kbr

KAUFMAN BORGEEST & RYAN LLP

KBR's Cyber Health 2017

Meet Our Firm

Kaufman Borgeest & Ryan LLP is a professional liability and insurance defense firm of dedicated and experienced attorneys. Our objective is to vigorously pursue cost-effective dispute resolution. We pride ourselves on the academic excellence of our lawyers and the outstanding results we have obtained in complex litigation and insurance matters.

Cyber Practice

KBR's Cyber Practice is focused on the ever-increasing risks and rapidly evolving liability exposures associated with the creation, transmission, security and storage of data, particularly private, personal and proprietary information. We are fortunate to have excellent attorneys with extensive knowledge and expertise in many areas, including coverage and litigation, as well as cyber risk assessment, analysis and mitigation. As a result, KBR is able to offer an array of cyber services to our clients.

Cyber Liability Healthcare Team

KBR is uniquely focused on healthcare organizations and our cyber liability experience is fine-tuned to the healthcare industry's particular cyber issues. Members of our Cyber Liability Healthcare Team include:

- **Andrew S. Kaufman, Esq. (Partner)**

Mr. Kaufman is a nationally recognized preeminent trial attorney, and brings over 30 years of litigation experience and knowledge of the law to the Cyber Liability Healthcare Team. He presents to and counsels healthcare individuals and entities on risk assessment issues, analyses and best practices at some of the top medical centers and providers around the country. He has tried more than one hundred cases to verdict, including numerous cases of multimillion-dollar exposure. He has also represented a number of well-known medical device and pharmaceutical manufacturers.

- **Carol S. Doty, Esq., CIPP/US (Partner)**

Ms. Doty has over 17 years of experience as an attorney, and over 20 years of experience as a practicing nurse. An active member on the Board of the American Society of Health and Risk Managers in Connecticut, Ms. Doty has extensive knowledge and understanding of the healthcare industry, and is a Certified Information Privacy Professional (CIPP/US) designated by the International Association of Privacy Professionals (IAPP). Ms. Doty counsels healthcare clients on cyber issues, including HIPAA compliance and pre-breach risk assessments and best practices. She has presented nationally at the Crittenden Medical Insurance Conference, the New England Regional Conference for Health and Risk Managers, and webinars for the Knowledge Group, as well as locally throughout the Northeast.

- **Betsy D. Baydala, Esq., CIPP/US (Senior Associate)**

Ms. Baydala has over 8 years of litigation experience and is a designated Certified Information Privacy Professional by the IAPP. She has focused her practice on cyber liability issues affecting the healthcare industry, and has written extensively in this area. Ms. Baydala counsels healthcare clients and insurers

on the ever evolving cyber liability risks and exposures affecting the industry. She has presented for the New York State Bar Association, the Connecticut Society for Health and Risk Managers, and webinars for the Knowledge Group.

- **Adrian Ruiz (In-House Technology Consultant)**

Mr. Ruiz leads technology assessments and network and systems audits related to cyber liability claims. He works collaboratively with the Cyber Practice to provide technological interpretation and assistance in the investigation and evaluation of cyber liability claims. Mr. Ruiz has over 20 years in the professional consulting industry and has led, and implemented, mid-to-large scale projects across many vertical markets in both the private and public sector.

Contact Information

For more information about our firm, please visit our website
www.kbrlaw.com

Please also feel free to contact us directly:

Carol S. Doty
cdoty@kbrlaw.com
(203) 557-5700

Betsy D. Baydala
bbaydala@kbrlaw.com
(212) 980-9600

TABLE OF CONTENTS

KBR's Cyber Health 2017

Introduction

One of the key objectives of the HITECH Act of 2009 was to encourage healthcare providers to adopt and meaningfully use electronic health records (EHRs). Since then, the health IT landscape has rapidly evolved. According to a recent report from the Office of the National Coordinator for Health Information Technology, adoption of EHRs among non-federal acute care hospitals is nearly universal with a nine-fold increase in the adoption of EHRs since 2008.[1] In 2008, only 17% of physicians and 9% of hospitals had at least a basic EHR, versus 78% of physician offices and 96% of hospitals using certified EHR technology in 2015.

The benefits of electronic health information are undeniable. EHRs allow healthcare providers to more efficiently share information and to improve patient care and coordination. Patients have easier access to their health information, which encourages active patient participation and management of their own health. EHRs also reduce paperwork and administrative burdens, cut costs, and reduce medical errors.

With the amount of electronic health information reaching unprecedented levels, the storing and transmitting of this information poses unique cybersecurity risks and challenges. According to NetDiligence's study of cyber claims submitted between 2013 and 2015, the healthcare industry was the most frequently breached sector, with the average payout totaling $726,000.[2] Hackers were the most frequent cause of loss (23%), followed by malware/virus (21%), staff mistakes (9%) and rogue employees (7%). Over 113 million records were affected due to breaches in the healthcare industry in 2015.[3]

With these statistics in mind, our paper is intended to provide an overview of the cyber legal landscape relative to the healthcare industry. We review the applicable federal and state laws, with a particular emphasis on the HIPAA Rules. We also take a look back at 2016 to examine the federal and state governments' enforcement of the HIPAA Rules, case law developments in active healthcare date breach litigation, and the hot topics of ransomware and cybersecurity of medical devices.

Statutes & Laws

HIPAA & the HITECH Act

The U.S. Department of Health and Human Services' (HHS) foremost regulations protecting patient health information are the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[4] and the Health Information Technology for Clinical and Economic Health (HITECH) Act of 2009.[5]

HIPAA applies to both "covered entities" and "business associates." A "covered entity" is defined as a health plan, a healthcare clearinghouse, or a healthcare provider who transmits any health information in electronic form in connection with a transaction covered under HIPAA.[6] With the widespread adoption of EHRs following the HITECH Act, nearly every healthcare provider is a "covered entity" and subject to HIPAA's requirements. A "business associate" is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information (PHI) on behalf of, or provides services to, a covered entity.[7] The HITECH Act expanded the responsibilities of business associates under HIPAA, and HHS is in the process of developing regulations to implement and clarify these changes.

The major components of HIPAA, and as amended by the HITECH Act, are the Privacy, Security, Breach Notification and Enforcement Rules. The HIPAA Rules are intended to enhance patient privacy and security protections, provide individuals with certain rights and control over their health information, and strengthen the government's ability to enforce the law. Below is a brief summary of each of these HIPAA Rules.

Privacy Rule

The HIPAA Privacy Rule establishes national standards to safeguard the privacy of individually identifiable health information (or PHI).[8] This rule sets limits and conditions on the use and disclosure of PHI without patient authorization. It also gives patients rights over their health information, such as the right to examine and obtain a copy of their health records and request corrections, which is vital to patients' health. The Privacy Rule requires a covered entity to obtain satisfactory assurances in writing from its business associate that the business associate will appropriately safeguard the PHI it receives or creates on behalf of the covered entity.

The HIPAA Privacy Rule is balanced in that it provides for the protection of PHI held by a covered entity, while permitting the disclosure of health information as needed for patient care and other important purposes. If a covered entity becomes aware of an improper disclosure of PHI, the HIPAA Privacy Rule requires the covered entity to mitigate, to the extent practicable, any harmful effect caused by such disclosure.

Security Rule

The HIPAA Security Rule sets forth a series of administrative, physical and technical safeguards for covered entities to ensure the confidentiality, integrity, and availability of individuals' electronic protected health information (ePHI).[9] For example, a covered entity must identify and protect against reasonably anticipated threats to the security or integrity of ePHI. Protecting ePHI's "integrity" means preventing the alteration or destruction of ePHI in an unauthorized manner. A covered entity must also protect against reasonably anticipated, impermissible uses or disclosures of ePHI, and ensure compliance by its workforce. If a covered entity knows of an activity or practice of its business associate that constitutes a material breach or violation of the business associate's obligation, the covered entity must take reasonable steps to cure the breach or end the violation.

The HIPAA Security Rule is flexible and allows a covered entity to analyze its own needs and implement safeguards appropriate for its own environment. When deciding on which security measures to implement, a covered entity must consider its size, complexity and capabilities; its technical hardware and software infrastructure; the costs of security measures; and the likelihood and possible impact of potential risks to ePHI. Because of the rapidly changing technological environment, the HIPAA Security Rule requires covered entities to periodically review and, as appropriate, modify their security measures.

Breach Notification Rule

The HIPAA Breach Notification Rule requires covered entities to provide notification following a breach of unsecured PHI.[10] Generally, "a breach" is defined as an impermissible use or disclosure of PHI that compromises the security or privacy of the PHI by posing a significant risk of financial, reputational, or other harm to the individual.[11] An impermissible use or disclosure of PHI is presumed to be a breach, unless after the performance of a risk assessment of a number of factors enumerated under HIPAA the covered entity demonstrates that there is a low probability that the PHI was compromised.

Enforcement Rule

The HIPAA Enforcement Rule contains provisions relating to compliance and investigations, as well as the imposition of civil monetary penalties (CMPs) for violations of HIPAA.[12] HHS' Office of Civil Rights (OCR) is responsible for enforcing the HIPAA Privacy and Security Rules.

Since compliance with the HIPAA Privacy Rule became effective in April 2003, OCR has received over 144,622 HIPAA complaints.[13] 17% of those cases have been resolved by requiring changes in privacy practices and corrective actions, or providing technical assistance to HIPAA covered entities and their business associates. Corrective measures have been applied in all cases where OCR's investigation demonstrated noncompliance by the covered entity or business associate, and OCR is likely to include a

settlement with the entity in lieu of imposing CMPs. To date, OCR has settled 41 cases totaling $48,679,700.[14] Twice OCR has sought CMPs for HIPAA violations.[15]

OCR also has the authority to refer appropriate cases to the U.S. Department of Justice (DOJ) for criminal investigation of the knowing disclosure or obtaining of protected health information in violation of the HIPAA Rules. To date, OCR has referred 589 cases to the DOJ.[16]

In addition, authority has been given to State Attorneys Generals to bring civil actions against a covered entity on behalf of state residents for violations of the HIPAA Privacy and Security Rules.[17]

Cybersecurity Information Sharing Act of 2015

On December 18, 2015, the Cybersecurity Information Sharing Act (CISA) of 2015 was signed into law. CISA is intended to improve cybersecurity in the U.S. through enhanced sharing of information about cybersecurity threats by and with the federal government. CISA directs the federal government to promulgate procedures to facilitate the timely sharing of certain cyber threat indicators in its possession, and to periodically share cybersecurity best practices based on information it receives.

Under CISA, companies are authorized to monitor and implement defensive measures on their own information systems in order to counter cyber threats. A "defensive measure" is defined as something applied to an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability. By providing certain protections, CISA encourages companies to voluntarily share information they obtain about cyber threat indicators and their defensive measures. In order to obtain the liability protections afforded under CISA, companies must comply with CISA's information sharing requirements, such as the removal of personal information.

CISA is additionally tailored to improve cybersecurity in the healthcare industry. Under Title IV of CISA, HHS was directed to establish a Healthcare Industry Cybersecurity Task Force to:

(A) analyze how other industries have implemented strategies and safeguards for addressing cybersecurity threats;

(B) analyze challenges and barriers private entities in the healthcare industry face securing themselves against cyber attacks;

(C) review challenges that covered entities and business associates face in securing networked medical devices and other software or systems that connect to an electronic health record;

(D) provide the Secretary of HHS with information to disseminate to healthcare industry stakeholders for purposes of improving their preparedness for, and response to, cybersecurity threats affecting the healthcare industry;

(E) establish a plan for creating a single system for the federal government to share information on actionable intelligence regarding cybersecurity threats to the healthcare industry in near real time; and

(F) report to Congress on the findings and recommendations of the task force regarding carrying out subparagraphs (A) – (E).[18]

In accordance with CISA, HHS created its Task Force, which held four in-person meetings in 2016. The Task Force's findings and recommendations report is expected to be delivered sometime in 2017.[19]

In June 2016, the U.S. Department of Homeland Security and the DOJ issued guidance to assist non-federal entities sharing information under CISA.[20]

FTC's Health Breach Notification Rule

In recent years, numerous web-based businesses and online applications, such as exercise trackers and wearable health technologies, have emerged whereby people collect their own health information. In most cases these business and applications do not fall under the definition of a "business associate" or "covered entity" under HIPAA. As a result, the Federal Trade Commission (FTC) promulgated the Health Breach Notification Rule, which requires certain businesses not covered under HIPAA to notify their customers and others if there is a breach of unsecured, individually identifiable electronic health information.[21]

The Rule requires notice when there is an unauthorized acquisition of identifiable health information that is unsecured (any information that is not encrypted or destroyed) and is in a personal health record. Notification must be given to each affected person who is a U.S. citizen or resident, the FTC, and in the case of certain breaches involving 500 or more people, the media. Breaches involving the health information of fewer than 500 individuals may be reported in an annual submission that includes all relevant breaches within the calendar year. The Rule specifies the timing, method, and content of any required notification.

State Breach Notification Laws

Nearly all the states have enacted legislation requiring private, governmental or educational entities to notify individuals of security breaches of information involving personally identifiable information. Below is a highlight of those laws applicable to New York and Connecticut.

New York: New York State Information Security Breach and Notification Act

Under the New York State Information Security Breach and Notification Act, which is comprised of sections from the State Technology Law and General Business Law, state entities and persons or businesses conducting business in New York who own or license computerized personal information must disclose any breach of the data to New York residents. Personal information is defined as a combination of name, social security number, driver's license number, account number, or credit and debit card number. A proposed bill seeks to add "any unsecured protected health information held by a 'covered entity' as defined in [HIPAA]" to the definition of "personal information."[22]

Under section 899-aa of the General Business Law, in addition to notifying NY residents, a person or business conducting business in New York must notify: (1) the NYS Attorney General; (2) the NYS Division of State Police; and (3) the Department of State's Division of Consumer Protection. Under section 208 of the State Technology Law, a state entity must also notify: (1) the NYS Attorney General; (2) the NYS Office of Information Technology Services' Enterprise Information Security Office; and (3) the Department of State's Division of Consumer Protection.

Upon determination of a data breach, disclosure must be made in the most expedient time possible and without unreasonable delay. Law enforcement may require a delay in notification if they believe disclosure would impede a criminal investigation. When notifying New York residents, there must be a description of the types of information believed to have been acquired by a person without valid authorization, and the disclosing entity or person's contact information. State entities are also required to notify non-residents. The NYS Information Security Breach and Notification Act Reporting Form must be completed and submitted to each specified state entity.[23]

Connecticut: Breach of Security re Computerized Data Containing Personal Information

Pursuant to Connecticut General Statutes § 36a-701b and Senate Bill 949 (Public Act. No. 15-142), anyone who conducts business in Connecticut and who – in the ordinary course of business – owns, licenses or maintains computerized data that includes personal information is required to disclose a security breach without unreasonable delay and no later than 90 days after the discovery of such breach (unless a shorter time is required by federal law) to state residents whose personal information is believed to have been compromised.

In addition, business owners must notify the Connecticut Office of the Attorney General no later than when the affected residents are notified. Failure to provide such notice may be considered a violation of the Connecticut Unfair Trade Practices Act.

In the case of a breach or suspected breach involving social security numbers, businesses are required to provide appropriate identity theft prevention services and, if applicable, identity theft mitigation services. These services are to be provided at no cost to such resident for a period of no less than 12 months.

Senate Bill 949 also requires health insurers, healthcare centers, and other similar regulated entities to "implement and maintain a comprehensive information security program to safeguard the personal information of insureds and enrollees that is compiled or maintained by such company." The program must be in writing and contain administrative, technical and physical safeguards appropriate in light of the size, scope and type of business of such company, the amount of resources available, the amount of data compiled or maintained, and the need for security and confidentiality of such data. These organizations are also required to update the program "as often as necessary and practicable but at least annually." These programs must be in place no later than October 1, 2017.

HIPAA Enforcement

HHS' Office of Civil Rights

HHS' OCR is responsible for enforcing the HIPAA Privacy and Security Rules. OCR's main functions are the investigation of HIPAA complaints filed with OCR; compliance reviews to determine if covered entities and business associates are in compliance with HIPAA; and performance of education and outreach to foster compliance with the HIPAA Privacy and Security Rules.

If OCR determines after an investigation or compliance review that a covered entity or business associate has not complied with HIPAA, OCR will attempt to resolve the case through voluntary compliance, corrective action and/or a resolution agreement. A resolution agreement is a binding contract signed by HHS and the covered entity or business associate, whereby the entity agrees to perform certain obligations (e.g., staff training) and likely agrees to the payment of a resolution amount. A resolution agreement is typically used to settle more serious violations of HIPAA. If the covered entity or business associate does not take satisfactory action to resolve the matter, OCR may decide to impose CMPs.

In 2016, OCR made public the following resolution agreements with covered entities and business associates, which highlights important lessons learned with regard to HIPAA compliance.

- **$1.55 million settlement underscores the importance of executing HIPAA business associate agreements**

North Memorial Health Care of Minnesota submitted a breach report to OCR following the theft of an unencrypted, password-protected laptop from a business associate's workforce member's locked vehicle, which impacted the ePHI of nearly 9,500 individuals. OCR's investigation revealed that North Memorial did not have a business associate agreement in place when it gave its business associate access to the hospital's database storing ePHI of 289,904 patients. North Memorial agreed to pay $1,550,000 to settle potential HIPAA violations.

"*Two major cornerstones of the HIPAA Rules were overlooked by this entity. Organizations must have in place compliant business associate agreements as well as an accurate and thorough risk analysis that addresses their enterprise-wide IT infrastructure.*" –Jocelyn Samuels, Director of OCR[24]

- **Improper disclosure of research participants' PHI results in $3.9 million HIPAA settlement**

Feinstein Institute for Medical Research filed a breach report with the OCR after a laptop containing the ePHI of approximately 13,000 patients and research participants was stolen from an employee's car.

After investigation, OCR determined that Feinstein's security management process was limited in scope, incomplete and insufficient to address potential risks and vulnerabilities to ePHI. Feinstein also lacked policies and procedures for authorizing access to ePHI by its workforce, failed to implement safeguards to restrict access to unauthorized users, and lacked policies and procedures to govern the receipt and removal of laptops containing ePHI into and out of its facilities. Feinstein paid $3.9 million to settle potential violations of the HIPAA Privacy and Security Rules.

"*Research institutions subject to HIPAA must be held to the same compliance standards as all other HIPAA-covered entities. For individuals to trust in the research process and for patients to trust in those institutions, they must have some assurance that their information is kept private and secure.*" –OCR Director Samuels[25]

- **$750,000 settlement highlights the need for HIPAA business associate agreements**

Raleigh Orthopaedic Clinic, P.A. of North Carolina submitted a breach report to OCR after it released the x-rays and related PHI of 17,300 patients to an entity that promised to transfer the images to electronic media in exchange for harvesting the silver from the x-ray films without executing a business associate agreement. Raleigh Orthopaedic agreed to pay $750,000 to settle charges that it potentially violated the HIPAA Privacy Rule.

"*HIPAA's obligation on covered entities to obtain business associate agreements is more than a mere check-the-box paperwork exercise. It is critical for entities to know to whom they are handing PHI and to obtain assurances that the information will be protected*." –OCR Director Samuels[26]

- **Business associate's failure to safeguard nursing home residents' PHI leads to $650,000 HIPAA settlement**

Catholic Health Care Services of the Archdiocese of Philadelphia (CHCS) provided management and information technology services as a business associate to six skilled nursing facilities. CHCS agreed to pay $650,000 to settle potential violations of the HIPAA Security Rule after the theft of a CHCS-issued employee iPhone, which was unencrypted and not password protected and compromised the ePHI of 412 nursing home residents. At the time of the incident, CHCS had no policies addressing the removal of mobile devices containing PHI from its facility or what to do in the event of a security incident. CHCS also did not have a risk analysis or risk management plan.

"*Business associates must implement the protections of the HIPAA Security Rule for the electronic protected health information they create, receive, maintain, or transmit from covered entities. This includes an enterprise-wide risk analysis and corresponding risk management plan, which are the cornerstones of the HIPAA Security Rule.*" –OCR Director Samuels[27]

- **Widespread HIPAA vulnerabilities result in $2.7 million settlement**

Oregon Health & Science University (OHSU) submitted multiple breach reports affecting thousands of individuals to OCR, including two reports involving unencrypted laptops and another large breach involving a stolen unencrypted thumb drive. OCR's investigation uncovered widespread vulnerabilities within OHSU's HIPAA compliance program, such as the storage of ePHI of over 3,000 individuals on a cloud-based server without a business associate agreement. OHSU also had no policies and procedures to prevent, detect, contain, and correct security violations. In addition, OHSU failed to implement a mechanism to encrypt and decrypt ePHI maintained on its workstations, despite having identified this lack of encryption as a risk. OHSU agreed to pay a monetary settlement of $2.7 million and address the widespread HIPAA compliance problems through a comprehensive three-year corrective action plan.

"*This settlement underscores the importance of leadership engagement and why it is so critical for the C-suite to take HIPAA compliance seriously*." –OCR Director Samuels[28]

- **Multiple alleged HIPAA violations result in $2.75 million settlement**

The University of Mississippi Medical Center (UMMC) suffered a breach of unsecured ePHI affecting approximately 10,000 individuals after a password-protected laptop went missing from its Medical Intensive Care Unit. The laptop was likely stolen by a visitor who had inquired about borrowing one of the laptops.

OCR's investigation revealed that ePHI stored on a UMMC network drive was vulnerable to unauthorized access via its wireless network because users could access an active directory containing 67,000 files after entering a generic username and password. OCR further determined that UMMC was aware of risks and vulnerabilities to its systems as far back as April 2005, but took no significant risk management activity until after the breach. OCR attributed this lack of action to organizational deficiencies and insufficient institutional oversight. UMMC agreed to pay a resolution amount of $2.75 million and to adopt a corrective action plan to assure future compliance with the HIPAA Rules.

"*In addition to identifying risks and vulnerabilities to their ePHI, entities must also implement reasonable and appropriate safeguards to address them within an appropriate time frame. We at OCR remain particularly concerned with unaddressed risks that may lead to impermissible access to ePHI*." -OCR Director Samuels[29]

- **Advocate Health Care settles potential HIPAA penalties for $5.55 million**

Advocate Health Care Network is the largest fully-integrated healthcare system in Illinois and one of the largest health systems in the country. Advocate submitted three breach notification reports to OCR with the combined breaches affecting the ePHI of approximately 4 million individuals. OCR's investigations revealed that Advocate had failed to: (1) conduct an accurate and thorough assessment of potential risks and vulnerabilities to all its ePHI; (2) implement policies and procedures and facility access controls

to limit physical access to the electronic information systems housed within a large data support center; (3) obtain satisfactory assurances in the form of a written business associate contract that its business associate would appropriately safeguard all ePHI in its possession; or (4) reasonably safeguard an unencrypted laptop when left in an unlocked vehicle overnight.

Advocate agreed to pay a settlement amount of $5.5 million, which to date, is the largest settlement against a single entity. OCR explained that this settlement amount was due to the extent and duration of the alleged non-compliance (dating back to 2007 in some instances), the involvement of the State Attorney General in a corresponding investigation, and the large number of individuals whose information was affected by Advocate.

"We hope this settlement sends a strong message to covered entities that they must engage in a comprehensive risk analysis and risk management to ensure that individuals' ePHI is secure. This includes implementing physical, technical, and administrative security measures sufficient to reduce the risks to ePHI in all physical locations and on all portable devices to a reasonable and appropriate level." – OCR Director Samuels[30]

- **HIPAA settlement illustrates the importance of reviewing and updating, as necessary, business associate agreements**

Care New England Health System (CNE) provides centralized corporate support for a number of hospitals and healthcare providers in Massachusetts and Rhode Island. OCR received notification from Women & Infants Hospital of Rhode Island (WIH), a covered entity member of CNE, of the loss of unencrypted backup tapes containing the ultrasound studies of approximately 14,000 individuals. WHI and CNE had executed a business associate agreement effective March 2005, but the agreement was never updated until after OCR's investigation in 2015 and, as a result, did not incorporate revisions required under the HIPAA Omnibus Final Rule, such as obtaining satisfactory assurances from CNE.

CNE agreed to a monetary settlement of $400,000 and a comprehensive corrective action plan. WIH entered into a separate consent judgment with the Massachusetts Attorney General's Office and reached a settlement of $150,000. While the Attorney General's action did not legally preclude OCR from imposing civil monetary penalties against WIH, OCR determined not to include additional potential violations against WIH.

"*This case illustrates the vital importance of reviewing and updating, as necessary, business associate agreements, especially in light of required revisions under the Omnibus Final Rule. The Omnibus Final Rule outlined necessary changes to established business associate agreements and new requirements which include provisions for reporting. A sample Business Associate Agreement can be found on OCR's website to assist covered entities in complying with this requirement.*" –OCR Director Samuels[31]

- **$2.14 million HIPAA settlement underscores importance of managing security risk**

St. Joseph Health (SJH), a nonprofit integrated Catholic healthcare delivery system in California, Texas and New Mexico, reported to OCR that files containing ePHI of 31,800 individuals were publically accessible through internet search engines from 2011 to 2012. The server SJH purchased to store the files included a file sharing application with a default setting allowing anyone with an internet connection to access them. Upon implementing the server, SJH did not examine or modify it. OCR determined that although SJH had hired a number of contractors to assess the risks and vulnerabilities to the confidentiality, integrity and availability of ePHI held by SJH, it was conducted in a patchwork fashion and did not result in an enterprise-wide risk analysis as required by the HIPAA Security Rule. SJH agreed to a settlement amount of $2,140,500 and to adopt a comprehensive corrective action plan.

"*Entities must not only conduct a comprehensive risk analysis, but must also evaluate and address potential security risks when implementing enterprise changes impacting ePHI. The HIPAA Security Rule's specific requirements to address environmental and operational changes are critical for the protection of patient information.*" –OCR Director Samuels[32]

- **UMass settles potential HIPAA violations following malware infection**

The University of Massachusetts Amherst (UMass) reported that a workstation in its Center for Language, Speech, and Hearing (the Center) was infected with a malware program resulting in the impermissible disclosure of ePHI of 1,670 individuals. The malware was a generic remote access Trojan that infiltrated their system and provided impermissible access to ePHI because UMass did not have a firewall in place. OCR's investigation revealed that UMass failed to designate all of its healthcare components when hybridizing the university because it did not determine that the Center was a healthcare component. As a result, UMass did not implement policies and procedures at the Center to ensure compliance with the HIPAA Rules. UMass agreed to pay a settlement of $650,000, which OCR advised was reflective of the fact that the University operated at a financial loss in 2015.

"*HIPAA's security requirements are an important tool for protecting both patient data and business operations against threats such as malware. Entities that elect hybrid status must properly designate their healthcare components and ensure that those components are in compliance with HIPAA's privacy and security requirements."* –OCR Director Samuels[33]

State Attorneys Generals

Under the HITECH Act, state attorneys generals became empowered to enforce the HIPAA rules by permitting civil actions against violators.[34] State Attorneys Generals are permitted to obtain damages on behalf of state residents or to enjoin further violations of HIPAA.

Connecticut

The Connecticut Attorney General's Office (CT AG) was the first state Attorney General to independently enforce HIPAA violations. In January 2010, the CT AG brought an action against Health Net alleging that it was responsible for "failing to secure private patient medical records and financial information involving 446,000 CT enrollees and for failing to promptly notify consumers endangered by the security breach" after a portable hard disk had been either lost or stolen at Health Net's Shelton, CT offices.[35] That disk contained 27.7 million pages of various types of documents, such as insurance claim forms, membership forms, appeals and grievances, correspondence and medical records of 1.5 million past and present members of Health Net plans, including over 500,000 CT residents.

Because the data was not encrypted or protected from access by unauthorized persons or third parties, the CT AG alleged that Health Net violated the HIPAA Security and Privacy Rules. After a year and a half of litigation, a judgment was entered into mapping out an onerous Corrective Action Plan and Health Net was directed to pay $250,000.

In November 2015, the CT AG's Office announced that it reached an agreement with Hartford Hospital and EMC Corporation following the breach of patient information.[36] In 2012, a laptop containing unencrypted patient information of approximately 8,883 CT residents was stolen. Hartford Hospital had retained EMC to assist with a quality improvement project concerning readmissions to the hospital. Pursuant to the agreement, Hartford Hospital and EMC Corporation paid $90,000 to the CT's General Fund and instituted additional training and control measures in response to the breach.

New York

In November 2015, the University of Rochester Medical Center (URMC) entered into a Resolution Agreement with the New York State Office of the Attorney General (NY AG) in connection with an impermissible disclosure of PHI when a nurse left the employment of URMC.[37]

In March 2015, the URMC nurse who was leaving to work at another facility, asked URMC for a list of patients she had treated at URMC. URMC gave the nurse over 3,400 patient names, addresses and diagnoses. The nurse then gave those names to her new employer without first obtaining authorization from the patients. The nurse's new employer mailed letters to those patients announcing that the nurse was joining the practice and giving them the option to be treated at the facility. The patients

complained to URMC about the letter and URMC notified HHS of the incident and sent a breach notification letter to those patients affected.

As part of the Resolution Agreement with the NY AG, URMC agreed to pay $15,000 in HIPAA penalties and other resolutions, including strict reporting requirements for three years and workforce training. NY AG Eric T. Schneiderman advised that the settlement with URMC has put "other healthcare entities on notice that [his] office will enforce HIPAA data breach provisions."[38]

Case Law Developments

Sixth Circuit affirms dismissal of action brought under the False Claims Act premised on non-compliance with the HITECH Act due to impermissible disclosures of ePHI

In U.S. ex rel. Sheldon v. Kettering Health Network, 816 F.3d 399 (6th Cir. 2016), the Sixth Circuit Court of Appeals affirmed the lower court's granting of Kettering Health Network's motion to dismiss. In the underlying *qui tam* action brought under the False Claims Act (FCA), Vicki Sheldon alleged that Kettering Health falsely certified its compliance with the HITECH Act and, as a result, received "meaningful use" incentive payments.

Sheldon alleged that Kettering Health's attestations of compliance under the HITECH Act were false because she received two letters from Kettering Health informing her that employees had impermissibly accessed her ePHI. Kettering Health had learned that Sheldon's ePHI had been accessed on several occasions by her (now former) husband, an employee of Kettering Health. Sheldon alleged that her former husband began an affair with a fellow employee and together they accessed her ePHI in furtherance of the affair.

Sheldon's allegation that Kettering Health falsely certified its compliance with the HITECH Act were premised on two conclusions: (1) that the individual breaches constituted violations of the HITECH Act in themselves or suggested that Kettering Health failed to implement security policies and procedures; and (2) that Kettering Health's failure to run "CLARITY reports" (a particular type of comprehensive reports Kettering Health used to monitor improper access to ePHI) on a regular basis constituted a breach of its duties under the HITECH Act. The Sixth Circuit affirmed the dismissal of the action because these two conclusions were either facially implausible or based on incorrect conclusions of law.

The Sixth Circuit agreed with Kettering Health's argument that the HITECH Act regulations do not impose a strict liability standard that requires hospitals to prevent all privacy breaches. Therefore, Kettering Health's admission that Sheldon's ePHI was improperly accessed could not, by itself, render "false" any of its attestations of HITECH Act compliance. The Sixth Circuit rejected Sheldon's argument that the individual breaches taken together indicated having no policies and procedures in place because there were no facts to support this claim. Indeed, Kettering Health stated in its letter to Sheldon that the access of her ePHI was inappropriate/unauthorized and in violation of its policy and procedure, that it conducted an investigation into the matter, and was notifying HHS of the breach. The Sixth Circuit ruled that Sheldon having received the letters indicated that Kettering Health had *some* procedure in place for detecting unauthorized access to ePHI, investigating such access, and notifying patients whose information was breached. Accordingly, the Sixth Circuit affirmed that Realtor's allegations that Kettering Health lacked the requisite policies and procedures was not facially plausible.

Finally, with respect to Realtor's claim that Kettering Health failed to run CLARITY reports constituting a breach under its duties under the HITECH Act, the Sixth Circuit affirmed that "the HITECH Act requires hospitals to implement a system to protect ePHI; it does not require covered entities to use a particular ePHI product or vendor to run a specific type of monitoring report." Accordingly, because Realtor's claim of false attestation of the HITECT Act was based on implausible inferences and incorrect conclusions of law, the Sixth Circuit held that Realtor failed to adequately plead the "false statement" element of her FCA claim.

Oregon District Court rules that multiple claims survive pleading stage in class action healthcare data breach case

On March 17, 2015, Premera Blue Cross publically disclosed that its computer network had been breached compromising the confidential information, including PHI, of approximately 11 million current and former members and employees. A consolidated class action ensued – In re Premera Blue Cross Customer Data Sec. Breach Litigation, Case No. 3:15-md-2633-SI (D. Or.). According to plaintiffs, the breach began in May 2014 and went undetected for almost one year. After discovering the breach, plaintiffs further allege that Premera waited several months before notifying those affected. Based on these allegations, plaintiffs claim to have been damaged and brought various common law and state statutory claims. Premera moved to dismiss several of plaintiffs' claims.

In August 2016,[39] the Oregon District Court denied Premera's motion to dismiss in part holding that plaintiffs sufficiently pled the following claims to withstand a motion to dismiss:

(1) *Restitution/Unjust Enrichment*;

Plaintiffs claim that they conferred a monetary benefit on Premera in the form of fees paid for healthcare insurance, that a portion of those fees were supposed to be used by Premera, in part, to pay for the administrative costs of data management and security, that Premera did not use such fees to pay for the administrative costs of data management and security, and that as a result of Premera's conduct, plaintiffs suffered actual damages in the amount equal to the difference in the free-market value of the secure healthcare insurance for which they paid and the insecure healthcare insurance they received, and that it was unjust for Premera to retain the benefits received.

(2) *Violation of California's Confidentiality of Medical Information Act (CMIA)*; and

CMIA prohibits entities from negligently disclosing or releasing any person's confidential medical information.

(3) *Violations of state data breach notification laws due to the alleged unreasonable delay in notification of the breach*.

The district court also granted Premera's motion to dismiss in part, but the ruling appears to be of little benefit because the district court also granted plaintiffs leave to file a second consolidated class action complaint in order to cure the deficiencies of the following improperly pled claims: (1) fraud through affirmative misrepresentation; (2) fraud through active concealment; (3) fraud through omission; (4) breach of express contract; and (5) breach of implied contract.

The only claim that the district court dismissed outright was plaintiffs' breach of fiduciary duty claim ruling that no fiduciary relationship had been established.

Fourth Circuit affirms insurer's duty to defend healthcare insured in cyber breach class action lawsuit under general liability insurance policies

In Travelers Indem. Co. of America v. Portal Healthcare Solutions, LLC, 644 Fed. Appx. 245 (4th Cir. 2016), a decision with far reaching implications for all healthcare insurers, the Fourth Circuit Court of Appeals affirmed the lower court's decision directing The Travelers Indemnity Company of America (Travelers) to defend its insured, Portal Healthcare Solutions, LLC (Portal), against a civil class action lawsuit pending in New York State Court under comprehensive general liability (CGL) policies.

In April 2013, a class-action complaint was filed in New York against Portal alleging that for over four months between November 2012 and March 2013, Portal and others engaged in conduct that resulted in patients' private medical records being on the internet. The class-action complaint alleged causes of action for negligence, breach of warranties, and breach of contract. During the time period at issue, Portal was insured under Travelers' CGL policies.

Travelers filed a lawsuit against Portal in the Eastern District of Virginia in July 2013 seeking a declaration that it was not obligated to defend Portal in the class-action lawsuit because the complaint failed to allege a covered "publication" by Portal. In July 2014, the district court ruled that Travelers was duty bound to defend Portal under the CGL policies; Travelers appealed.

In deciding the declaratory action on appeal, the Fourth Circuit was bound by Virginia's "Eight Corners' Rule," which required the court to look at the four corners of both the class-action complaint and the underlying insurance policies to determine whether Travelers was obligated to defend Portal.

Applying this Virginia rule, the Fourth Circuit affirmed that the class-action complaint at least potentially or arguably alleged a "publication" of private medical information by Portal triggering coverage under the policies. Such conduct, if proven, gave unreasonable publicity to, and disclosed information about, the patients' private lives because anyone with internet access could have viewed the patients' medical records during the four month period the records were available online.

In affirming the district court's holding that Travelers has a duty to defend Portal against the class-action lawsuit, the Fourth Circuit explicitly noted that under Virginia law, an insurer's duty to defend an insured is broader than its obligation to pay or indemnify an insured. Virginia law further provides that the insurer must use language clear enough to avoid ambiguity if there are particular types of coverage that it does not want to provide.

Although the Fourth Circuit ruled in favor of Portal with respect to Travelers' duty to defend it in the class action lawsuit, healthcare insureds must carefully review their insurance policies to determine whether cyber breach claims are covered. It is recommended that healthcare insureds maintain separate cyber insurance policies to explicitly cover these types of claims because as the Fourth Circuit highlighted, even though Travelers' has a duty to defend, it may not have a duty to pay or indemnify.

Hot Topics

Ransomware

Ransomware, as defined by the FBI, is "a type of malicious software cyber actors use to deny access to systems or data. The malicious cyber actor holds systems or data hostage until the ransom is paid. After the initial infection, the ransomware attempts to spread to shared storage drives and other accessible systems. If the demands are not met, the system or encrypted data remains unavailable, or data may be deleted."[40]

Over the past year, there has been an alarming increase in the number of ransomware attacks. According to a U.S. government interagency report, since early 2016 there are 4,000 daily ransomware attacks on average.[41] This is a 300% increase since 2015 and represents the fastest growing malware threat. Criminals prefer bitcoin as ransom because it is an anonymously traded digital currency.

Ransomware Extortion Hits Hollywood Presbyterian Medical Center

Ransomware garnered national attention in February 2016, when hackers used malware to infect Hollywood Presbyterian Medical Center and seize control of its computers.[42] Hospital staff was unable to access the system and resorted to paper record keeping. The hackers demanded 40 bitcoin (approximately $17,000) in exchange for a decryption key to regain access to the computer systems. Although the FBI does not encourage paying a ransom, the hospital determined that in the best interest of restoring normal operations, it paid the ransom to bring its system back online. The hospital alerted authorities and was able to regain control of its computer systems with the assistance of technology experts.

Since the Hollywood Presbyterian incident, a number of other hospitals have been hit with ransomware attacks.[43] The risk of a ransomware attack is of utmost concern for patient safety because the blackout of a hospital's computer system puts patient lives in peril.

Guidance from the OCR

In order to help health care entities better understand and respond to the threat of ransomware, in July 2016, OCR released new HIPAA guidance on ransomware.[44] The guidance describes the role HIPAA has in assisting covered entities and business associates from preventing and recovering from ransomware attacks; how HIPAA breach notification processes should be managed in response to a ransomware attack; and how a ransomware attack can be detected.

- **How compliance with the HIPAA Security Rule can help prevent infections of malware, including ransomware**

OCR highlighted the following required measures under the HIPAA Security Rule as some of the ways to help prevent the introduction of malware, including ransomware:

  - Implementing a security management process, which includes conducting a risk analysis to identify threats and vulnerabilities to ePHI and implementing security measures to mitigate or remediate those identified risks;
  - Implementing procedures to guard against and detect malicious software;
  - Training users on malicious software protection so they can assist in detecting malicious software and know how to report such detections; and
  - Implementing access controls to limit access to ePHI to only those persons or software programs requiring access.

- **How compliance with the HIPAA Security Rule can help recover from infections of malware, including ransomware**

In order to effectively recover from infections of malware, the HIPAA Security Rule requires covered entities and business associates to implement a data backup plan as part of maintaining an overall contingency plan.[45] Maintaining frequent backups and ensuring the ability to recover data from backups is crucial to recovering from a ransomware attack that denies access to data. Test restorations should be periodically conducted to verify the integrity of backed up data and provide confidence in restoration capabilities.

The HIPAA Security Rule also requires security incident procedures, including procedures for responding to and reporting ransomware attacks. Robust security incident procedures should include processes to:

  - Detect and conduct an initial analysis of the ransomware;
  - Contain the impact and propagation of the ransomware;
  - Eradicate the instances of ransomware and mitigate or remediate vulnerabilities that permitted the ransomware attack;
  - Recover from the ransomware attack by restoring data lost during the attack and returning to business as usual operations; and
  - Conduct post-incident activities, which could include a deeper analysis of the evidence to determine if the entity has any regulatory, contractual or other obligations as a result of the incident, and incorporating any lessons learned into the overall security management process of the entity to improve incident response effectiveness for future security incidents.

- **How to detect a ransomware attack**

Typically an entity is alerted to the presence of ransomware only after the ransomware has encrypted the user's data and alerted the user to its presence and demands payment. In some cases, however, an entity may notice early indications of a ransomware attack, such as:

- A user's realization that a link that was clicked on, a file attachment opened, or a website visited may have been malicious in nature;
- An increase in activity in the central processing unit of a computer and disk activity for no apparent reason;
- An inability to access certain files as the ransomware encrypts, deletes and re-names and/or re-locates data; or
- Detection of suspicious network communications between the ransomware and the attackers' command and control server(s).

HIPAA's requirement that an entity's workforce receive appropriate security training can assist entities in preparing their staff to detect and respond to ransomware. If the entity believes a ransomware attack is underway, the entity should immediately activate its security incident response plan and contact its local FBI or U.S. Secret Service field office.

The presence of ransomware on a covered entity or business associate's computer systems is a security incident under the HIPAA Security Rule.[46] Once the ransomware is detected, security incident and response and reporting procedures must be initiated.[47] A covered entity or business associate must also make a fact-specific determination whether the presence of ransomware was "a breach" under the HIPAA Rules.[48]

Cybersecurity of Postmarket Medical Devices

In October 2016, Johnson & Johnson warned that one of its insulin pumps was vulnerable to cyber hacking.[49] Although the risk was considered low, the company warned that a hacker could exploit the insulin pump and overdose a diabetic patient with insulin. The pump had a wireless remote control that patients could use to activate a dose of insulin. A systems vulnerability was detected because the communication between the remote control and the insulin pump was not encrypted to prevent hackers from gaining access to the device.

FDA's Guidance for Postmarket Management of Cybersecurity in Medical Devices

On December 27, 2016, the Food and Drug Administration (FDA) issued guidance on the agency's recommendations for managing postmarket cybersecurity vulnerabilities for marketed and distributed medical devices.[50] As seen in the example of the Johnson & Johnson insulin pump, networked medical devices designed to facilitate patient care can be vulnerable to cybersecurity threats and risk patient safety. Effective cybersecurity risk management is intended to reduce the risk to patients by decreasing the likelihood that device functionality is intentionally or unintentionally compromised by inadequate cybersecurity.

Because cybersecurity risks to medical devices are continually evolving, the FDA acknowledged that it is not possible to completely mitigate risks through premarket controls alone. Therefore, the FDA's guidance emphasizes that manufacturers should monitor, identify, and address cybersecurity vulnerabilities and exploits as part of their postmarket management of medical devices. Cybersecurity risk management programs should emphasize addressing vulnerabilities that may permit the unauthorized access, modification, misuse or denial of use, or the unauthorized use of information that is stored, accessed, or transferred from a medical device to an external recipient, and may result in patient harm. A key purpose of conducting the cyber-vulnerability risk assessment is to evaluate whether the risk of patient harm is controlled (acceptable) or uncontrolled (unacceptable).

Manufacturers should respond in a timely fashion to address identified vulnerabilities. Manufacturers should also have a process for assessing the severity of patient harm if the cybersecurity vulnerability were to be exploited.

The guidance further establishes a risk-based framework for assessing when changes to medical devices for cybersecurity vulnerabilities require reporting to the FDA and outlines circumstances in which the FDA does not intend to enforce reporting requirements. The FDA requires notification from medical device manufacturers for a small subset of actions taken by manufacturers to correct device cybersecurity vulnerabilities and exploits that may pose a risk to health.

Conclusion

The healthcare industry continues to take advantage of advances in technology in order to improve patient care. But these technological advances do not come without risk to the security and integrity of patient's health information and the medical devices themselves. As required under the HIPAA Rules, healthcare providers and their business associates must maintain a robust and ever-evolving cyber security plan.

In 2017, healthcare providers and insurers will continue to face challenges related to cyber attacks, the loss and theft of devices containing ePHI, protecting the cyber security of medical devices, and preparing for and defending against malware attacks, including ransomware.

With 2017 underway, we believe it is imperative for all those involved in the healthcare industry to become aware of the risks their organization may face, as well as the consequences of that risk, in those areas in which ePHI and cyber security matters are involved. One can begin this process by performing a risk assessment survey within your organization in order to identify specific areas of potential vulnerability. Organizational risk assessments should be ongoing, should take into consideration the changing needs of your particular organization, including software and computer programs, and there should be a process in place to prioritize the risks identified. Once the risks with respect to these vulnerabilities have been identified, plans can be put into place to mitigate these risks.

Our goal at Kaufman Borgeest & Ryan, LLP is to assist our clients with identifying and mitigating their cyber security risks, and to partner with them to develop plans and strategies to educate their employees and business associates as to how to manage the risks and vulnerabilities identified.

[1] Adoption of Electronic Health Record Systems among U.S. Non-Federal Acute Care Hospitals: 2008-2015. ONC Data Brief 35 (May, 2016) https://dashboard.healthit.gov/evaluations/data-briefs/non-federal-acute-care-hospital-ehr-adoption-2008-2015.php#summary (December 28, 2016).

[2] NetDiligence 2016 Cyber Claims Study.

[3] Electronic Health Information: HHS Needs to Strengthen Security and Privacy Guidance and Oversight. GAO-16-771 (August 26, 2016); http://www.gao.gov/products/GAO-16-771 (December 28, 2016).

[4] Pub. L. No. 104-191, 110 Stat. 1936 (1996).

[5] Pub. L. No. 111-5, 123 Stat. 115 (2009).

[6] 45 CFR §160.103.

[7] Id.

[8] 45 CFR §§160 and 164, Subparts A and E.

[9] 45 CFR §§160 and 164, Subparts A and C.

[10] 45 CFR §§164.400-414.

[11] HIPAA provides for three exceptions to the definition of "breach." See 45 CFR §164.402(2).

[12] 45 CFR §160, Subparts C, D, and E.

[13] https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html

[14] Id.

[15] https://www.hhs.gov/about/news/2016/02/03/administrative-law-judge-rules-favor-ocr-enforcement-requiring-lincare-inc-pay-penalties.html

[16] https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html

[17] 42 U.S.C. §1320d-5(d).

[18] CISA, Sec. 405(d)(1)(A)-(F).

[19] https://www.phe.gov/Preparedness/planning/CyberTF/Pages/default.aspx

[20] https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf

[21] 16 CFR Part 318.

[22] Bill No. A10475A (May 27, 2016).

[23] See https://its.ny.gov/eiso/breach-notification

[24] https://www.hhs.gov/about/news/2016/03/16/155-million-settlement-underscores-importance-executing-hipaa-business-associate-agreements.html

[25] https://www.hhs.gov/about/news/2016/03/17/improper-disclosure-research-participants-protected-health-information-results-in-hipaa-settlement.html

[26] https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/raleigh-orthopaedic-clinic-bulletin/index.html

[27] https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/catholic-health-care-services/index.html

[28] https://www.hhs.gov/about/news/2016/07/18/widespread-hipaa-vulnerabilities-result-in-settlement-with-oregon-health-science-university.html

[29] https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/UMMC/index.html

[30] https://www.hhs.gov/about/news/2016/08/04/advocate-health-care-settles-potential-hipaa-penalties-555-million.html

[31] https://www.hhs.gov/about/news/2016/09/23/hipaa-settlement-illustrates-importance-of-reviewing-updating-business-associate-agreements.html

[32] https://www.hhs.gov/about/news/2016/10/18/214-million-hipaa-settlement-underscores-importance-managing-security-risk.html

[33] https://www.hhs.gov/about/news/2016/11/22/umass-settles-potential-hipaa-violations-following-malware-infection.html

[34] 42 U.S.C. §1320d-5(d).

[35] Attorney Gen v. Health Net of NE Inc., et al., Civ. No. 3:2010CV-00057(PCD).

[36] http://www.ct.gov/ag/cwp/view.asp?Q=573262&A=2341

[37] http://www.ag.ny.gov/pdfs/URMC_Letter_Agreement_Fully_Executed_11_30_2015.pdf

[38] http://www.ag.ny.gov/press-release/ag-schneiderman-announces-settlement-university-rochester-prevent-future-patient

[39] 2016 U.S. Dist. LEXIS 100198 (Aug. 1, 2016).

[40] FBI's Ransomware Prevention and Response for CEOs (2016).

[41] https://www.justice.gov/criminal-ccips/file/872771/download

[42] http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html

[43] http://www.nbcnews.com/tech/security/big-paydays-force-hospitals-prepare-ransomware-attacks-n557176

[44] https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

[45] See 45 CFR 164.308(a)(7).

[46] See 45 CFR 164.304.

[47] See 45 CFR 164.308(a)(6).

[48] See 45 CFR 160.103 and 45 CFR 164.402.

[49] http://www.reuters.com/article/us-johnson-johnson-cyber-insulin-pumps-e-idUSKCN12411L

[50] http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf