July 29, 2014

Encryption – Don't Leave Home (or Work) Without It

By: Robert G. Marasco | 619.906.5732 | robert.marasco@procopio.com

Encryption is more commonly becoming the recipe to avoiding the harsh consequences of a data breach. Some of those consequences include penalties for violations of the Health Insurance Portability and Accountability Act ("HIPAA") and similar state laws, governmental enforcement actions for failing to disclose a breach, or private litigation by the victims of a breach. Unsecured data is what leads to these types of consequences. So why aren't more companies that deal with confidential personal information not sufficiently securing that data? Most likely, it's the financial cost of changing the way they have done business for so long. As more and more companies, however, are dealing with data breaches and the costly consequences, there is more and more incentive to ensure the data they store is encrypted. While encryption likely will not prevent the number of unauthorized attempts to access confidential personal information, it will significantly decrease the amount of confidential personal information that is actually viewed or accessed, which is a critical aspect of being deemed liable for any of the consequences mentioned above. Indeed, the California courts have recently explained that ensuring confidential personal information is not viewed, which can be done through encryption, will permit companies and health care providers in particular from being liable for at least one of those costly consequences.

In *Sutter Health v. Superior Ct.* 2014 WL 3589699 (Cal. App. 3 Dist. July 21, 2014), the Third District Court of Appeal provided guidance for both litigants and health care providers with respect to a provider's liability under the California Confidentiality of Medical Information Act (Civil Code § 56 *et seq*.) (the "Confidentiality Act") for the release of a patient's medical information. The lesson to be learned from this case (as well as from another recent case on the topic, *Regents of University of California v. Superior Court* (2013) 220 Cal.App.4th 549) is that ensuring the confidentiality of medical information, even after it has left the provider's possession, will permit the provider to avoid liability, and this is done by encrypting the information.

The court in *Sutter Health* addressed whether a provider could be found liable for the release of medical information of approximately 4 million patients that was stored on a computer stolen from the provider, Sutter Health. The stolen computer was password protected, but the medical information had not been encrypted. The plaintiffs could not establish that their medical information was actually viewed or accessed, but they asserted that the lack of encryption amounted to a per se violation of the Confidentiality Act. On this basis the plaintiffs sought class certification for all 4 million patients and sought nominal damages of $1000 per person, as permitted by the statute, for total nominal damages of $4 billion.

The court ultimately found that plaintiffs had failed to plead a breach of confidentiality because the mere loss of possession did not amount to a breach of confidentiality. The court explained: "No breach of confidentiality takes place until an unauthorized person views the medical information. It is the medical information, not the physical record (whether in electronic, paper, or other form), that is the focus of the Confidentiality Act." *Id.* at *6. Further, "[w]hile loss of possession may result in breach of confidentiality, loss of possession does not necessarily result in a breach of confidentiality. For that reason, a plaintiff must allege a breach of confidentiality, not just a loss of possession, to state a cause of action for nominal or actual damages under sections 56.101." *Id.* Finally, the court held that "[t]he duty is to preserve confidentiality, and a breach of confidentiality is the injury protected against. Without an actual confidentiality breach there is no injury and therefore no negligence under section 56.101 [of

the Confidentiality Act]. That the records have changed possession even in an unauthorized manner does not mean they have been exposed to the view of an unauthorized person." *Id.* at *7.

Similarly, in *Regents of University of California v. Superior Court* (2013) 220 Cal.App.4th 549), the Second District Court of Appeals also considered a provider's liability under the Confidentiality Act. That case involved a stolen encrypted hard drive for which the password may have been available to the thief. Despite this distinction, along with a different analysis, the *Regents* court came to same conclusion as the *Sutter Health* court – that the analysis of a provider's liability hinges on the breach of confidentiality. "What is required is pleading, and ultimately proving, that the confidential nature of the plaintiff's medical information was breached as a result of the health care provider's negligence." *Id.* at 570.

This brings us back to the lesson at hand: Information that needs to be secured should be encrypted and not just password protected. You might ask "Why?" given that the information in the *Sutter Health* case was unencrypted and Sutter Health still prevailed. That resulted only because the plaintiffs could not establish that their information had been viewed. The unencrypted information, however, was viewable. As a result, Sutter Health was the beneficiary of simple good luck in that there was no evidence of the medical information having been viewed. The hard drive in the *Regents* case was encrypted, but possibly not password protected, which is a better scenario from a security perspective. In reality, encrypted information is a much tougher egg to crack than information that is solely password protected. This is because encryption scrambles the data on the computer and even if the data is accessed it cannot be read without the information being "decrypted," which requires a separate key. Passwords, however, simply restrict access to the data and once bypassed the data can be accessed fully. Obviously, it is better to encrypt the information to make sure it cannot be viewed than to rely on mere chance, as Sutter Health did.

In sum, encrypting the information will go far in helping a provider defend against an action under the Confidentiality Act, and more importantly demonstrate the provider is taking its obligations seriously to keep such information confidential. Such a lesson should be heeded by all companies dealing with confidential personal information because a data breach of unencrypted information could cause the company's ruin.

Robert G. Marasco utilizes his experience as a former Assistant United States Attorney to effectively and efficiently defend corporate clients and individuals, in all contexts, who are working through complex internal or government investigations, responding to grand jury and administrative subpoenas, or facing criminal prosecution. In the business context, for example, Mr. Marasco assists clients with matters involving the Foreign Corrupt Practices Act (FCPA) and other anti-bribery provisions; fraud allegations; privacy and security breaches; and the defense of professional licenses.