Published on *The National Law Review* https://natlawreview.com

Massachusetts Enforces Data Security Regulations Against Out-of-State Entity

Article By:

Privacy and Data Security

On July 23, 2014, the Massachusetts Attorney General announced a consent judgment with an out-of-state Rhode Island hospital, Women & Infants Hospital of Rhode Island ("WIH" or the "Hospital"), resolving a lawsuit against WIH for **violations** of federal and state information security and privacy laws involving the loss of over **12,000 Massachusetts residents' sensitive patient health records.** The regulations and laws at issue were Mass. G.L. c. 93A, Mass. G.L. c. 93H and its implementing regulations codified at 201 C.M.R. 17.00 et. seq., as well as federal regulations under the Health Insurance Portability and Accountability Act ("HIPAA").

Massachusetts' data security regulations 201 C.M.R. 17.00 et. seq. are among the most comprehensive in the country. When the regulations first went into effect in March of 2010, many wondered whether the Massachusetts Attorney General would pursue actions against out-of-state enterprises given the regulations' unique reach to all "persons" or entities inside or outside of Massachusetts that own or license the personal information of Massachusetts residents. Since 2010, however, the Massachusetts Attorney General has predominately focused efforts on data breaches of Massachusetts-based businesses—launching enforcement proceedings against Massachusetts hospitals, a major Boston restaurant group, and a medical billing practice and associated medical providers.

In 2011, WIH misplaced nineteen backup tapes from two prenatal centers—one in Providence, Rhode Island and one in New Bedford, Massachusetts. The tapes contained personal information and protected health care information, including patients' names, dates of birth, Social Security numbers, dates of medical examinations, physicians' names and ultrasound images, for 12,127 Massachusetts residents and approximately 1,200 Rhode Island residents. The Massachusetts Attorney General's Office cited to "deficient employee training and internal policies" which prevented the breach from being discovered and reported in a timely manner. The Hospital did not discover that the tapes were missing until the spring of 2012 and failed to report the breach to consumers and the Massachusetts Attorney General's Office until the fall of 2012.

The consent agreement requires the Hospital to pay $150,000 to the Commonwealth of Massachusetts and to take steps to ensure compliance with state and federal security laws, including hiring an outside firm to perform audits and maintaining an up-to-date inventory of all locations, custodians, and descriptions of unencrypted electronic media and patient charts containing personal

information. Unlike Massachusetts, however, the Rhode Island Attorney General did not bring a civil suit against WIH, stating that under the Rhode Island identity theft protection law, the Attorney General was satisfied by the actions taken by the hospital to notify Rhode Island residents potentially impacted by the data breach and to offer them one year of credit monitoring. This may be a sign of Massachusetts' more aggressive approach to privacy and data security enforcement.

The case is significant because it represents one of the first Massachusetts enforcement actions against an out-of-state entity under both Massachusetts regulation 201 C.M.R. 17.00 and the new provisions of the Health Information Technology for Economic and Clinical Health ("HITECH") Act. The HITECH Act provides state attorneys general with the authority to enforce out-of-state violations of HIPAA, including disclosure of Protected Health Information ("PHI"), on behalf of state residents. Thus, this case also represents the continued efforts of state attorneys general to use their relatively new enforcement power to enforce HIPPA under HITECH.

If this consent judgment is representative of future privacy enforcement proceedings launched by the Massachusetts Attorney General, then businesses outside the Commonwealth that hold relevant privacy information may be well-advised to broadly re-examine their data security procedures, including preventative measures, to avoid running afoul of Massachusetts' strict data security regulations. Furthermore, any business entity that handles PHI under the protection of HIPPA and the HITECH Act may want to undergo a similar internal data security review given the increasing frequency of enforcement proceedings by attorneys general nationwide.

National Law Review, Volume IV, Number 226