HLB
Hooper, Lundy & Bookman, PC
HEALTH CARE LAWYERS & ADVISORS

HEALTH LAW PERSPECTIVES

Newsletter | Volume 17 | No. 1

January 2015

You've Been Hacked – Disclosing Protected Health Information to Law Enforcement in a Criminal Investigation

By Stanton J. Stock

Health care providers are quickly transitioning into the digital age. Effective security measures, however, have been slow to follow. Hackers are increasingly capitalizing on this gap by targeting health care data. This puts health care providers and their patients at risk.

Hacking personal data is, of course, a crime. An appropriate response to any crime includes preserving the evidence and contacting law enforcement. Doing so in the event of a privacy breach is especially important. Prompt apprehension of the perpetrators may mitigate further harm to patients, such as identity theft. Before turning over protected health information to the authorities, however, health care providers must be aware that state and federal laws create certain prerequisites to disclosure. Without proper compliance, providers may inadvertently turn one breach of privacy into two.

This article highlights immediate steps that should be taken in the event of a hacking incident as well as certain state and federal laws that a healthcare provider must consider when preparing to report the crime to law enforcement. Though not a comprehensive analysis of such laws, it emphasizes the importance of proper planning and preparation.

In This Issue

I. The Crime Scene

Health care providers should think of a hacking incident as a crime scene and preserve the evidence accordingly. Malware can find its way onto computers through suspicious e-mails, infected hardware, malicious websites, and compromised network connections (See following article). Once on a computer, malware may permit thieves to capture data in a number for ways. For example, some malware allows a hacker to remotely access a computer as well as any vulnerable information on the computer. Other types of malware may transmit images of information exactly as it appears on the computer screen. The route of entry, the type of malware, and the stolen data are all evidence of the crime. Once discovered, the best method for preserving the scene is to shut it down: power off affected electronic devices and disconnect them from the internet.

II. Disclosing Patient Information to Law Enforcement

In the ensuing investigation, law enforcement officials will want to quickly gather as much evidence about the crime as possible. Such evidence will include information concerning captured data. For health care providers, relevant information will probably include patients' protected health information, the disclosure

of which is restricted by federal and state laws. There are a number of permissible routes to production in the event of a hacking incident. With proper preparation, health care providers will be in a position to facilitate an investigation by clearly and quickly communicating what is required for production.

A. Federal Law

The Health Insurance Portability and Accountability Act of 1996, as amended, and regulations issued thereunder (HIPAA) establishes a minimum floor of requirements that must be met prior to disclosure, and state patient privacy laws apply if they create heightened requirements. HIPAA creates several pathways for disclosure to law enforcement officials.

The preferred HIPAA pathway is production in response to a federal grand jury subpoena. In the event of a criminal hacking incident, a criminal investigator should have no issue obtaining such a subpoena. Similarly, HIPAA also permits disclosure for law enforcement purposes pursuant to a court order, a court-ordered warrant, or a subpoena or summons issued by a judicial officer. In practice, however, a federal grand jury subpoena is an investigator's preferred choice.

Another possible option for disclosing the data is obtaining a valid authorization from the affected patients. In hacking incidents, however, the breach often involves a large number of patients, and it may be difficult or impossible to ascertain which patients were affected. Thus, patient authorization is typically not a viable option because providers are usually not able to obtain authorizations in a timely manner.

Finally, HIPAA also permits disclosure to law enforcement officials if a crime occurs on the healthcare provider's premises. If the data was stolen from computers in the facility, for example, then disclosure under HIPAA is probably permitted. It is less clear, however, whether a breach of cloud data, which is physically stored over multiple locations, would qualify as a crime on the facility's premises. Thus, another exception may be required.

B. State Law

Although any of the exceptions above may permit production under HIPAA, healthcare providers must also comply with state laws that create heightened requirements for disclosure. For example, depending on the type of records that were breached, California has several laws that may require additional precautions, even for a hacking incident.

The Confidentiality of Medical Information Act (Civil Code §§ 56.10, et seq.) (CMIA) is California's preeminent law concerning the confidentiality of medical records. As with HIPAA, CMIA also expressly permits disclosure in response to a lawfully issued search warrant or a subpoena issued by a party to a proceeding before a court. This is another reason why requesting a federal grand jury subpoena is the preferred means of production. Notably, valid subpoenas have different requirements under state and federal law. If someone in your organization is not well-versed in the legal requirements for a valid subpoena, it is best to consult legal counsel immediately.

Other California laws may impose more stringent requirements for disclosing certain types of health records. Most mental health records, for example, are covered by the Lanterman-Petris-Short Act (California Welfare and Institutions Code §§ 5328, et seq.). There are also California laws that apply only to the disclosure of HIV test results and records of substance abuse.

Finally, California also creates several statutory privileges for health records that may apply in addition to the laws discussed above. For example, a commonly applicable privilege exists for confidential communications between a physician and a patient, as defined in California's physician-patient privilege (Evidence Code §§ 990, et. seq.).

Although a physician is usually required to assert the privilege when the patient is unavailable to do so, the privilege does not apply in a criminal proceeding. This is yet another reason to request a federal grand jury subpoena before producing the records.

III. Conclusion

Again, this article does not and cannot provide a comprehensive summary of all potentially applicable laws; there are simply too many variables. It is important for healthcare providers to plan ahead so

that they know what laws apply to their data, and what steps must be taken before disclosure to law enforcement is permitted. If your facility's data has been hacked, contacting law enforcement is the right thing to do. It may prevent further harm to your facility as well as to your patients, who are your top concern. Although there are privacy concerns with reporting hacking incidents – even to law enforcement officials – proper preparation and planning will ensure an organized and timely response.

The attorneys at Hooper, Lundy & Bookman have substantial experience in assisting health care providers with responding to hacking incidents and other data breaches.

If you are in need of assistance, please contact: In San Francisco, Steve Phillips or Paul Smith at 415.875.8500; in Los Angeles, Hope Levy-Biehl or Amy Joseph at 310.551.8111; in San Diego, Jennifer Hansen or Stanton Stock at 619.744.7300; and in Washington, D.C., Kelly Carroll at 202.580.7700.

Malware Attack Exposes Security Flaws, Leads to $150,000 HIPAA Breach Settlement

By Stanton J. Stock

On Monday, December 8th, 2014, the U.S. Department of Health and Human Services (HHS), Office of Civil Rights (OCR), issued a bulletin about its $150,000 settlement with Anchorage Community Mental Health Services (ACMHS), relating to potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule. OCR's bulletin is available at: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/acmhs/acmhsbulletin.pdf The settlement agreement is available at: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/acmhs/amchs-capsettlement.pdf

The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities to provide notification to HHS following a breach of unsecured protected health information. After notification is provided, OCR investigates whether covered entities complied with the applicable provisions of the Privacy and Security Rules. If OCR identifies violations, it may pursue a civil money penalty in the amount of $100-$50,000 per violation, up to a maximum penalty of $1.5 million for identical violations.

In determining the appropriate amount of a penalty, OCR will consider several factors, including the nature and extent of the violation, the nature and extent of resulting harm, the covered entity's history of compliance, and the covered entity's financial condition.

ACMHS is a five-facility, nonprofit organization providing behavioral health care services in Anchorage, Alaska. On March 2, 2012, ACMHS reported a breach of unsecured electronic protected health information (ePHI) affecting 2,743 individuals.

The breach occurred over the span of approximately

HLB Briefs

HLB Attorney Charles Oppenheim has authored the just released AHLA book: ***Stark Law: Comprehensive Analysis + Practical Guide.*** A nationally recognized Stark Law expert, Mr. Oppenheim previously wrote all five editions of the *American Health Lawyers Association Monograph on Stark Law*, beginning in 1998. The book is available at http://www.lexisnexis.com/ahla/ProductDetail.aspx?id=141

Hooper, Lundy & Bookman, PC, is pleased to announce that the following attorneys have been named Senior Counsel: Nina Adatia Marsden and Amanda Hayes-Kibreab of the firm's Los Angeles Office, and Joseph LaMagna of the firm's San Diego Office.
HLB is also pleased to announce that Partner Hope Levy-Biehl has been named Co-Chair of the firm's Regulatory Department.

two weeks, from December 20, 2011, through January 4, 2012. The breach was caused by malware that had been installed on a desktop computer.

OCR initiated an investigation and alleged that ACMHS violated HIPAA's Security Rule in at least three ways. First, OCR alleged that ACMHS failed to conduct an accurate and thorough assessment of the potential risks to the confidentiality and availability of its ePHI, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A). Second, although ACMHS adopted sample policies and procedures requiring the implementation of security measures, OCR alleged ACMHS altogether failed to implement its policies and procedures, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(B). Third, OCR alleged ACMHS failed to implement basic technical security measures to guard against a breach, including ensuring that adequate firewalls were in place and that information technology resources were both supported and regularly updated with available patches. The bulletin describes these measures as part of a "common sense approach to assessing and addressing the risks to ePHI on a regular basis[.]". ACMHS complied with OCR's investigation and ultimately agreed to settle the alleged violations for a total civil monetary penalty of $150,000. In addition to the penalty, the settlement agreement includes a corrective action plan and requires ACMHS to report on the state of its compliance to OCR for two years. OCR provides a Security Rule Risk Assessment Tool, which is available at: http://www.healthit.gov/providers-professionals/security-risk-assessment

The settlement highlights an important issue for HIPAA covered entities. As the health care industry rapidly transitions towards technology-based care, proper compliance requires frequently assessing ePHI security risks and updating protective measures. It is not enough to simply adopt model security policies and procedures. Policies and procedures must be effectively implemented, periodically renewed and updated as necessary to address new threats and changes in the organization's operations and structure.

Hooper, Lundy & Bookman assists clients with federal and state medical-privacy law compliance, including assessing and addressing security risks and responding to breaches of privacy.

For more information, please contact: In San Francisco, Steve Phillips or Paul Smith at 415.875.8500; in Los Angeles, Hope Levy-Biehl or Amy Joseph at 310.551.8111; in San Diego, Jennifer Hansen or Stanton Stock at 619.744.7300; and in Washington, D.C., Kelly Carroll. 202.580.7700.

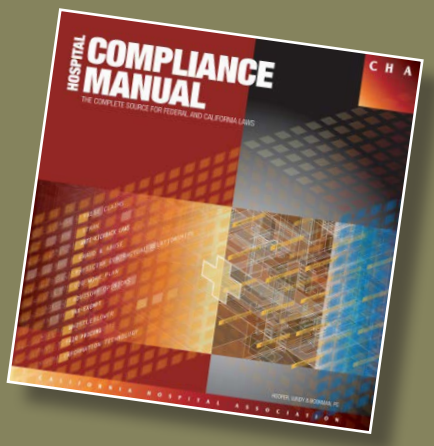
CHA Announces New Edition of Hospital Compliance Manual

The California Hospital Association (CHA) has just released the 2015, 6th Edition of the California Hospital Compliance Manual.

New to the 2015 edition are detailed explanations of state law regarding hospital financial assistance policies required by SB 1276 and IRS regulations that impact not-for-profit hospitals released on Dec. 31, 2014.

CHA's compliance manual is the only publication written for hospital compliance officers that integrates California with federal law regarding high-risk compliance areas.

Written by Hooper, Lundy & Bookman, PC, attorneys and CHA, the manual focuses on key components of an effective compliance program. The manual features nearly 700 pages of content including 16 chapters, a model hospital compliance plan, numerous compliance forms and appendixes, and an index.



The Manual includes the following Chapters:

- **Hospital Compliance Plans**
- **Governing Boards**
- **Federal and State False Claims Acts**
- **Submission of Accurate Claims Information**
- **Proper Cost Reporting Practices**
- **Physician Self-Referral Laws**
- **Federal and State Anti-Kickback Laws**
- **Financial Assistance Policies — NEW chapter includes federal regulations**
- **Issues for Tax-Exempt Hospitals**
- **Fundamentals of Hospital Licensing and Certification**
- **Screening for Excluded Providers and Suppliers**
- **Hospital Signage Requirements**
- **Patient Safety Organizations**
- **Other Laws**
- **Repayment and Self-Disclosure**
- **Responding to Government Audits and Investigations**

To order the new manual or for more information, see www.calhospital.org/compliance.

CALENDAR

January 7-11

2015 National CLE Conference Health Law Program, Vail, CO
Robert Roth presented ***Report from the Capitol – Reflections on a Gridlocked Year and Prospects for 2015.***

February 3,10

CHA Annual Hospital Compliance Seminar, Long Beach, CA
Hooper Lundy and Bookman attorneys are once again lead faculty for this annual seminar. Attorneys presenting include Lloyd Bookman, Patric Hooper, Hope Levy-Biehl, Felicia Sze, and Joseph LaMagna. Information and registration is available at:
http://www.calhospital.org/hospital-compliance

February 11

LACBA Presents A Conversation on 1206(l) Medical Foundations
Charles Oppenheim moderates and Jennifer Hansen participates on the panel.

February 19

CHA Rural Hospital Symposium , Redondo Beach, CA
Steve Lipton presents ***Managing Challenging Patients in the ED***

February 24-25

AHLA LTC & The Law Conference, New Orleans
Mark Reagan co-presents ***Post-Acute Providers and Understanding The Focus on Quality from a Managed Care Plan Perspective.***

March 31

Medtrade Spring Convention, Las Vegas
Felicia Sze presents ***Managed Care Contracting: Cutting Through the Legalese and Managing the Managed Care Relationship: Enforcing Your Contracts with Plans.***

HLB
HOOPER, LUNDY & BOOKMAN, PC
HEALTH CARE LAWYERS & ADVISORS
1875 Century Park East, Suite 1600
Los Angeles, California 90067-2799