TIP Jar

Public Agency Notification Requirements under the Information Practices Act

Spring 2017

State and federal law generally require agencies to protect the privacy of students, families and employees. Statutes like the Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g) and Education Code section 49073 prohibit the unauthorized disclosure of student records. In recent years, the California Information Practices Act of 1977 (Civ. Code, § 1798, et seq.) was amended to address the specific threat of electronic data breaches.

Data breaches can occur in a number of ways. Error is the most common reason for data breaches, and many of these breaches occur when an agency accidentally emails out private data or inadvertently puts private data on a public website. Physical breaches of data can also result if, for example, a computer or thumb drive is stolen or disposed of improperly and private data makes its way into the hands of an unauthorized third party. Additionally, approximately 15 percent of government records breaches are the result of malicious online activity such as malware, hacking or ransomware.

Data breaches are widespread and their effects are growing. In February 2016, California's Attorney General released a report on known breaches from 2012 through 2015 that affected 500 or more California residents. In 2015, approximately 178 breaches occurred and approximately 24 million records were affected, with government agencies representing about 5 percent of the total breaches. The breaches are also becoming increasingly costly: The FBI estimates that in 2015, victims of ransomware attacks paid approximately $24 million in ransom. In the first few months of 2016, that figure skyrocketed to $209 million.

The Information Practices Act requires public agencies (and other entities, such as corporations) to notify affected California residents if their personal information has been, or is reasonably believed to have been, acquired by an unauthorized party. If your agency experiences a data breach which compromises personal information, the law now requires your agency to provide notice of the breach to those affected. In addition, if 500 or more California residents are affected, notice of the breach must be provided to the California Attorney General. Notification is required by law if an individual's name is disclosed along with any of the following items: a Social Security number; driver's license number or California identification card number; account number or credit or debit card number, along with any required security code or password; medical information; health insurance information; or information or data collected through the use or operation of an automated license plate recognition system. (Civ. Code, § 1798.29(g).) Breach notification is also required if a username or email address is disclosed with a password or security question and answer that would permit access to an online account.

Interestingly, ransomware is a legal ambiguity in terms of the notice requirements set forth in the Information Practices Act because it is not clear whether the data has been "acquired" by a third party, which is the focus of the Information Practices Act, or merely encrypted. Because the law is unsettled in

Devon B. Lincoln
Partner and Co-Chair
Facilities & Business Practice Group
Monterey Office
dlincoln@lozanosmith.com

Ellen N. Denham
Associate
Walnut Creek Office
edenham@lozanosmith.com

Lozano Smith
ATTORNEYS AT LAW

this area, it is good practice to err on the side of caution and provide notice of the breach or, at a minimum, that a breach may have occurred. This will assure affected individuals that the proper steps are being taken to protect personal data and demonstrate the agency's commitment to compliance with the law.

To comply with the Information Practices Act, the breach notice must be made "in the most expedient time possible and without unreasonable delay." (Civ. Code, § 1798.29(a).) The notice must also be written in plain language and contain the following information:

- Name and phone number of the reporting agency;
- The date of breach (if known);
- A general description of the incident;
- The information subject to the breach;
- Whether notification was delayed due to a law enforcement investigation; and
- If Social Security or driver's license numbers were exposed, the notice must also include the phone numbers and addresses of the major credit reporting agencies. (Civ. Code, § 1798.29(d).)

At the discretion of the reporting agency, the security breach notification may also include information regarding what the agency has done to protect individuals whose information has been breached and advice on steps that affected individuals can take to protect themselves.

If your agency experiences a data breach, there are several steps you can take to help protect the agency, including:

1. Immediately document the incident by preparing a complete report of what happened.
2. Preserve all evidence of the breach.
3. Contact legal authorities and your insurance carriers.
4. Contact legal counsel to determine whether notification to affected persons should be provided.
5. Provide notification promptly, in the manner required by law.
6. Develop appropriate notice documentation in advance to have the notice readily available.

Unfortunately, data breaches are a common occurrence. Understanding the notification requirements of the Information Practices Act can protect government agencies from additional risk.