Union Internationale des Avocats
International Association of Lawyers
Unión Internacional de Abogados

59th UIA CONGRESS

Valencia / Spain
October 28 – November 1, 2015

Insurance Law/Biotechnology Law
Health Law/Tort Law

Thursday, October 29, 2015

HOW WOULD YOU LIKE YOUR PACEMAKER TO BE HACKED?
Healthcare Cyber Vulnerability: A Risk Management Nightmare for the 21st Century

Janice F. Mulligan
MULLIGAN & BANHAM & FINDLEY
San Diego, California USA
www.janmulligan.com
001.619.238.8700
mulligan@janmulligan.com[1]

© UIA 2015

1 **Janice F. Mulligan** is also a clinical professor at the University of California San Diego School of Medicine. Research assistants: **Amy Marks**, J.D. Candidate 2017 University of San Diego School of Law, **Sabrina Gonzales**, J.D. Candidate 2017 Thomas Jefferson School of Law, San Diego, California USA, **Vanessa L. Berger**, M.A. London, England, U.K.

I. INTRODUCTION

A recent *conservative* study found that close to *a thousand large data breaches affected 29 million U.S. medical records between 2010 and 2013*.[2] Data and identity theft threaten not only privacy and financial security, but also pose an even greater threat to patient safety. [3] Both U.S. government and private industry studies establish that medical devices[4] in hospitals are *routinely* riddled with malware (software that is intended to damage or disable computers), which often goes undetected for several months or longer.[5]

Such software infections can wreak havoc. Researchers established that life-saving medical devices such as heart monitors and insulin pumps have been hacked and malware installed with the potential to remotely control the devices.[6] While patient deaths associated with cyber-attacks have yet to be reported, such cyber-attacks have the potential to flood a patient with a deadly dose of insulin or kill a patient with an electric charge aimed directly at the pacemaker in his heart. If these risks sound like science fiction, consider that when U.S. politician Dick Cheney was Vice President, he had the wireless function on his pacemaker disconnected because of concerns that hackers might try to kill him by remotely interfering with his device.[7]

Isolated medical devices and patient records aren't the only target: Hospital networks are also vulnerable to being ***completely shut down*** by cyber-attacks.[8]

Why is health care targeted? One reason is that health care insurance information yields a value twenty times greater *or more* than a credit card on the hacker black market.[9] Experian estimates that the potential cost of breaches for the healthcare industry worldwide could be as much as $5.6 billion *annually*.[10] Large-scale breaches are virtually certain to continue because health care is becoming more dependent on technology that is vulnerable to being hacked.

Another reason healthcare is targeted is that unlike the layers of security shrouding regular corporate IT networks, there are typically few, if any, independent cyber-defense products operating on most medical devices. While the medical devices are generally installed "behind the firewall" of hospital security systems, once a firewall is breached, there are few diagnostic cybersecurity tools providing additional protection. This is typically because most U.S. healthcare and security teams view medical devices as inaccessible operating

---

[2] *Data Breaches of Protected Health Information in the United States* by Vincent Liu, MD. Other studies show the number may be as high as over 99 million records exposed in the U.S. alone in just the year 2015. *Anatomy of an Attack: MEDJACK [Medical Device Hijack]*. http://deceive.trapx.com/rs/929-JEW-675/images/AOA_Report_TrapX_AnatomyOfAttack-MEDJACK.pdf?aliId=85489 (last viewed September 13,2015)

[3] *Cybersecurity in Health Care* by Eric D. Perakslis, The New England Journal of Medicine.

[4] What is a medical device? Any item used to diagnose, prevent, or treat conditions that are *not* a drug. The FDA has ruled that medical device regulation includes "software, electronic and electrical hardware, including wireless". See US Food and Drug Administration [homepage on the Internet] MDDS Rule.FDA Federal Register; 2011. (76 FR 8637). http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/GeneralHospitalDevicesandSupplies/MedicalDeviceDataSystems/ucm251897.htm. (last viewed September 14,2015)

[5] *Computer Viruses Are "Rampant" on Medical Devices in Hospitals: A meeting of government officials reveals that medical equipment is becoming riddled with malware* by David Talbot, MIT Technology Review. (last viewed September 13,2015) http://www.technologyreview.com/news/429616/computer-viruses-are-rampant-on-medical-devices-in-hospitals/

[6] C*ybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem* by Patricia A. Williams and Andrew J. Woodward. http://www.ncbi.nlm.nih.gov/pmc/articles/PMC4516335/#b6-mder-8-305 (last viewed September 13,2015)

[7] *Cheney's Defibrillator was Modified to Prevent Hacking* by Dana Ford October 24, 2013 http://www.cnn.com/2013/10/20/us/dick-cheney-gupta-interview/ (last viewed September 12,2015)

[8] *Hospital Medical Devices Used as Weapons in Cyber—attacks,* by Kelly J. Higgins, DARK Reading. http://www.darkreading.com/vulnerabilities---threats/hospital-medical-devices-used-as-weapons-in-cyber--attacks/d/d-id/1320751 (last viewed September 4, 2015)

[9] *Anatomy of an Attack: MEDJACK [Medical Device Hijack]* by TrapX Labs, A division of TrapX Security. http://deceive.trapx.com/rs/929-JEW-675/images/AOA_Report_TrapX_AnatomyOfAttack-MEDJACK.pdf?aliId=85489

[10] *Data Breach Industry Forecast,* 2015. http://www.experian.com/assets/data-breach/white-papers/2015-industry-forecast-experian.pdf (last viewed September 13,2015)

systems. Medical devices used in the United States are designed to be turnkey systems that require approval by the U.S. Federal Drug Administration (FDA). Hospital risk managers fear that tampering with an FDA approved medical devices, even to install cybersecurity software, may increase hospital liability if the device malfunctions. Often the devices are maintained only by the device manufacturer's own external technicians who have limited access to the devices. [11]

Another reason healthcare is targeted is that many mobile devices used to transmit and save patient records are not encrypted and do not have the ability to be "wiped" remotely if they are lost or stolen. Medical devices existed long before the internet, and most were originally designed to stand alone, yet we are now in an environment where 90% of healthcare professionals use personal smart phones for work and expect to be able to be remotely connected to all available health care data.[12] With so many mobile devices containing data lacking encryption and incapable of being wiped remotely, loss of even a single device can be a recipe for disaster if it falls into the wrong hands. At least one study shows that hacking only accounts for 23% of healthcare data breaches. ***Loss or theft of employee mobile devices with information on them accounts for 68% of all breaches since 2010***.[13]

This paper looks at the trends in healthcare cyber vulnerability, the flaws in American law available to protect patient's safety and privacy, and risk management recommendations as to what can and should be done to deter twenty-first century cybersecurity losses in healthcare systems. While this paper focuses on U.S. law, the problems described are universal whenever modern technology is used in the delivery of healthcare. Data protection and privacy are fundamental rights attributed to all individuals, irrespective of nationality or residence. The need for international standards and safeguards for collecting and processing personal data are paramount.

II. MODERN HEALTHCARE IS GROWING INCREASINGLY RELIANT ON SYSTEMS THAT CAN BE HACKED

Few would deny the amazing benefits available because of technological advances in modern medicine. On the upswing are health care providers use of such technology for consulting, diagnosing, and treating patients. While this offers a variety of lifesaving treatment options that are simply unavailable without technology, it also opens the door to increasing risk of cyber vulnerability.

There are two main trends in American healthcare that pose increasing risks to patient safety and security: First, technological devices are increasing in use at every step of the delivery of healthcare services; and, Two, there is a widespread adoption of Health Information Technology (HIT) to put all patient health records (PRH), electronic health records (EHR) and electronic medical records (EMR) online and to make this information readily available to more people. [14]

---

[11] *Id.,* p.9

[12] *Mobile Devices and Apps for Health Care Professionals: Uses and Benefits* by C.Lee Ventola, MS, Journal of Pharmacy and Therapeutics. http://www.ncbi.nlm.nih.gov/pmc/articles/PMC4029126/ (last viewed September 13,2015)

[13] *Bitglass Healthcare Breach Report: Is Your Data Security Due For a Physical?* The Bitglass Report. http://pages.bitglass.com/rs/bitglass/images/WP-Healthcare-Report-2014.pdf (last viewed September 13,2015)

[14] **Health information technology (HIT) is information technology applied to health care.** It provides the umbrella framework to describe the comprehensive management of health information across computerized systems and its secure exchange between consumers, providers, government and quality entities, and insurers. Electronic medical records (EMR) and electronic health records (EHR), Patient Health Records (PRH) are just a few of the terms becoming commonplace in American health systems. Electronic medical records (**EMRs) are *digital versions of the paper charts* in clinician offices, clinics, and hospitals.** EMRs contain notes and information collected by and for the clinicians in that office, clinic, or hospital and are mostly used by providers for diagnosis and treatment. **Electronic health records (EHRs) go beyond standard clinical data collected in a provider's office and are inclusive of a broader view of a patient's care.** EHRs contain information from *all the clinicians involved in a patient's care* and all authorized clinicians involved in a patient's care can access the information to provide care to that patient. EHRs also share information with other health care providers, such as laboratories and specialists. EHRs follow patients – to the specialist, the hospital, the nursing home, or even across the country. **Personal health records (PHRs)** contain the same types of information as EHRs—diagnoses, medications, immunizations, family medical histories, and provider contact information—but are designed to be set up, accessed, and ***managed by patients***. Patients can use PHRs to maintain and manage their health information in a private, secure, and confidential environment. PHRs can

A. More electronic devices are being used for every step of healthcare delivery

Many medical devices contain configurable embedded computer systems and they are increasingly interconnected with other devices, the internet and/or hospital networks. ***Any medical device with internet connectivity is vulnerable to cyberattack***,[15] including diagnostic equipment (such as CT and MRI machines), therapeutic equipment (such as infusion pumps and medical lasers) and life support equipment (ventilation, heart-lung machines and dialysis equipment) and much more.

Aside from the medical devices themselves, modern medicine also includes a growing variety of other interconnected applications and electronic devices using two-way video conferencing, email, smart phones and other forms of telecommunications technology to deliver healthcare services. With increasing frequency, telemedicine services are used with the patient in one place and the health care provider physically at another, distant location. [16] Such telemedicine services include real-time video, store and forward, and home monitoring[17], all of which are vulnerable to being hacked. Real-time video telemedicine involves a patient and his practitioner interacting with a remote specialist via video-conferencing or other real-time technology. "Store and forward" involves the transmission of medical or health information, such as an x-ray, lab results, or prescriptions, from one provider to another for a consultation or interpretation. Additionally, home monitoring telemedicine includes the ability to monitor one's health status by capturing data through a medical device in the patient's home, and then transmitting it to a provider via the internet.

There are already over 200 telemedicine networks and nearly 3,500 service sites in the United States[18] and the number is set to skyrocket. In a recent annual survey, the National Business Group on Health found that 74% of large American employers plan to offer telemedicine services in 2016.[19] This promises to cause a rapid increase in such remote services. In addition, over half of all United States hospitals now use some form of telemedicine and the trend is on the rise.

1. Cyber Vulnerable Medical Devices are Ridden With Infected Software

Medical devices are vulnerable to unauthorized access configuration settings affecting how a medical device operates as well as wholesale breach of confidential patient data. Often, hospitals and other providers are unaware that the malware is even operating in their systems because the medical devices are "closed" devices behind firewalls managed by the manufacturer of the device to which the medical provider doesn't have access. [20]

While many U.S. government organizations play a role in medical device regulation, the FDA is the main regulator. In 2013, the FDA issued "draft guidance" in which it identified cybersecurity vulnerabilities that could directly impact medical device and /or hospital network operations including: [21]

---

include information from a variety of sources including clinicians, home monitoring devices, and patients themselves. See HealtHit, 2014, *What are the differences between electronic medical records, electronic health records, and personal health records?* http://www.healthit.gov/providers-professionals/faqs/what-are-differences-between-electronic-medical-records-electronic (last viewed September 5, 2015)

[15] *Supra*, TrapX p 11

[16] Medical technology is moving at such a fast pace in the United States that there aren't even universally accepted names yet for all of the recent developments: While **telemedicine** often refers specifically to remote clinical services **telehealth** is often broader in scope and also includes remote non-clinical services and electronic medical records,. ***Often times, these two terms and the vague term E-health, are used interchangeably.***

[17] *Telehealth,* U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES. (Mar. 2015), https://healthit.ahrq.gov/key-topics/telehealth. (last viewed September 1 2015)

[18] *Telemedicine Practice,* AMERICAN TELEMEDICINE ASSOCIATION. (2012), http://www.americantelemed.org/about-telemedicine/faqs#.VdOiC2C4mu0. (last viewed September 1,2015)

[19] *Coming soon to a screen near you: Doctors* by Beth Pinsker, Reuters**.** http://www.reuters.com/article/2015/08/12/us-usa-health-telemedicine-idUSKCN0QH1S820150812 (last viewed September 1, 2015)

[20] *Supra,* Trap X, p 12

[21] *Cybersecurity for Medical Devices and Hospital Networks: FDA Safety Communication.* June 13, 2013. http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm (last viewed September 1,2015)

- Network connected or configured medical devices infected or disabled by malware**.**
- The presence of malware to access patient data, monitoring systems and implanted patient devices on hospital computers, smart phones and other mobile devices using wireless technology.
- Uncontrolled distribution of passwords, disabled passwords intended for limited access.
- Failure to provide timely security software updates to medical devices and networks.
- Security risks in off-the-shelf software that have only plain text without encryption, required no authentication and or weak or absent password requirements.

The FDA draft guidance instructs device manufacturers to conduct a "risk analysis" of software, including both unintentional and intentional security threats. Despite this guidance, the FDA has yet to develop an enforceable systemic software policy designed to prevent new cyber-attacks. Nor has this or any other U.S. governmental agency implemented incentives to encourage the medical device manufacturers to develop innovative security for medical devices.

2. Mobile Medical Apps, Big Data and Risks of Re-Identification

Many modern medical devices collect sensitive health data and use it aggregately for "research"(commonly referred to as "big data".) Additionally, outside of healthcare, Fitbit, Apple watch and scores of other mobile apps also collect a mass of consumer personal data and make recommendations about exercise and activity levels. Much of this big data information, both from medical devices and consumer mobile apps, *provides near identical information available for the bidding.*

Both medical devices and mobile health apps are in some ways the Wild West of big data collection, with uncertainty as to what data is allowed to be sold and what is impermissible. There isn't even a clear division as to which U.S. government agency is primarily in charge of regulating such data.

While the apps privacy policies typically provide that the individual's data is collected and used in the aggregate for marketing purposes, *nothing is said about how easy it may be to relate the big data back to an individual user.* It turns out that it is not that difficult at all- it is in fact surprisingly easy for individuals to be identified from metadata collected about them. [22]

The big data generated by these devices is at risk of being used for purposes unpredicted by the consumer. For example, how much would a life insurance company pay to know the actual daily activity level and vital signs of an individual wearing one of these devices before a new life insurance policy is issued?

In January 2015 the FDA released draft guidance on general wellness mobile apps and devices saying it would regulate devices on a "discretionary basis."[23] The FDA's guidelines red-flag health apps that attempt to practice medicine (such as diagnosing, psychiatric conditions or making treatment recommendations for specialized treatment), allowing the majority of other app-makers to cut costs and avoid the long process for FDA approval.

In this grey area, the future is uncertain because the FDA is not the only U.S. government agency with authority to regulate these wellness apps. While companies may have to go to the FDA to make sure they're following rules, they may later be on the receiving end of an injunction from the Federal Trade Commission (FTC) or a lawsuit from the Centers for Medicare & Medicaid Services (CMS) if it finds the apps are misleading or are inappropriately collecting consumer data. In at least one instance, the CMS prosecuted and settled with a medical billing provider for deceptively collecting patient information. [24]

---

[22] *Privacy Challenges Analysis: It's surprisingly easy to identify individuals from credit-card metadata* by Harry Hardesty, MIT News Office. http://newsoffice.mit.edu/2015/identify-from-credit-card-metadata-0129 (last visited August 23, 2015)

[23] *General Wellness: Policy for Low Risk Devices Draft Guidance for Industry and Food and Drug Administration Staff* issued January 20, 2015. http://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm429674.pdf (last visited August 20, 2015)

[24] *Medical Billing Provider and its Former CEO Settle FTC Charges That They Misled Consumers* About *Collection of Personal Health Data Respondents Failed to Inform Consumers They Would Seek Detailed Info From Pharmacies,*

B. Rise in Electronic Health Information Such as EHR/EMR Cause a Proliferation of Sensitive Data Stored Online

Internet connected systems and medical devices described above are often also connected to the EMR/EHR being implemented at a fast pace across the United States because of government financial incentives. [25] With the boom in EHR/EMR comes the proliferation of information stored online and available to more people.
This creates a highly connected community bringing some of the *most vulnerable devices* together with some of the *highest value data.*

Changes in technology create both different formats and types of data that never used to be part of a patient's record. More information than ever before is now maintained about individual patients, including audio recordings, videos, and remote monitoring data (such as printouts of heart rates and/or glucose readings taken from a home monitoring system).

Additional information never even conceived of in generations past includes personal genetic test results. Whether to even keep this genetic data with the patient's health record and how to secure it from prying eyes creates an additional risk of privacy breach not only for the patient but also for *all of the patient's family members* since the implications of genetic test results are far reaching and have consequences to members of the family tree far afield from the patient who is tested.

With traditional documentation of an examination, the practitioner has discretion to selectively record findings. With telemedicine, however, the entire session may be memorialized and become part of a patient's record.
This leaves the practitioner with less discretion to remove sensitive information that might otherwise not have been recorded. In California, a telemedicine session involving patients may be recorded only if specific conditions have been satisfied.[26] However, the guidelines are not uniform and not all U.S. states even have such a telemedicine act in place.

With the ease of purchasing prescription drugs online, the opportunity to Skype with physicians, and the requirement of additional non-medical technical teams to facilitate the medical technology, the concept of patient privacy grows more vulnerable. Because telemedicine is based on the use of technology, more staff members must be included in maintaining such health care services. This presents privacy and security challenges by increasing the number of people with potential access to patient records.[27] There is a need for data confidentiality in regards to transmission and retention, and data integrity is also a key concern to ensure correct diagnosis and quality of care.

It is anticipated that *the number of EHR/EMR breaches will likely expand* as the move to pool and share more patient data increases. For example, two of the United States' largest health insurers are currently creating the California Integrated Data Exchange, a statewide health information bank [28], with a vast database comprised of *all patient information available to all providers throughout the state*. Although there are some privacy safeguards,[29] they are so general that they may easily become void. The Exchange seeks to automatically enroll all patients in this exchange, leaving unwilling patients to affirmatively take steps to dis-enroll.

III. EXISTING U.S. LAW IS ILL-EQUIPPED TO HANDLE HEALTHCARE CYBER VULNERABILITY

Insurance Companies and Laboratories, December 2014 https://www.ftc.gov/news-events/press-releases/2014/12/medical-billing-provider-its-former-ceo-settle-ftc-charges-they (last visited September 13,2015)

[25] *The Digital Doctor: Hope, Hype, and Harm at the Dawn of Medicine's Computer Age* by Robert Wachter, p.2017, McGraw Hill.
[26] California Code of Regulations, Title 16, Div. 39, Art. 8, Sec. 4172.
[27] *Developing a Training Strategy,* 2015, TELEHEALTH RESOURCE CENTERS. http://www.telehealthresourcecenter.org/toolbox-module/developing-training-strategy. (last visited August 9, 2015)
[28] All patients are to be included in the database, subject to an affirmative "opt-out". https://www.calindex.org/ Unfortunately, in order to opt-out, the patient is required to provide additional personal information online in order to ensure their identity.

While the latest technology creates a range of opportunities within the healthcare system, it also brings to light an array of legal issues American laws are ill equipped to handle:

A. Criminal Law

U.S. federal laws include the Computer Fraud and Abuse Act (CFAA)[30] and the Federal Anti-Tampering Act,[31] both of which impose criminal liability on the individuals behind cyber-attacks. The problem with these laws is that often the people behind the attack are never identified and/or they are in countries beyond the reach of American law.

Additionally, neither of these acts extends liability to healthcare institutions or medical device manufacturers who implicitly aid and abet the cyber-attacks by failing to take precautions to prevent the occurrences from happening in the first place. As discussed above, the vast majority of cyber-problems to date have come from healthcare providers losing encrypted mobile devices which are incapable of being swiped from afar, or from systems ill-designed to prevent the installation and/or detection of malware. While this is reckless behavior, it has not yet been found to rise to the level of criminal culpability, perhaps in large part because no patient lives have yet been reported lost due to such mishaps.

B. Regulatory Law Regarding Private Health Information EMR/HER

Unfortunately, existing American laws by and large address institutional *compliance* with privacy laws rather than providing actual security and protection from cyber vulnerability. For example, the Health Insurance Portability and Accountability Act (HIPAA), provides national standards to protect the privacy of personal health information and to require safeguards to ensure confidentiality of EMR and EHR information.[32] Further, the Health Information Technology for Economic and Clinical Health Act (HITECH) was created in response to technology changes in HIPAA, with the stated goal of further improving the efficiency of electronic health record systems while protecting patient's rights.[33] The HITECH Act broadens the scope of covered entities to include additional related "business associates" (including health lawyers, insurance carriers, accountants, IT teams etc.) The Act also imposes a sliding scale liability approach from strict liability at one end to various shades of willful neglect with corresponding penalties for various HIPAA violations. This Act also requires health care providers to promptly notify both patients affected by the breach, as well as the government and the media in cases where the breach affects more than 500 people. [34][35]

There are several problems with these regulatory schemes:

The first problem with the HIPAA and HITECH Acts is that there has historically been little enforcement. There is no private right of action and government enforcement is spotty at best. While the HITECH Act empowers the U.S. Department of Justice to bring criminal cases against covered entities that knowingly violate HIPAA, this is rarely done. In addition to monetary fines, the steepest civil penalty levied is exclusion from Medicare, which is a serious penalty, but again, this too is seldom invoked.

A second problem with existing HIPAA and HITECH laws are their limited scope: They are focused solely on patient ***information***, not patient ***health***. Neither HIPAA nor the HITECH Act was designed to address disruption of medical devices or hospital networks unless they involve a breach of EMR/EHR.[36]

Third, HIPAA and HITECH laws do not focus on hackers nor on manufacturers of medical devices- instead,

---

[30] 18 U.S.C. Section 1030 (2012)
[31] 18 U.S.C. Section 1365 (2012)
[32] HIPAA; 45 C.F.R. §§160 & 164
[33] HITECH; 42 U.S.C. §§ 300jj et seq.; §§17901 et seq.
[34] 45 CFR Part 160 and Subparts A and E of Part 164, available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/index.html

[36] *Cyber-attacks on Medical Devices and Hospital Networks: Legal Gaps and Regulatory Solutions* by Katherine Booth Wellington, Santa Clara High Techl L.J. 139 (2014). http://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1578&context=chtlj (last visited September 13,2015)

they focus on the health care entities subject to being attacked. There is little in these acts to incentivize medical device manufacturers, (although devices sold to patients and billed to Medicare may possibly be covered under these laws.)[37]

One bright spot is that now that recent amendments broaden these laws to include "business associates", the U.S. Office of Civil Rights[38] takes the position that any company that transfers unencrypted health data (even temporarily) may be liable under HIPAA as a "business associate."[39] With this change, there now is a greater emphasis on the responsibility of business associates and subcontractors to protect patient privacy.

C. Civil Litigation

While health care providers and device manufacturers may attempt to defend lawsuits brought by patients on the theory that medical devices and/or EHR/EMR are *incapable of being better protected from cyberattacks*, such arguments may fall on deaf ears given the developments of built-in encryption in Apple's 2014 operating system which is represented to make it all but impossible for *anyone except the phone user* to open stored content without an authorized access code. [40] [41]

The question is what theories or causes of action may be brought by patients? The answer lies in the whether the breach is of patient health information EHR/EMR) ***or*** a medical device and in what state the patient is in when the breach occurs.[42]

1. Litigation arising out of EHR/EMR: Breach of privacy / breach of confidentiality actions

There is no consensus among the American courts as to whether there is a federal, constitutional right to privacy.[43] State laws vary widely in the right to recovery and available damages. This lack of conformity in confidentiality and privacy legislation across the United States has the potential to cause confusion swarming liability.

Many courts insist that plaintiffs demonstrate evidence of compensable harm, in addition to just increased risk of identity theft. In just one of an increasing number of examples, In 2014, most of a $4.9 billion class-action lawsuit involving the U.S. Department of Defense and its TRICARE health insurance program was dismissed

---

[37] *Privacy Basics: A Quick HIPAA Check for Medical Device Companies* Posted on August 1, 2009. http://www.mddionline.com/article/privacy-basics-quick-hipaa-check-medical-device-companies

[38] The enforcement agency for HIPPA (last visited September 13,2015)

[39] HIPAA, 45 C.F.R §§§164.502(e), 164.504(e), 164.532(d) and (e). See, http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.pdf.

[40] *Apple and Other Tech Companies Tangle With U.S. Over Data Access,* Matt Apuzzo, David E. Sanger and Michael S. Schmidt, The NY Times. http://www.nytimes.com/2015/09/08/us/politics/apple-and-other-tech-companies-tangle-with-us-over-access-to-data.html?_r=0 (last visited September 12,2015)

[41] While the Apple hardware may be impervious to hacking, the software apps and password saving keychain can and has been hacked. *Major zero-day security flaws in iOS & OS X allow theft of both Keychain and app passwords*, June 15, 2015. http://9to5mac.com/2015/06/17/major-zero-day-security-flaws-in-ios-os-x-allow-theft-of-both-keychain-and-app-passwords/ (last visited September 13,2015)

[42] One of the very few issues in telehealth law in which all fifty United States agree is that if the patient is in one state and the health provider is in a different state when the telehealth services are provided, the state the patient isphysically located in prevails for choice of law and jurisdiction. *Telemedicine: The Invisible Legal Barriers to the Health Care of the Future* by Heather A. DALEY. District Court Annals. http://lawecommons.luc.edu/cgi/viewcontent.cgi?article=1276&context=annals (last visited September 13,2015)

[43] **Nine circuits *support* a constitutional privacy right against disclosures:** *Daury v. Smith*, 842 F.2d 9, 13 (1st Cir. 1988) ;*Fadjo v. Coon*, 633 F.2d 1172, 1175 (5th Cir. 1981) ;*Norman-Bloodsaw v. Lawrence Berkeley Lab.*, 135 F.3d 1260, 1269 (9th Cir. 1998) ; *A.L.A. v. West Valley City*, 26 F.3d 989, 990 (10th Cir. 1994) ;*Doe v. City of New York*, 15 F.3d 264, 267 (2d Cir. 1994); *Harris v. Thigpen*, 941 F.2d 1495, 1513 (11th Cir. 1991) ;*United States v. Westinghouse Elec. Corp*, 638 F.2d 570, 577 (3d Cir. 1980); *Woods v. White*, 689 F. Supp. 874, 876 (W.D. Wis. 1988), aff'd, 899 F.2d 17, 17 (7th Cir. 1990) ;*Walls v. City of Petersburg*, 895 F. 2d 188, 193 (4th Cir. 1990) **One Circuit court *denies a* constitutional right of privacy for personal information**: *Doe v. Wigginton*, 21 F.3d 733, 740 (6th Cir. 1994)(AIDS info disclosed to Parole Office); **One Circuit only regards right applicable if *egregious disclosure***: *Alexander v. Peffer*, 993 F.2d 1348, 1350 (8th Cir. 1993)

for that reason. [44]

One state, California, has enacted a relatively progressive state law allowing for *recovery of attorney's fees* in addition to a statutory penalty and actual damages. The California Confidentiality of Medical Information Act (CMIA), provides that no health care provider shall disclose or release medical information regarding a patient of the provider without first obtaining authorization. It specifically provides that an individual may recover $1,000 nominal damages against any person or entity that negligently released confidential medical information. [45] *The individual does not have to show that he suffered or was threatened with actual damages in order to recover the penalty, although actual damages are also recoverable.*

To recover under CMIA, there must be essentially:

1. A disclosure of "individually identifiable information" combined with "a patient's medical history, mental or physical condition, or treatment."[46]
2. The breach must be a result of the healthcare provider's negligence. [47]
3. Plaintiffs must prove that an unauthorized person actually viewed the medical information.[48]

CMIA has been successfully used in class action litigation. Stanford Hospital and Clinics contracted with a business associate, Multi-Specia Collection Services (MSCS), to perform a revenue cycle review. Using data supplied by Stanford, MSCS generated a spreadsheet listing the names, diagnosis codes, account numbers, admission and discharge dates, and billing charges for 20,000 patients at the hospital's emergency room during a six-month period in 2009. MSCS then contracted with Corcino & Associates, LLC, to convert the data into graphics. Someone associated with Corcino posted an inquiry – *along with the data rich spreadsheet*—to a now defunct website called Student of Fortune, which allowed students to solicit paid assistance with schoolwork. The spreadsheet remained posted on the website for more than a year until it was discovered by a patient who reported it to Stanford. Stanford investigated and reported the incident as required by HIPAA, including written notice to the patients whose information had been posted. After receiving the breach notice from Stanford, one of the patients filed a $20 million class action lawsuit against Stanford, MSCS, and Corcino. She alleged violation of CMIA. The parties recently reached a $4.125.000 settlement.

---

44 *Judge Dismisses Most of Class-Action Lawsuit Over DOD Data Breach*
http://www.ihealthbeat.org/articles/2014/5/13/judge-dismisses-most-of-class-action-lawsuit-over-dod-data-breach

[45] *California Civil Code* §56.36 (b)(1)

[46] In *Eisenhower Medical Center v. Superior Court,* 226 Cal.App.4th 430 (2014), a computer was stolen containing an index of over 500,000 patients including the patient's name, medical record number, age, date of birth, and the last four digits of his or her Social Security number. Plaintiffs sought $1,000 each for negligent release of medical information in violation of the CMIA. The appellate court interpreted the definition of "medical information" as used in the CMIA to exclude demographic information, such as the information in Eisenhower Medical Center's stolen computer. **The court found that some element of information "regarding a patient's medical history, mental or physical condition, or treatment" is needed to constitute "medical information**." This definition becomes important in determining whether a breach of medical information has occurred, as well as when making intentional disclosures of this information. (Note: If the provider of health care is not a general hospital, but a provider connected to a certain disease or condition (such as a psychiatrist, oncologist, obstetrician, AIDS clinic, etc.) where revealing the fact that a patient is connected to that provider also reveals something about the patient's medical condition, then disclosure of a patient's name alone could possibly constitute the disclosure of medical information. No court has yet ruled on this point.)

[47] In *Sutter Health v. Superior Court* , 227 Cal.App.4th 1546 (2014) a thief stole a computer containing medical records of about four million patients. The plaintiffs filed an action under the CMIA seeking to represent, in a class action, all of the patients whose records were stolen, with a potential award of about $4 billion against the health care provider. **The court held that "disclosure" as used in the CMIA requires an affirmative communicative act by the provider — not merely being the victim of a theft. In addition, the court held that: No breach of confidentiality takes place until an unauthorized person views the medical information.**

[48] In *Regents of the University of California v. Superior Court*, 220 Cal.App.4th 549 (2013), a lawsuit resulted from the theft of an encrypted external hard drive containing personally-identifiable medical and financial information about approximately 16,000 patients. The encryption key had been written on an index card near the device and was also missing. Neither the hard drive nor the encryption key was recovered; there was no evidence that any unauthorized person ever viewed the information. The court found that to succeed in a CMIA lawsuit, **plaintiffs must prove that an unauthorized person actually viewed the medical information**.

2. Traditional U.S. Negligence Actions: Lawsuits for Injury/Death

While no one has yet reported a serious injury or death from a corrupted medical device, garden variety negligence principles would likely apply in lawsuits brought by harmed patients against cyber-attackers, hospitals, providers and medical device manufacturers.

While lawsuits against cyber-attackers may be challenging because of difficulty finding the attacker, and the perception that most cyber-attackers are likely to be judgment proof.

Litigation against the hospital and provider may be easier under general negligence principles, and justified, especially if the data is not encrypted and there is no remote wiping capability on all mobile devices where sensitive information is stored.

Additionally, many states have caps on damages in medical malpractice lawsuits. While these are not per se malpractice cases, some courts may still cap damages on recovery on a negligence cause of action against the hospital and its providers because the events occur in a health care setting. Even in states with caps, most states do not have caps in place in lawsuits against medical device manufacturers or other business associates.

The scope of liability of medical device manufacturers is in a flux depending on the type of the medical device and the theory of liability.[49] Congress enacted the Medical Device Amendments (MDA) to amend the U.S. Food, Drug, and Cosmetic Act (FDCA) in order to extend coverage of the FDCA to medical devices.[50] The MDA divides medical devices into three classes according to perceived patient risk:

Class I – These devices present minimal potential for harm to the user and are often simpler in design than Class II or Class III devices. Examples include stethoscopes and elastic bandages. 47% of medical devices fall under this category and 95% of these are exempt from the regulatory process. Few of these devices have wireless connections or are subject to cyber-attacks *with the exception of medical device data systems, "hospital-derived software", and hardware such as modems, which are expressly promoted as part of the system.* These are now all considered Class I devices, with little U.S. federal regulatory oversight. [51]

Class II – Most medical devices are considered Class II devices. Examples of Class II devices include powered wheelchairs and some pregnancy test kits. 43% of medical devices fall under this category.

Class III – These devices usually sustain or support life, are implanted, or *present potential unreasonable risk of illness or injury*. Examples of Class III devices include implantable pacemakers and breast implants. 10% of medical devices fall under this category. [52] Only Class III devices are subject to the pre-market approval ("PMA") process of the FDA. [53] During the pre-market approval process, the FDA performs a risk-benefit assessment. The FDA can then approve the application, deny it, or approve it with conditions on distribution.[54] Following the U.S. Supreme Court's decision in *Riegel v. Medtronic, Inc*., [55] many courts have found that state-law claims concerning PMA devices are preempted. *Subject to limited exceptions, the most difficult devices/drugs for patients to successfully sue the device manufacturer over are these Class III drugs, which have been subjected to PMA.*

---

[49] Except about 1% of select Class III medical devices cleared through the FDA's PMA process cannot be sued by plaintiffs in tort under most circumstances. *Riegel v. Medtronic,* 552 U.S. 312 (2008).

[50] 94th U.S. Congress (December 11, 1975). "H.R.11124: Medical Device Amendments". *U.S. House of Representative Bill Summary & Status*. Library of Congress.

[51] *Cyberattacks on Medical Devices and Hospital Networks: Legal Gaps and Regulatory Solutions* by Katherine Booth Wellington (2014).http://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1578&context=chtlj

[52] *Learn if a Medical Device Has Been Cleared by FDA for Marketing* (last updated June 4, 2014) http://www.fda.gov/MedicalDevices/ResourcesforYou/Consumers/ucm142523.htm

[53] 21 U.S.C. § 360c(a)(1)(C). **While subject to premarket approval (PMA), most Class III devices are cleared by the FDA without PMA.** *Overview of Medical Devices and Their Regulatory Pathways,* FDA http://www.fda.gov/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/CDRHTransparency/ucm203018.htm (last visited Sept.9,2015).

[54] 21 U.S.C. § 360k(a).

[55] 552 U.S. 312 (2008)

After FDA approval of any medical device (Class I, II, or III), the device manufacturer is required to report any information that reasonably suggests the device (1) may have caused or contributed to a death or serious injury or (2) has malfunctioned and that any recurring malfunction would be likely to cause or contribute to a death or serious injury. [56] It is a violation of this reporting duty that forms the basis of an exception to the broad preemption doctrine, and which may form the basis for a state-law "failure to warn the FDA" claim lawsuit over a Class III device, even if the device was subjected to PMA[57] [58]

This exception allowing even Class III devices to be potentially ripe for attack in a U.S. state court claim is particularly intriguing in cyber-attack litigation ***given that the FDA has already warned the device manufacturers to increase cybersecurity and take additional steps to guard against malware and other cyber-attacks.***

IV. POTENTIAL SOLUTIONS MUST BE IMPLEMENTED

None of the existing legal frameworks are wholly effective in addressing the colossal threat of cyber vulnerability in the delivery of health care in the United States. New carrots (incentives) and sticks (penalties or damages) must be created to help remedy the looming cyber vulnerability of worldwide health care systems. The following are intended to be a springboard for discussion of some potential solutions:

A. "Carrots" or incentives

1.Malpractice and liability insurers most likely paying claims for cyber-attack and privacy lawsuits should give financial incentives to health care providers and device manufacturers to institute programs designed to limit exposure.

2. While the FDA guidance[59] is not binding, it should be implemented by device manufacturers *or the manufacturers may have to answer in a class action lawsuit as to why they didn't adopt such recommendations if and when their devices are infected with malware that causes patient harm.*

3.Health care providers need ongoing training on healthcare cyber vulnerability and how to prevent it.

4. Health care providers must develop and enforce policies and procedures regarding cybersecurity:

a. Such policies may include a ban on *personal* mobile devices transmitting health data of any kind. Health providers would instead make available mobile devices that are regularly updated with the latest encryption software and equipped with remote wiping capability. The mobile devices should be regularly checked for malware and passwords must be changed on a regular basis.
b. "One-way use" of new-USB ports should be used to manage access to medical devices. Such ports are known to be a way malware invades medical devices and are used as an entry for infection of other medical devices. [60]
c. Hospitals and health care providers should have medical devices isolated in a secure network zone that is protected with an internal firewall allowing only limited access to approved IP

---

[56] 21 C.F.R. § 803.50(a); 21 U.S.C. § 360i(a)

[57] *Stengel Tangles MDA Preemption: Ninth Circuit Decision Creates Split on Buckman Preemption of Post-Market Reporting Requirements* Erin M. Bosman, Joanna L. Simon, and Julie Y. Park, Morisson & Foerster. http://media.mofo.com/files/Uploads/Images/130114-Buckman-Preemption.pdf (last visited September 4, 2015)

[58] *Stengel v. Medtronic, Inc*., 704 F. 3d 1224 Court of Appeals, 9th Circuit 2013

[59] *Guidance for Industry - Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software* http://www.fda.gov/RegulatoryInformation/Guidances/ucm077812.htm (last visited Sept. 9, 2015) In sum, the FDA recommends as follows: First, that companies establish quality management principles to ensure safe and effective products. Second, it emphasizes the necessity of developing industry standards and best practices. Third, it envisions industry leveraging voluntary conformity assessment tools—such as certification, accreditation, and product testing to provide transparency and accountability. Finally, it highlights that the future of responsible health IT requires continual learning and improvement.

[60] *Supra,* TrapX p.38.

addresses and specific services. This is to limit malware infecting the device *and to prevent the infected device from infecting the entire network.*

5. Health care providers should avoid use of off-the-shelf commercial software with little or no cybersecurity in place.[61].[62]

6. Medical devices should have digitally signed software and encrypted internal data with passwords that can be modified and reset *by the health care provider.*[63]

7. Contracts between health care providers and medical device suppliers must be reviewed and updated to include specific express language:

a. Outlining the respective duties of each party in the detection, remediation, and refurbishment of all medical devices that have internet connectivity.
b. A documented test process must be conducted on all such medical devices to determine if they are infected and a documented standard process must be in place to rebuild any devices with malware.[64]
c. Medical device manufacturer technicians must be demonstrably trained and skilled to handle complex security issues with installed medical devices. [65]

8. Require a written representation that any and all persons who may have access to the covered entity's patient HRE/EMR, whether working for a business associate or a subcontractor, have received appropriate cyber training and signed confidentiality agreements.

B. "Sticks" or Expanded Liability for Violations

Many of the recommendations below are admittedly overlapping and cumulative, but intend to provide a springboard for a discussion of innovative ways to use the system of justice to crackdown on cyber attacks in health care. Any one or more of these proposals, in combination, would likely trigger significant preventative steps being taken industry wide to avoid malware attacks on medical devices and apps as well as greater protection of personal healthcare information. Prevention is the point, isn't it?

1. International standards recognizing an enforceable privacy right is needed. In the United States, a federal constitutional right of privacy[66] is a necessary step**.** Given the disparate court rulings around the nation,[67] the U.S. Supreme Court will *eventually* have to decide if there is a constitutional right to protect personal information and /or if such information, including genetic information, is a personal property right, subject to a civil lawsuit if the privacy right is infringed.

Acknowledging this basic human right will give health care providers, medical device manufacturers and mobile health app creators an incentive to create products and systems better able to protect EHR/EMR information at the risk of being held civilly liable for such breaches.

2. Adding a private cause of action to criminal statutes, such as the American Computer Fraud and Abuse Act

---

[61] *Public Health Effectiveness of the FDA 510(k) Clearance Process: Measuring Postmarket Performance and Other Select Topics: Workshop Report*. Kevin Fu, PhD. http://www.ncbi.nlm.nih.gov/books/NBK209656/ (last visited September 13,2015)
[62] *Supra,* Wellington at p.150.
[63] *Supra,* TrapX p.38
[64] TrapX Security, *supra,* report p.12 citing Moshe Ben Simon.
[65] *Id*., p.11
[66] Unanimous decision *Riley v. California,* 573 U.S. 134 S.Ct. 2473 (2014) requiring a warrant before searching smart phone seized during arrest. Privacy advocates applaud *Riley* protecting digital privacy, but *Riley* relied on reasonableness balancing test from other Fourth Amendment cases. Footnote in *Riley* left open whether collection or inspection of aggregated digital information is a search *under different circumstances*.
[67] See above footnote # 42

(CFAA)[68] and the Federal Anti-Tampering Act would help to prevent cyberattacks. The U.S. government does not have the resources to prosecute all violations of these criminal statutes. By expanding the coverage of these criminal statutes and allowing a private cause of action, and attorneys' fees, not only will more meritorious claims be prosecuted, but also the mere existence of these statutes will likely have an effect on *preventative steps being taken to prevent hacking.*

3. Expanding HIPAA/ and add a private cause of action would deter violations of patients' privacy. There is currently no private cause of action allowed under HIPAA.[69] Given little funding for government enforcement and no private cause of action for attorneys to prosecute, there is scant evidence that HIPAA safeguards are effective in preventing wholesale disclosure of confidential patient information.

Absent an express private cause of action, HIPAA should be viewed as the *minimum standard* of care required of health care providers, and civil lawsuits under general negligence principles should be brought.

4. CMIA should be expanded beyond its narrow state scope in California, and federalized into the law across the land to allow private causes of action and class action lawsuits for violations of patient HRE/EMR information.

Why should big data of personal health information be profitable for corporations at the expense of the individual? Because Fitbit, Apple Watch and other apps and devices can pull all that together and create almost an equivalent of a health record from the information garnered from these devices, they should also be subject to CMIA type legislation, especially because these apps are almost universally on mobile devices, re-identification is often possible, and there is a higher likelihood for breaches to occur with mobile devices.

5. A new tort, "negligent data security", may arise out of hackers infiltrating the adultery/cheating website Ashley Madison and downloading private information of the estimated 37 millions of users who registered on the site. Details, including names, emails, home addresses, financial data, message history and ***sexual proclivities -- were posted publicly online***. While this does not arise in the healthcare arena, *given the highly sensitive nature of the information disclosed,* parallels can be drawn.

Multiple lawsuits are being brought across the U.S. by individuals who registered to use Ashley Madison and who are now suing in various states all seeking class-action status to represent the millions of registered users of the site. The lawsuits are based on numerous theories including negligence, breach of contract and privacy violations. They claim Ashley Madison failed to take reasonable steps to protect the security of its users, including those who paid a special fee to have their information deleted.

Some of these lawsuits have been couched in traditional negligence language, but other lawsuits coin a new phrase "negligent data security" as the theory of liability. The first approach is garden-variety negligence, the kind routinely plead in a personal injury suit. The second approach is much closer to a products liability claim, where the failure to take commercially reasonable and viable steps to protect consumers led to harm. This new cause of action integrates the established theory in products cases of a "**commercial reasonableness test**" premised on the fact that businesses holding private data are providing a "product" (i.e., data security) and that failure to provide that product in a reasonably safe manner creates liability.

There is some overlap because proving either traditional negligence or the negligent data security action both require an establishing a duty of care. Still, at least some legal commentators believe there is a critical difference between the two theories that underscores the relative novelty of data breach negligence suits:

> "If a data breach suit is simply a negligence action, then the plaintiff's critical step is to show what the defendant knew about foreseeable risks and whether they ignored those risks. **Both the burden of proof and the pre-suit economic burden are on the plaintiff** in that scenario.
>
> But if the "commercially reasonable options" approach prevails, then the **economic burden shifts**

[68] 18 U.S.C. Section 1030 (2012)

[69] For example, California privacy in healthcare standards is contained in the Confidentiality of Medical Information Act (CMIA). Cal. Civ. Code §§ 56-56.16

> **to the *defendant*, which must demonstrate that it kept up with and abided by industry standards on data security**.…**That standard is advantageous to plaintiffs suing companies that did not keep pace with the industry**.
>
> Second, it would provide some measure of comfort to those companies that do employ best practices, because **it would create a presumption of reasonable care, even in the event of a data breach**. As the federal government's recent data security problems demonstrate, no amount of resources can prevent every hack. For businesses that take the commercially reasonable steps to protect customer data, then a breach might not signal automatic liability."[70]

Much time will pass before we will know if this new potential tort is viable as it winds its way through the court system, but if it is viable in the Ashley Madison breach case over personal sexual information, there is scant reason why it should not apply equally well in the healthcare arena.

6. The need for international standards for collecting and processing personal data are acknowledged worldwide. However, the lack of a binding international instrument has been the subject of much debate. In just one example, at the International Organization for Migration's 31st International Conference of Data Protection and Privacy Commissioners,[71] a resolution was adopted by a number of States calling for a universal convention and recognizing that data protection and privacy are fundamental rights attributed to all individuals, irrespective of nationality or residence.

V. CONCLUSION

While telemedicine, use of connected medical devices and apps and utilization of cloud services for the storage and exchange of patient health information is growing, policies and laws are lagging, exponentially increasing the risk of loss of personal information. Current U.S. law only provides a baseline of protection for personal health information. If people are to maintain any semblance of privacy and confidentiality with regards to their personal medical data, international standards for integrated data and privacy governance programs must be quickly implemented or the future of medical privacy will be a bygone concept.

---

[70] *Legal Precedent May Come From Ashley Madison Breach* By Philip R. Stein and James J. Ward, http://www.law360.com/articles/698349/legal-precedent-may-come-from-ashley-madison-breach (last visited September 13, 2015)

[71] *IOM Data Protection Manual*, http://publications.iom.int/bookstore/free/IOMdataprotection_web.pdf

REFERENCES

Books

IOM Data Protection Manual, 2010, International Organization for Migration.

WACHTER Robert, 2015, **The Digital Doctor: Hope, Hype, and Harm at the Dawn of Medicine's Computer Age**, McGraw Hill.

Articles

APUZZO Matt, SANGER David and SCHMIDT Michael, Sept. 2015, **Apple and Other Tech Companies Tangle With U.S. Over Data Access**, The New York Times.

Bitglass Report, 2014, **Bitglass Healthcare Breach Report: Is Your Data Security Due For a Physical?**

BOSMAN Erin M., PARK Julie Y., and SIMON Joanna L., January 2013, **Stengel Tangles MDA Preemption: Ninth Circuit Decision Creates Split on Buckman Preemption of Post-Market Reporting Requirements**, Morisson & Foerster.

DALEY Heather A., June 2000, vol.9: Iss.1, **Telemedicine: The Invisible Legal Barriers to the Health Care of the Future**, Annals of Health Law. District Court Annals.

FU Kevin, 2011, **Public Health Effectiveness of the FDA 510(k) Clearance Process: Measuring Postmarket Performance and Other Select Topics: Workshop Report**, National Academy of Sciences.

HARDESTY Harry, January 2015, **Privacy Challenges Analysis: It's surprisingly easy to identify individuals from credit-card metadata**, MIT News Office.

HealtHit, 2014, **What are the differences between electronic medical records, electronic health records, and personal health?**

HIGGINS Kelly J., July 2015, **Hospital Medical Devices Used as Weapons in Cyber—attacks**, Dark Reading.

iHealth Beat, May 2014, **Judge Dismisses Most of Class-Action Lawsuit Over DOD Data Breach**, The Advisory Board Company.

KREBS, June 15, 2015 **Major zero-day security flaws in iOS & OS X allow theft of both Keychain and app passwords**.

LIU Vincent, April 2015, vol.313(14): p.1471-1473, **Data Breaches of Protected Health Information in the United States**, The JAMA Network.

MDDIAMIN (username), August 2009, **Privacy Basics: A Quick HIPAA Check for Medical Device Companies**, Medical Device and Diagnostic Industry.

PERAKALIS Eric D July 31 2014, 395-397, **Cyber-security in Health Care**, The New England Journal of Medicine.

PINSKER Beth, August 2015, **Coming soon to a screen near you: Doctors**, Reuters.

STEIN Philip R. and WARD James J., September 2015, **Legal Precedent May Come From Ashley Madison Breach,** Law360.com.
TALBOT David, October 2012, **Computer Viruses Are "Rampant" on Medical Devices in Hospitals: A meeting of government officials reveals that medical equipment is becoming riddled with malware**, MIT Technology Review.

Telehealth Resource Centers, 2015, **Developing a Training Strategy**.

TrapX Labs Fireye May 2015, p.8, **Anatomy of an Attack: MEDJACK [Medical Device Hijack]**, TrapX Security.

U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES. March 2015, Telehealth.

U.S. FOOD AND DRUG ADMINISTRATION, June 2013, **Cybersecurity for Medical Devices and Hospital Networks: FDA Safety Communication**.

U.S. FOOD AND DRUG ADMINISTRATION, 2015, **Guidance for Industry - Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software**.

VENTOLA C. Lee, May 2014, vol.39(5); p.356-364, Mobile Devices and Apps for Health Care Professionals: Uses and Benefits**, Journal of Pharmacy and Therapeutics.**

WELLINGTON, Katherine B., 2014, p.139, **Cyber-attacks on Medical Devices and Hospital Networks: Legal Gaps and Regulatory Solutions**, Santa Clara High Tech Law Journal.

WILLIAMS Patricia, July 2015, vol.8; p.305–316, **Cyber-security vulnerabilities in medical devices: a complex environment and multifaceted problem**, Med Devices.

Case law citations:

Daury v. Smith, 842 F.2d 9 (1st Cir. 1988).

Fadjo v. Coon, 633 F.2d 1172 (5th Cir. 1981).

Norman-Bloodsaw v. Lawrence Berkeley Lab., 135 F.3d 1260 (9th Cir. 1998).

A.L.A. v. West Valley City, 26 F.3d 989 (10th Cir. 1994).

Doe v. City of New York, 15 F.3d 264 (2d Cir. 1994).

Harris v. Thigpen, 941 F.2d 1495 (11th Cir. 1991).

United States v. Westinghouse Elec. Corp, 638 F.2d 570 (3d Cir. 1980).

Woods v. White, 689 F. Supp. 874 (W.D. Wis. 1988), aff'd, 899 F.2d 17 (7th Cir. 1990).

Walls v. City of Petersburg, 895 F. 2d 188 (4th Cir. 1990).

Doe v. Wigginton, 21 F.3d 733 (6th Cir. 1994).

Alexander v. Peffer, 993 F.2d 1348 (8th Cir. 1993).

In Eisenhower Medical Center v. Superior Court, 226 Cal.App.4th 430 (2014).

Sutter Health v. Superior Court, 227 Cal.App.4th 1546,(2014).

Regents of the University of California v. Superior Court, 220 Cal.App.4th 549, (2013).

Riegel v. Medtronic, 552 U.S. 312, (2008).

Riley v. California, 573 U.S. __, 134 S.Ct. 2473 (2014).