weaken those inferences, and thus, the potential for a successful claim for damages.

While still at an early stage, this case is worth monitoring, as it may result in the expanded use by patients of the Massachusetts privacy statute to seek remedies for "breaches" of health care information security or "invasions" of health care information privacy.

Peter J. Martin, Esquire, is a partner in the Worcester office of Bowditch & Dewey, LLP, his practice concentrating on health care and nonprofit law.