



Sutter Health Data Breach – Preventative Actions Could Have Helped

by **ERIC NELSON** | December 5, 2011

Guest Blog by Eric Nelson, Practice Leader – Privacy and Information Security, Lyndon Group

The Sutter Health breach is an unfortunate example of how many healthcare-related organizations currently manage an individual's personal health information. Privacy and information security may be recognized as a compliance risk, but organizations may not take a proactive approach due to limited resources or budget constraints.

It appears that the Sutter breach could have either been prevented or the scope of the breach mitigated by following some basic best practices and adhering to HIPAA privacy and security rule requirements. Some basic preventative actions that Sutter should have taken include:

- Perform a periodic inventory of protected health information (PHI) to identify internal and external systems and/or applications that contain personal data – Sutter was quoted that it took them a month to notify affected individuals because they couldn't determine which patient's data may have been on the computer.
- Conduct periodic risk assessments and gap analysis relating to privacy and information security-related policies, processes and procedures – a comprehensive risk analysis may have identified the physical vulnerability of Sutter's locations; the administrative vulnerabilities associated with storing 4 million patient records on one computer; and, the technical vulnerabilities including the need to restrict unauthorized access and encrypt at-risk data.
- Develop privacy and information security related performance and activity metrics, e.g., performing ongoing compliance reviews, physical walk-throughs (roundings), hotline and complaint management, etc. and ensure that these metrics are an integral part of an organization's corporate governance program.
- Develop a comprehensive incident response plan that includes primary and secondary response team contacts, third party contacts, state and federal reporting procedures, risk assessment procedures (to determine notification requirements) and incident review and mitigation policies and procedures.

Sutter still has many questions to answer, including why did a single desktop workstation contain the data on approximately 4 million individuals since 1995 and if encryption efforts started in 2007, how many other computers that contain PHI are still unencrypted?

Perhaps the good news is that other organizations may become aware of the Sutter breach and take appropriate steps to protect their patient's information and mitigate the financial and reputational impact of a data breach.



Are You Compliant?

Don't leave your HITECH privacy requirements to chance.

Get compliant >

 *Follow us on Twitter*

 *RSS Subscribe*

Twitter

@MN_GoBeavers Thanks for the RT!

06 Dec

@eromang Thanks for the RT!

06 Dec

Tip #6: Monitor ALL of your financial accounts
<http://t.co/ruPqf2SE>

06 Dec

CDC data on EHR adoption overlooks inconvenient facts
<http://t.co/zeEMhHHJ>

06 Dec

@dataprivacyrisk Thanks for the RT!

About the Author



ERIC NELSON

Eric Nelson is a Practice Leader with Lyndon Group serving clients that have healthcare-related needs with privacy and information security. He is a Certified Information Privacy Professional (CIPP) and specializes in federal and state privacy and information security compliance and breach mitigation and response. Eric has contributed to federal identity theft legislation and developed privacy and information security curriculum currently used by the University of Illinois. He is a frequent speaker on the subject of privacy and information security and has been interviewed and published in numerous healthcare and financial periodicals. Before leading Lyndon Group's Privacy and Information Security Practice, Eric was the Senior Principal of Secure Privacy Solutions, a risk management and compliance consulting firm offering retained privacy officer services, risk assessment, policy development, training and awareness and breach mitigation programs. He developed a best-of-breed privacy risk assessment and gap analysis process based on domestic and international frameworks, including the American Institute of Certified Professional Accountant's (AICPA) Generally Accepted Privacy Principles (GAPP) and the National Institute of Standards and Technology (NIST). Eric is a member of the International Association of Privacy Professionals (IAPP), the Health Information and Management Systems Society (HIMSS), the Health Care Compliance Association (HCCA) and the Association of Contingency Planners (ACP). He is also an active member of The Privacy Consortium, a collaborative group of leading international privacy experts.

Newsletter

Read about the latest solutions, tools, case studies and regulations from the industry experts. Sign up now.

Categories

Tags

There are no comments for this entry yet.

Add a Comment

Your comment may need to be approved before it will appear on the site. Thanks for waiting.

Submit the word you see below *

