ROBERTS
CARROLL
FELDSTEIN
& PEIRCE
ATTORNEYS AT LAW RCFP.COM

Emerging Threats: Data Breaches, Government Sanctions and Privacy Class Actions

By:

JASON C. PRECIPHS, ESQ.

JAMES D. CULLEN, ESQ.

With the proliferation of electronic medical records and the exponential growth in the use of mobile computing devices, the risks of widespread data breaches in the healthcare industry have grown exponentially. The release of protected health information not only raises the specter of government investigation, fines and other enforcement action, but, as demonstrated by recent developments in California and elsewhere, there is an increased risk that healthcare providers could be the subject of a class action lawsuit.

According to a December 2011 Ponemon study (Ponemon is a well-regarded organization dedicated to research in the area of privacy, data protection and information security policy), 81% of medical providers now use mobile computing devices (cell phones, laptops, and tablet computers) to gather, store and exchange health information. While the utility of these devices cannot be underestimated, the proliferation of electronic medical records and the use of mobile computing devices bring with them significant risks relating to the protection of patient information. In fact, 49% of the health care providers surveyed indicated that they were not taking measures to protect patient information or secure their mobile computing devices.

While patient information has long been protected under HIPAA (Health Insurance Portability & Accountability Act), enforcement of the HIPAA regulations has never been stringent. The HITECH (Health Information Technology for Economic & Clinical Health) Act of 2009 has, however, changed this. Although it was enacted to encourage the use of electronic medical records, the 2009 HITECH Act simultaneously strengthened the protection of health information and provided for increased enforcement of those privacy protections. In order to comply with HITECH, it will be incumbent upon medical providers to do more than place a

ROBERTS, CARROLL, FELDSTEIN & PEIRCE INCORPORATED
Ten Weybosset Street | Providence, RI 02903-2808 | Phone 401.521.7000 | Fax 401.521.1328
Member: Legal Netlink Alliance • An International Alliance of Independent Law Firms

password on their computers and storage devices, the protected health information itself must be encrypted.

Since the enactment of HITECH, and particularly in the last year, the Department of Health and Human Services Office for Civil Rights (OCR) has stepped up its investigatory and enforcement activity as it relates to protected health information. For example, in March 2012, Blue Cross and Blue Shield of Tennessee and OCR agreed to a settlement amounting to $1.5 million. This settlement arose out of an OCR complaint resulting from a data breach after 57 hard drives were stolen from Blue Cross and Blue Shield. The hard drives included 300,000 video recordings and over 1 million audio recordings of customer service calls; including names, ID numbers, diagnosis codes, dates of birth and social security numbers. State authorities have also taken enforcement action. The Connecticut Attorney General recently levied a fine of $375,000 against Health Net, which was found to have left the information of over 1.5 million members unprotected. These examples show that healthcare providers who do not take adequate steps to secure and protect patient information will risk investigation, administrative action and corresponding costs and fines.

In addition to the risks posed by government enforcement action, data breaches may also result in lawsuits, particularly class actions. Although there is no direct cause of action under HIPAA or HITECH, those patients whose protected health information has been exposed could proceed under state statutes. In Rhode Island, R.I. Gen Laws § 9-1-28.1(a)(3), which provides for "the right to be secure from unreasonable publicity given to one's private life," is a likely basis for such a suit.

A class action is a type of civil action in which one person, or potentially several people, sues on behalf of a large group. In order to bring a class ac-

tion, the representative party must not only demonstrate that the purported class is sufficiently large, but that the injuries, damages and issues in the case are sufficiently common to the group as a whole to justify the use of the class action mechanism. While there are therefore significant hurdles to be overcome before a class action can be brought, where a data breach has occurred these hurdles are likely to be easy to overcome.

There has been a recent uptick in the number of class actions arising from data breaches. Thirteen class actions were filed in California relating to the exposure of over 4 million peoples' data by Sutter Health. These suits relate to a single incident, the theft of one of the company's desktop computers. Although the computer was password protected, the information stored on the computer was not encrypted – as required under HITECH. In addition, St. Joseph Health Systems is the subject of a class action suit brought after 31,800 patients protected health information was made available on the internet. Stanford University Hospital is also the subject of a class action as the result of the exposure of data relating to over 20,000 patients, including names, diagnosis codes, discharge dates and billing charges.

While it may be difficult for plaintiffs (those bringing suit) to show that they have suffered damage as a result of the release of their protected health information, class actions tend to be particularly expensive to defend. Therefore, even if the class members suffered no apparent damage as a result of the data breach, the risk of a class action is still significant. In addition, even if the damages suffered by any individual member of the class appear to be insignificant, the aggregation of multiple claims in a class action leads to a potentially significant exposure.

With some statistics indicating that 71% of health care organizations have had at least one data breach in the last year, the risks of data breach must be taken seriously and addressed sooner rather than later.

Return to:
IN THE
NEWS

ROBERTS, CARROLL, FELDSTEIN & PEIRCE INCORPORATED
Ten Weybosset Street | Providence, RI 02903-2808 | Phone 401.521.7000 | Fax 401.521.1328
Member: Legal Netlink Alliance • An International Alliance of Independent Law Firms