Cybersecurity and Cybercrime: Are they in the Patient Safety Wheelhouse?

Cybersecurity and Cybercrime: Are they in the Patient Safety Wheelhouse?

AUTHORS:
John J. Nance, JD
SMU Edman School of Law,
Executive Board Member
Aviation Analyst ABC World News

Christopher R. Peabody, MD, MPH
Assistant Clinical Professor
Department of Emergency Medicine
1001 Potrero Avenue Room 1E21
San Francisco, CA 94110
christopher.peabody@ucsf.edu

FUNDING:
Funding in part by Texas 1115 Waiver DSRIP Demonstration Project

PRESENTATION:
The content of this paper was presented at University of North Texas Health Science Center Patient Safety Summit on November 6-7, 2015.

Suggested Citation:
Nance JJ, et al. 2016. Cybersecurity and Cybercrime: Are They In The Patient Safety Wheelhouse? *Threat Safety Community at Texas Medical Center.* 2016.

ABSTRACT

A critical question healthcare institutions have to answer is: Are the new healthcare cybercrime issues in the patient safety leader's wheelhouse? We believe the answer is an unequivocal yes, absolutely. The pattern of preventable harm to patients, caregivers, authors, and institutions is exploding as rapidly as the evolution of information technology. Like other areas of patient safety impacted by multiple dimensional and complex factors, "everyone owns it and no one owns it". An existing healthcare cybercrime classification is presented with examples from the literature and industry. We make the case that healthcare leaders need to waste no time in addressing this exploding problem, multidisciplinary teams need to tackle it, and much of this new domain is directly in the wheel house of patient safety leaders. Multiple national polls of patient safety leaders in 2015 and 2016 confirmed the importance of healthcare cybercrime to patient safety. Those polled expressed substantial interest in pursuing education in this arena.

FINDINGS

HEALTHCARE CYBERCRIME – NO ONE OWNS IT – EVERYONE OWNS IT

Leaders of healthcare organizations are being challenged on all fronts as their revenue generation moves from volume of care transactions to risk sharing and population management contracts. The healthcare cybercrime and cybersecurity problems are yet another set of new issues layered on the backs of already overtaxed executives.

Information Technology leaders typically are overwhelmed with the challenges of keeping technology running and updated. Security officers are trying to prevent insider breaches and outsider hack attacks. Safety and quality leaders are charged with the growing visibility of preventable harm due to medical error, now being recognized as the 3rd leading cause of death.[1] If you ask any one of these leaders who has the responsibility for the prevention of, preparedness against, protection from, and performance improvement related to cybercrime causing harm to patients, caregivers, and academics; none would likely stake a claim. Yet, it is the patient safety leader who has more of the needed tools, plus an understanding of performance improvement, and an appreciation for the ultimate physical and reputational harm from cybercrime to patients, caregivers, and healthcare academics.

HEALTHCARE CYBERCRIME: A REAL PATIENT SAFETY ISSUE – CONFIRMED

The existing healthcare cybersecurity classification which will be described in more detail below has been presented on multiple occasions to a national community of patient safety and quality leaders who were polled on their interest. Of 68 organizations polled, 72% very strongly agreed that cybercrime was a patient safety issue and wanted a deep dive on the topic. A second poll of 60 organizations revealed only 25% agreed or very strongly agreed they were prepared for medical record breach.[2,3] In fall of 2015 this topic was presented at a national audience of patient safety innovators at a global summit at the University of North Texas Health Science Center.[4] It resonated with

them and is provided in a more comprehensive fashion here to make the case that healthcare cybercrime is indeed in the wheel house of patient safety leaders. It may even give them a new role in leading their institution's approach to deal with the exploding problem of preventable clinical harm resulting from the use of computers, the internet, and communication network technologies.

- **Health Information Technology Errors, Harm, and Threats:**
  For clarity, typical Health Information Technology errors, unintentional harm and threats are not within the scope of this paper, nor do we consider them cybercrime categories. However, they are increasingly recognized by the patient safety community and we mention them here to acknowledge them.

There are some behaviors and issues not included in the classification described below, that must be carefully tracked. It will be the responsibility of others to define them as criminal in nature. They include:

- **Widespread Information Blocking:** In a stunning report to the U.S. Congress in 2015, the Office of the National Coordinator for Health Information Technology (ONC) confirmed that both provider groups and electronic record suppliers were actively blocking access to medical records by patients.[5] This was a great surprise to many, but not to those close to the action. A great source of harm to patients is the lack of timely access to this information which can be lifesaving. Indeed, the increasingly important principle of "Nothing about me without me" automatically excoriates such blocking.
- **The Foxes Are the Architects of the Hen House":** The Food and Drug Administration Safety and Innovation Act (FDASIA) of 2012 required a report from the HHS Secretary by January 2014 that "contains a proposed strategy and recommendations on a risk-based regulatory framework pertaining to health IT, including mobile applications, that promotes innovation, protects patient safety, and avoids regulatory duplication." The FDASIA Committee produced such a report, which among other things recommended that "vendors should be required to list products which are considered to represent at least some risk if a non-burdensome approach can be identified to doing so." However it was reported by the press that the committee charged with developing the recommendations approved the following wording: "vendors should be required to list products which are considered to represent at least some risk and a non-burdensome approach should be developed for this." The distinction between "if a non-burdensome approach can be identified" and "a non-burdensome approach should be developed" is vast and somehow the word change between what was reported to be the committee's recommendations and the final report raised concerns of motivation tied to conflict of interest.[6] The slight change in wording let the industry off the hook. An investigation by the press revealed the chair of the committee controlling the report to have substantial conflicts of interest including consulting fees from 12 groups that included start-ups, established vendors, and patient-safety groups leading to the "Foxes are the Architects of the Hen House" concern.[7]

Both of the above issues have direct impact on patient safety and demand the attention of safety and quality leaders.

HEALTHCARE CYBERCRIME LEXICON

Non-healthcare and Healthcare Identity and Professional Cybercrime:

Cybercrimes threatening individuals and institutions are evolving as rapidly as are the technologies we use. As such, we need to evolve a lexicon of operational terms and use reconciling frameworks to organize an approach for healthcare leaders.

The Healthcare Cybercrime Classification used below to address the role patient safety leaders can play provides such a reconciling framework and lexicon to address this evolving set of problems.[8] While there are great benefits and explosive growth that computers, networks, and the internet generate, there are correspondingly new threats to both medical identity and healthcare professional identities that will demand the attention of leaders.

- **The Identity Cybercrime Continuum:**
  The continuum of personal identity cybercrimes and medical healthcare identity cybercrimes fall along a very similar continuum from mere breach to full contamination and vandalism. Non-healthcare cybercrime targeting individuals began with the theft of their credit card and personal information that can be sold on the black market or used to generate cash from products purchased. This has evolved to the refined state of using one's personal identity to go so far as to submit federal tax returns for fraudulent refunds. This is where the medical identity information became very valuable to thieves in their quest. The operational definitions and classification of breach, theft, counterfeit, and harm due

to contamination and intentional vandalism which we explore in more detail provide a way of understanding and tackling potential threats.

- **Healthcare Professional Identity Cybercrime:**
  Harm to ones Healthcare Professional Identity is another exploding problem under the waterline. Although WWW stands for World Wide Web, in reality it might just well be considered to stand for the Wild Wild West. The new digital frontiers that have been opened to us are still missing the rule of law and checks and balances of ethics and civility.[9] Just like the pioneers opening any new territories, we must rely on ourselves for protection. Digital media on the web is immediate, permanent, and searchable. It is a world where the volume of disseminated hits trumps the veracity of the message. Where rumor is more likely to become widely accepted as fact, the more it is repeated it becomes an electronic version of the Third Reich's "Big Lie" principle. Indeed, history teaches us that any new form of power will be abused. The intersection of the internet and the integrity of healthcare professional identities is no different.

The categorization of professional identity cybercrimes used below addresses those that threaten both individuals and indirectly their organizations. They include clinical trial misconduct, fraudulent healthcare publication, sham peer review, healthcare workplace cyberbullying, healthcare journalism fraud, and website fraud and vandalism. All of these issues potentially threaten our caregivers and in turn the safety of our patients and their families.

IDENTITY CYBERCRIME CONTINUUM

The non-healthcare identity cybercrime continuum from breach to vandalism was the forerunner of what we are now experiencing in healthcare. What has been learned by thieves there has been applied to healthcare cybercrime and is very instructive.

- **Identity Breach: A cyber-attack or unauthorized access to an individual or organization's information systems without known or apparent use of the data is an Identity Breach.[3]**
  The hack attack that breaches an organization's information systems without known or apparent use of the data may have occurred merely due to the challenge of independent hackers, a nation state attempting to cause harm, or revenge by disgruntled former employees. The Sony Pictures Entertainment breaches in 2011 and 2014 are examples of an unknown individual who did hundreds of millions of dollars of damage and exposed tens of thousands of individuals to identity theft.[10] Breaches can occur through unintentional events such as what happened with the National Archive and Records Administration in 2008 when 76 million records were exposed when a hard drive sent for repair was not sanitized[11].

- **Identity Theft: When the personal identity information of an individual or individuals is intentionally stolen using computers, communication networks, or the internet is Identity Theft. This may occur through computer software or hardware vulnerabilities.[3]**
  The 2013 breach and theft of as many as 110 million records of Target customers' credit card information captured substantial media attention, however they were not alone. There have been and continue to be many more. In 2014 Home Depot had 56 million payment cards compromised when thieves infected point-of-sale systems with malware that pretended to be antivirus software. When it was discovered in 2007, the TJX breach was the biggest theft of consumer data ever in the United States. Albert Gonzales, a known hacker, stole at least 45 million credit card numbers and the estimates have risen as high as 90 million. Selling them on the black market and turning them into cash cost TJX $256 million.[12] These examples are important to us in healthcare because they follow a common pattern. Healthcare information is many times more valuable to thieves than credit card data, because they can use it to generate far more reward as we will discuss below, and because healthcare has not hardened its defenses as has the lay community.

- **Identity Counterfeit: When an individual or organization unlawfully forge, copy, or imitate the personal identity of an individual or organization using computers, communications networks, or the internet; the cybercrime may be described as Identity Counterfeit.[3]**
  Thieves who have stolen or purchased financial and credit card information represent themselves as the owner and obtain products, services, or turn the information into cash. Combined with the richness of medical information, they can apply for more credit, submit tax returns, and create no end of havoc to the unsuspecting public. Early in 2015, Intuit, the company behind TurboTax, had to shut down e-filing in several states after the company noticed an uptick in what appeared to be fraudulent tax returns. Tax-related identity theft is a big-money crime, and the statistics prove it. The IRS stopped 19 million suspicious tax returns last year, and stopped more than $63 billion in fraudulent refunds. An enormous $5.8 billion in tax refunds were paid

out to fraudsters. In 2012, the Treasury Inspector General for Tax Administration projected that cybercriminals would fraudulently net $26 billion through the year 2017.[13]

- **Identity Contamination, Harm and Vandalism: When an organization or individual or individuals with illegal intent use the personal and financial identity of a person to generate fraudulent gains using computers, communication networks, or the internet; they can contaminate the credit and financial history of that person and thus have committed an Identity contamination. Such contamination is very difficult to correct and sometimes causes lifelong damage to the victims.[3]**
  Once enough information is obtained that can be used to convert it to the benefit of thieves, they are on the way to contaminating the credit, financial records, and causing harm that may be irreparable. The cost to an individual family that has had its financial identity stolen and credit ruined is on average $4,930 according to the U.S. Department of Justice. This is more than the average United States monthly salary.[14]

MEDICAL IDENTITY CYBERCRIME CONTINUUM

In May of 2016, the Ponemon Institute released its *Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data* which year over year has seen a dramatic rise in healthcare data breach frequency, damage, and cost. The survey included 91 healthcare organizations and 84 business associates with whom they share medical data.[15] Their findings are enlightening and sobering:

- The cost of healthcare cybercrime may be $6.2B and the cost for the average breach is $2.2 million.
- Half of healthcare organizations have little or no confidence that they can detect all data loss or theft.
- In 2016, ransomware, malware, and denial-of-service (DOS) attacks are the top healthcare cyber threats.
- "Approximately two thirds of all respondents don't offer any protection services for breach victims, nor do the majority have a process in place for protecting errors in the victim's medical records".
- Incident response is often outsourced to outside counsel and forensic specialists.
- "More than half of covered entities in the survey say they are not vigilant in ensuring partners and third parties protect patient information".
- The majority of both healthcare organizations and Business Associate organizations have not invested in the technologies necessary to mitigate a data breach, nor have they hired enough skilled IT security practitioners.
- Little appears to be done to help patients and families after an event occurs.

Unfortunately, there is no healthcare equivalent of the *Fair Credit Reporting Act*, which limits consumers' financial losses if someone fraudulently uses their credit information.[16] Caveat emptor, the Latin term that means "let the buyer beware" could never have been more applicable than to the issues of healthcare cybercrime.

- **Medical Identity Breach: A cyber-attack or unauthorized access to an individual or healthcare organization's medical information systems using computers, communication systems, or the internet without known or apparent use of the data is a Medical Identity Breach cybercrime.[3]**
  The Office of Civil Rights (OCR) under Health and Human Services publishes data breaches as reported to them and required by HIPAA. The numbers for 2015 are staggering with 253 healthcare breaches that affected 500 individuals or more with a combined loss of over 112 million records – almost 35% of the US population**.** Anthem–represented almost 79 million records breached and over 70% of the total records compromised, leaving 33 million records breached through other healthcare organizations including Premera, and Excellus Blue Cross plans and UCLA Health. In 2015, 64% more Social Security Numbers were exposed, and there was a 110% increase in data on medical records made available to fraudsters.[17]

Theresa Payton, former White House CIO predicts that 1 in 3 health care recipients will be the victim of a health care data breach in 2016.[18] Although criminal attacks are 50% of breaches and the leading cause of data breaches in healthcare, 13 percent are due to a malicious insider.[19]

Although a breach does not guarantee theft and contamination will occur, it makes it very likely. One in five data breach victims suffered fraud in 2015, up from one in seven in 2014.

Ransom is most recent form of breach that can impact patient safety. Hollywood Presbyterian Medical Center paid a $17,000 ransom in bitcoin currency to a hacker who seized control of the hospital's computer systems and would give back access only when the money was paid, The ransom malware locked the system by encrypting files allowing the cybercriminals to demand ransom to release them.[20] The risk to patients of such an occurrence includes delayed and interrupted care and errors when alternative paper systems

have to be used. Lost minutes can lose lives.

The lessons for healthcare leaders are clear. Be prepared for breach, theft, interrupted access, and contamination of your patients' records. Is your patient safety and quality team prepared for a breach and shut down of your CPOE and Electronic Record System?

- **Medical Identity Theft: When the personal medical information of an individual or individuals is intentionally stolen using computers, communication networks, or the internet, it is a cybercrime. This typically happens through a Medical Identity Breach cybercrime.[3]**
  A breach becomes a theft when it is verified that outside actors possess the data and records from a breach. Medical records and identity may be stolen for purposes other than to fraudulently obtain money. Celebrities and public figures records and medical records of their families may be stolen to be sold to less principled branches of the press. The theft of records that are ultimately published generate preventable costs including financial damages and awards, legal fees, and harm to the reputation of the healthcare institution. Recent examples of celebrities whose records were wrongfully accessed and/or stolen by hospital staff include George Clooney, Britney Spears, Richard Collier (NFL), Michael Jackson, U.S. Rep. Gabrielle Giffords, and Kim Kardashian.[21]

- **Medical ID Counterfeit: When an individual or organization unlawfully forge, copy, or imitate the medical identity of an individual using computers, communications networks, or the internet; the cybercrime or unethical behavior may be described as Medical Identity Counterfeit.[3]**
  In the 2015 *Wall Street Journal* article "How Identity Theft Sticks You With Hospital Bills", the use of stolen personal medical data to get treatment, drugs, and medical equipment is described. Multiple cases were presented in which thieves have used a patient's personal identification information, medical insurance data, and personal medical records to defraud payers and hospitas of services. Amazingly, numerous individuals have even undergone complex surgical procedures requiring many days of hospitalization using stolen identities including organ transplants and even elective surgery such as penile implant procedures.[22] The fraudulent pursuit of healthcare, prescriptions, and medical equipment generates an enormous risk to the victim patient's future care which may only be identified when they are sick or injured.

- **Medical ID Damage, Contamination, or Vandalism: When an organization or individual or individuals with unethical intent use the medical identity of a person to generate fraudulent gains using computers, communication networks, or the internet; they can contaminate the medical records of that person and thus have committed medical Identity contamination. Such contamination is very difficult to correct and sometimes causes lifelong damage to the victims.[3]**
  Despite the risks to patients who have had their records lost or stolen, only 19 percent of healthcare systems responding to the 2016 Ponemon study cited above have a process in place to correct errors in victim's medical records.[23]
  If a breach, theft, and counterfeit process has occurred with a patient's medical records, an enormous patient safety threat has developed landing squarely in the safety leader's wheelhouse:
  - False information about diabetes, cancer, heart disease, and other conditions may impact their next episode of care.
  - False drug allergies or medication history falsified to obtain pain medications can impact emergency care.
  - Medical benefits may become exhausted and certain care may be erroneously declined.
  - Almost one third of patients who have their medical identity stolen ultimately lose their healthcare insurance. (prior to the Accountable Care Act).[24]
  - The relationship and trust between a good compliant and ethical patient and their care providers may be permanently destroyed.
  - The financial risk and risk to the reputation of the care provider may be very high and unknown until a patient sues.

  Such victims may not find out medical record fraud until they get a bill or a call from a collection agency. Clearing up an erroneous billing situation with a healthcare provider, collections agencies, and credit agencies can be very complicated, time-consuming, and even ultimately unsuccessful for patients. What is worse, the thief's generated counterfeit data used to steal becomes incorporated into the victim's medical records. Proving that the services were provided to someone else who stole personal information can be a Catch-22 situation. While it may be the victim's medical file, because of a gross but widespread misinterpretation of HIPAA laws, the victim may be declined access to the file itself merely because information that effectively is not his or hers has been mixed in. [25, 26] This is not a hypothetical risk; it has been

documented by the Wall Street Journal cited above.

Sixty-five percent of medical identity theft victims in the 2015 Ponemon Institute report had to pay an average of $13,453.38[27] to resolve the crime. This average sum included lost time the victims spent correcting records and restoring their true identities; money spent out-of-pocket for medical services and medications due to a lapse in healthcare coverage; and reimbursements to healthcare providers to pay for services provided to impostors.[28] As noted above, one third of victims ultimately lose their healthcare insurance with little protection from this consequence which is a tragedy. Time will tell whether this will happen with the changes driven by the Affordable Care Act.

Contamination of a medical identity can cause invisible errors that can result in very visible deaths with very real financial and reputational consequences.

HEALTHCARE PROFESSIONAL CYBERCRIME CONTINUUM

- **Healthcare Professional Identity Cybercrime: New Tech – Old Crimes.**
  The new and dramatically growing power of computers, the internet, and networks now disseminate information at the speed of light. In the hands of some, this new power is being abused in ways as old as time. These new technologies can accelerate and disseminate evil as well as they can good. Preventable harm to those who serve our patients is critically important and the professional identity that took a lifetime to build can be ruined in a second.

- **The Bullies' Pulpit:**
  Many believe that the opaque, hierarchical, and parochial guild system of medical academics that has served us in a pre-digital age may be leveled by the democratization of information. Others believe it may in fact be perpetuated in domains such as patient safety if the power of the internet and academic notoriety is abused. Some feel that more well-known academics and institutions are using their voice through the press and on the web to discredit competitors for their own gain. The powers of their reach through statements to the press that go viral have a unique force, especially if their comments are critical of others. Such individuals can skew public opinion and destroy reputations overnight. Historically, their ability to attract funding, have a national voice, and disseminate best practice came from the length and value of their curriculum vitae generated through a small number of paper journals and books. Now, those with name recognition and a following in in the press and social media have more reach and power through the internet echo chamber. When there is no check and balance for veracity of the messages released and virally scaled across the web, there is the potential for mob behavior, especially when notable figures breathe life into rumor. The words of Adolf Hitler in *Mein Kampf* are sobering:

  > *In the big lie there is always a certain force of credibility; because the broad masses of a nation are always more easily corrupted in the deeper strata of their emotional nature than consciously or voluntarily; and thus in the primitive simplicity of their minds they more readily fall victims to the big lie than the small lie.*[29]

  Hitler and Josef Goebbels, his propaganda minister, did not have the power of the internet at their disposal, yet they knew the fundamental powers at play. On this identical principle (the Big Lie), the bully pulpit in the new digital world can become the "bullies' pulpit". The short term endorphin incentives fueling vanity may in the long term harm institutions and lives permanently. Safety and quality leaders must make sure they are aware of the risks within and outside of their organizations. The ancient proverb "Pride goeth before the fall" is a warning sign and everyone is susceptible.

- **Professional Identity Breach:**
  It is unknown how many pure professional identity breach and theft occurrences have happened and are happening. At first glance, this threat does not seem very serious. However when a thief couples provider identity information with payer numbers, the combination can be used to submit fraudulent claims to insurers. Such claims are on the rise. In a 2015 report by KPMG, eighty-one percent of healthcare executives say that their organizations have been compromised by at least one malware, botnet, or other cyber-attack during the past two years, and only half feel that they are adequately prepared in preventing attacks.[30] It is also known that nation state hackers are formally targeting academic institutions not only for intellectual property, but to identify human sources of the information they seek. A substantial proportion of I.P. theft incidents also occur through insiders who have been approached by nation states or commercial entities. Many such incidents are not reported due to their embarrassing nature to the victim organizations.

- **Professional Identity Theft:**
  Movies such as *Catch Me If You Can* have popularized

professional identity theft or the process of stealing someone's identity. This 2002 motion picture told the true story of Frank Abagnale Jr., who, before his 19th birthday, successfully forged bank checks and stole millions of dollars' while impersonating a Pan Am pilot, a doctor, and legal prosecutor.[31] This is much more common than once believed. For instance, a review of the literature reveals numerous cases. California is just one example of the problem at scale. The California Statewide Law Enforcement Association (CSLEA) working with investigators and the state's medical board on Operation Safe Medicine between June 2011 and June 2012 alone, presented prosecutors with 61 cases in just 12 months. These cases involved people posing as doctors, undertaking risky procedures, and unsafe if not illegal practices while treating patients.[32] There are numerous accounts of people posing as care providers who use stolen names, provider numbers, and even write prescriptions for patients. For instance one such impersonator wrote prescriptions with a similar and uncommon name of another doctor that led pharmacists to believe they were filling prescriptions for providers they work with all the time.

- **Professional Identity Counterfeit:**
  With the advent of the internet, professional counterfeit of invented identities is easier. For instance, an 18-year-old not only masqueraded as a doctor, but even convinced an investor to develop a full-blown clinic by providing computer-generated transcripts and credentials.[33] Network news TV reporters even interviewed him at his clinic when he continued to impersonate a caregiver. He was arrested in February 2016 for practicing medicine without a license.[34]

  It is hard to believe in the digital world today that someone would so fully counterfeit their education and use that to sell consultancy services as a doctor to other doctors and even apply for grants, but it has happened. Take the case of William Hamman, an airline pilot who claimed to have a medical and doctoral degree from the University of Wisconsin-Madison. When his credentials were checked by the Associated Press, he was found to be a complete fraud. He was caught when applying for a grant and found to have no MD, no PhD, nor did he attend the residency and fellowship he claimed. He purported himself to be a fully trained cardiologist. According to NBC News, he served as a paid consultant with cardiology groups; taught webinars on what doctors do right and how to improve; and held academic posts and shared in government grants.[35] In reality, he was a licensed pilot and an airline captain who was grounded after his bogus medical career was revealed. He gave lectures at continuing medical education conferences that were designed to train physicians and sharpen their skills in their specialties. Hamman did apparently go to medical school for a few years, but dropped out before he graduated, the AP reported.[36] When his name is searched in the PubMed index (our most trusted source for credible medical papers), as recently as July 2016, seven papers remain posted with him as an author in the body of medical science. In as much as a noted and published figure of the quality improvement movement was an outright fraud, the continued presence of his publications in the medical literature stains the integrity of the rest of the publications we rely on to care for our patients.

- **Professional Identity Contamination, Harm, and Vandalism:**
  The professional identity of legitimate healthcare professionals can be harmed by intentional actions of actors who are their collaborators, colleagues, and competitors inside their institutions or outside them. Digital technologies have provided a force multiplier of harm. Categories of harm include the following:

  - **Clinical Trials Misconduct:** The FDA is very well aware of the misconduct of clinical trials and contamination of the resulting publications. It uses the definition of unethical behavior of the "FFP" (fabrication, falsification, and plagiarism) model put forth by the United States Office of Integrity. In the *JAMA* article by the FDA entitled "Research Misconduct Identified by the US Food and Drug Administration: Out of Sight, Out of Mind, Out of the Peer-Reviewed Literature", the FDA reviewed Fifty-seven published clinical trials for which an FDA inspection of a trial site had found significant evidence of 1 or more of the following problems: 39% of trials with falsification or submission of false information, 25% with problems with adverse events reporting, 74% with protocol violations, 61% with inadequate or inaccurate recordkeeping, and 53% failure to protect the safety of patients and/or issues with oversight or informed consent. Only 3 of the 78 publications (4%) that resulted from trials in which the FDA found significant violations mentioned the objectionable conditions or practices found during the inspection.[37] It is sobering to consider that the clinical trials being run at one's organization may have these problems and that the global literature may be contaminated by unethical or sloppy work by one's researchers. When articles do not transmit reality through

the lens of integrity, our profession has a major problem. With no check and balance, the deck is stacked against the truth.

- **Fraudulent Healthcare Publication:** *The National Academy of Sciences*, the most trusted source of scientific information for the U.S. Congress, found an enormous incidence of fraud and misconduct requiring retraction of peer-reviewed publications in the medical literature. In its 2012 article entitled "Misconduct Accounts For The Majority Of Retracted Scientific Publications", it published its extensive review of all 2,047 biomedical and life-science research articles indexed by PubMed that had been retracted by May 3, 2012. They used the same “FFP” (fabrication, falsification, and plagiarism) model of the United States’ Office of Research Integrity, described above.[38] Their work revealed that 67.4% of retractions were attributable to misconduct – including fraud or suspected fraud (43.4%), duplicate publication (14.2%), and plagiarism (9.8%). Only 21.3% of retractions were attributable to error. The articles reviewed were only those existing in PubMed and did not include articles not indexed by that system.[39] Fraudulent medical publications are a threat to the entire organization and the community at large.

- **Sham Peer Review.** Sham peer review is characterized as a review of clinical or scholarly work called for by either a single, or group of physicians, conducted in order to lead to adverse action taken by a review committee.[40] Both the process of clinical peer review of a caregiver’s behavior and peer review of publications can be corrupted. Sham clinical peer review is thought to represent 10-15% of peer review events.[41] In the case of publications, the bad faith actors with a conflict of interest pretend to provide scholarly, arms-length feedback on a paper or postulate. The internet has weaponized the healthcare peer review process. It has shifted exponential power to those bad actors who seek to circumvent due process. Again digital technologies can be a mediator of cybercrime.

  In 1952 the Joint Commission on Accreditation (JCAHO) began requiring peer review at all U.S. hospitals.[42] Clinical peer review is the process by which health care professionals evaluate each other’s clinical performance.[43] Merriam-Webster defines peer review related to work product as “a process by which such scholarly work is checked by a group of experts in the same field to make sure it meets the necessary standards before it is published or accepted”.[44] Sham peer review is the act of corrupting the typical peer review process.

  Undertaken by individuals and groups who have something to gain by discrediting someone, there are common tactics of such an approach. Computers, networks, and the internet weapon-ize sham peer review by overwhelming the target through surprise, speed, and dissemination. Mark Twain, who died in 1910, has been quoted as saying “A lie can travel halfway around the world before the truth can get its boots on”…Whether he said it or not, it was pre-internet. Now a lie can travel around the world in a blink of an eye.

  According to Huntoon, in a 2009 article entitled "Tactics Characteristic of Sham Peer Review" in the *Journal of American Physicians and Surgeons* states,” the characteristics of sham peer review are “remarkably similar across the country.”[45] He states that “the common feature of these tactics is that they violate due process and/or fundamental fairness, and they often represent an attempt make the incident or event ‘fit the crime.’” Such sham peer tactics include:

  - Ambush Tactic and Secret Investigations
  - Depriving Targeted Physician of Records Needed to Defend Himself
  - Guilty Until Proven Innocent
  - Numerator-Without-Denominator
  - Misrepresenting the Standard of Care
  - Trumped-Up and/or False Charges
  - Abuse of the “Disruptive Physician” Label
  - Dredging Up Old Cases to Justify Summary Suspension
  - Ex-Parte Communications
  - Hospital Attorney or Conflicted Attorney Used to Influence Peer Review Process
  - Bias – Stack Investigative Committee Deck and Use Rumor Mill to Damage Reputations

  When individuals or institutions use computers, networks, or the internet to practice clinical or publication peer review, have they committed a cybercrime? Whether this is technically a legal violation in a given state of the union or not, we believe such behavior is a crime against the ethical standards our patients and caregivers deserve.

  An extremely common ploy by defense attorneys is to discredit a plaintiff or make a caregiver appear to be “the

one bad apple" in order to protect the financial assets of an institution. This is where patient safety leaders need to stand up for the truth. Is this in their wheelhouse? Absolutely.

- **Healthcare Workplace Cyberbullying:** Bullying occurs when a real or perceived imbalance of power is used to impact another individual or organization. Bullying in healthcare is amazingly frequent in terms of patients and families abusing caregivers and healthcare workplace abuse is 5 times more frequent than other sectors according to a 2016 US Government Accounting Office report[46] In the *Joint Commission* 2016 "Bullying Has No Place in Healthcare" report, it recognized five categories of workplace violence.[47]
  - Threat to personal standing (name calling, insults, teasing)
  - Threat to personal standing (name calling, insults, teasing)
  - Isolation (withholding information)
  - Overwork (impossible deadlines)
  - Destabilization (failing to give credit where credit is due)

  The first two of these categories can be weaponized through the use of the internet. Digital technologies have opened a whole new world of bullying of staff and caregivers within an institution and the use of press releases in the community that can serve motives other than the news.

  Take for example the highly publicized case of Kimberly Hiatt, a highly recognized nurse who made a wholly inadvertent medication error that led to the death of a child in Seattle. The dissemination of content from her human resources file strikes at the heart of the first two categories described above. Was it to discredit her in the court of public opinion to reduce financial consequences, was it to make the story more sensational, or was it to bully her to keep quiet regarding circumstances around the death? No one will know for sure. She committed suicide.[48]

  Was it a healthcare cybercrime when nurse Julie Thao's private statement to the hospital regarding the medication error she made that led to a pregnant teenagers' death was transmitted to the local prosecutor? [49, 50] No one is knows for sure because she was fired and without the financial resources to augment a defense, was essentially bullied into accepting a ruinous plea bargain. There is no need to debate the legality of the behavior… the ethics lie directly in the wheelhouse of the patient safety officer who owns the treatment of the second victim of an error.[51]

- **Academic Cyberbullying:**
  Academic bullying occurs when the real or perceived imbalance of power is used to impact another individual's career, professional reputation, or opportunity for advancement. This may occur within an organization to discredit an individual's advancement or may be undertaken by institutions or individuals to discredit a competitive organization or individual. Whether the motives are some combination of jealously, competitive financial incentive, academic competition, or revenge; the internet has become a weapon of mass reputational destruction. Take for example the case of Clayton Christensen, the father of the concept of disruptive innovation and author of "The Innovator's Prescription: A Disruptive Solution for Health Care", a valuable reference to those practicing patient safety and performance improvement.[52] An author who was a fellow Harvard academic blindsided him with an article in the New Yorker challenging the integrity of his research and thought by many to be an assassination of his character. The article was fraught with numerous errors which he described as a criminal act of dishonesty. It was not provided to him ahead of time and published without an opportunity for discussion.[53, 54] The dissemination through the internet was broad and deep and there was no real opportunity to right the wrong.

- **Healthcare Journalism Fraud:**
  The fabrication, falsification, and plagiarism (FFP) model appropriately covers some of the issues of healthcare journalistic fraud. Under the guise of journalistic integrity, sources may purposefully cause intentional omission of information; cite alleged activities that violate the law, or violate ethical rules; alter or stage an event being documented; or make substantial reporting or researching errors with the results leading to libelous or defamatory statements. These strikes at the heart of journalism ethics. Bloggers who have no peer review and little editorial support are now writing pseudo-investigational articles under the brand and banner of major news organizations. These brands often accept no liability for fraudulent work in the fine print of their disclosures, and yet such articles are even being cited in medical journals leading the reader to believe the reference is a legitimate

news or medical source. This is a house of cards being built over a pool of gas. This has happened in the patient safety domain and poses a threat to the trust in medical journals, the press, and safety leaders.[55, 56, 57]

- **Website Fraud and Vandalism:**
  With the advent of democratized websites like Wikipedia, seemingly anonymous editors can gain advantage for secondary interests such as maligning the reputations of people who are competitors. Wikipedia is an internet encyclopedia which is free, collaboratively edited, multilingual, regularly ranked as one of the top 10 websites visited in the world. It's 30 million articles in 287 languages are written collaboratively by volunteers, yet its power lies in integrity – being a source of truth. According to Wikipedia, "vandalism is the act of editing the project in a malicious manner that is intentionally disruptive. Vandalism includes the addition, removal, or other modification of the text or other material that is either humorous, nonsensical, a hoax, or that is of an offensive, humiliating, or otherwise degrading nature.[58] Known patient safety advocates including one the authors of this paper have had their biographies vandalized by competitors and a digital band of muggers. Incredibly, according to the rules of Wikipedia, one cannot correct their own biography, while those with malicious intent can vandalize anyone's biography at will entirely without accountability.

- **The 4 P's - Prevention, Preparedness, Protection, and Performance Improvement:**
  The purpose of this article is make the case for safety and quality leaders to realize that cybercrime is in their purview, however we share brief thoughts regarding the actions they may take. Patient safety leaders and quality leaders have an enormous opportunity to bring the stress tested tools of performance improvement to the new and growing threat of cybercrime. The four "P's" below represent the categories of work that lies in the wheelhouse and domain of safety and quality leaders.

  - **Prevention:** In a narrow view, 'prevention' could mean any activity undertaken to avoid, prevent, or stop a threatened or actual act of cybercrime. A broader view such as one through the lens of public health, one might consider primary prevention (preventing an event from happening), secondary prevention (reducing the harm from an event), and tertiary prevention intended to reverse, arrest, or delay the harmful impact of an incident. Clearly multidisciplinary teams must tackle healthcare cybercrime. Breach and theft may not be in the wheelhouse of patient safety leaders; however prevention of the harm after theft and contamination of medical records is squarely if not fully in the lap of safety officers. Prevention of the harm of an institution's academic leaders and prevention of the impact of harm from dishonest academics and researchers must drive a "trust but verify" philosophy. Widespread support for new federal laws which statutorily criminalize such behavior as well as provide strong civil remedies is needed.
  - **Preparedness:** A good definition for the term "preparedness" is provided by the Department of Homeland Security as "a continuous cycle of planning, organizing, training, equipping, exercising, evaluating, and taking corrective action in an effort to ensure effective coordination during incident response.[59 60]

    Safety and quality leaders certainly can develop strategies, tactics, checklists, and simulation exercises that can prepare an organization for breach, theft, contamination, and harm to medical identities. They can help academic and clinical research leaders improve their state of readiness for competitive attacks on their work and professional identities.
  - **Protection:** This term is of protection can mean shielding an individual, groups, or institutions from injury or harm during an incident. Again, safety and quality leaders have a role in shielding patients, staff, and academics from the harm of an incident of medical record contamination and the harm to their professional teams.
  - **Performance Improvement:** Performance improvement know how and activities can be applied to continuously optimize prevention, preparedness, and protection. The Institute for Healthcare Improvement (IHI) and others have taught us the vital activities of this discipline: measurement, education, skill building, process improvement, and competency verification currency.[61]

THOSE WHO SERVED AND THOSE WE SERVE

The new healthcare cybercrime issues are in the patient safety leader's wheelhouse. Given that one in three Americans will be subject to medical identity breach in 2016 and one in five of them will have medical record contamination, and one in three of those who have contamination may lose their health insurance; we have a crisis. Given one in six peer review events are subject to sham activities, leaders of organizations need to be ready to protect the integrity of their organizations.

These issues pose a threat and harm to those who serve and those we serve.

The pattern of preventable harm to patients, caregivers, authors, and institutions is exploding as rapidly as the evolution of information technology. It is true that it may appear “everyone owns it and no one owns it”, yet our the great patient safety leaders at academic centers and at the frontline who have brought us innovations and sustainable safety in medication management, surgery, hospital acquired conditions, and many other areas do have the knowledge, skill, and grit to help. They can help multidisciplinary teams in prevention, preparedness, protection, and performance improvement.

Caveat emptor, the Latin term mentioned earlier which means “let the buyer beware” will not be the strategy of great healthcare organizations. Great organizations believe their bond with their patients is a sacred trust and will do everything to preserve it.

This is a call to action to act now. If not now, when? If not safety leaders, who? We owe it to those who serve and those we serve.

WORKS CITED

1. Makary M, Daniel M. Medical Error – the third leading cause of death in the US. *The BMJ.* 2016 May 3.
2. TMIT Webinar 09-17-16 Patient Safety Cybercrimes, and TMIT Webinar 01-21-16, HIT Community of Practice.*TMIT* website.
3. Healthcare Cybercrime Classification Report. *TMIT* 2016 http://www.globalpatientsafetyforum.org/pdf/Healthcare%20Cybercrime%20Classification%20Report,%20TMIT%202016.pdf
4. Friauf B. Confronting the problem of medical errors at Patient Safety Summit. *UNT Health Science Center Newsroom*. 2015 Oct 19.Source: https://www.unthsc.edu/newsroom/story/confronting-the-problem-of-medical-errors-at-patient-safety-summit/
5. ONC. Report on health information blocking. Report to Congress. Washington, DC: *Office of the National Coordinator for Health Information Technology (ONC), Department of Health and Human Services.* 2015 Apr. Available at https://www.healthit.gov/sites/default/files/reports/info_blocking_040915.pdf
6. FDASIA Committee Report. Health IT Policy Committee: Recommendations to the National Coordinator for Health IT web page. 2014 Feb 20. Available at http://www.healthit.gov/sites/faca/files/FDASIARecommendationsFinal.pdf
7. Tahir D. Feds criticized for lax oversight of health IT. *Modern Healthcare.* 2015 Apr 4. Available at http://drupal.prod.modernhealthcare.com/article/20150404/MAGAZINE/304049988/feds-criticized-for-lax-oversight-of-health-it
8. Healthcare Cybercrime Classification Table. *TMIT.* 2016 Available at: http://www.globalpatientsafetyforum.org/pdf/Healthcare%20Cybercrime%20Classification%20Report,%20TMIT%202016.pdf
9. BBC Technology. Sarkozy to host key internet forum ahead of G8 summit. *BBC.* 2011 May 24. Source: http://www.bbc.com/news/world-europe-13513958
10. Palermo E. 10 Worst Data Breaches of all Time. *Tom’s Guide*. 2015 Feb 6.
11. Palermo E. 10 Worst Data Breaches of all Time. *Tom’s Guide*. 2015 Feb 6.
12. Palermo E. 10 Worst Data Breaches of all Time. *Tom’s Guide*. 2015 Feb 6.
13. Levin A. 5 Identity Theft Facts That Will Terrify You. *ABC News*. 2015 May 24. https://abcnews.go.com/Business/identity-theft-facts-terrify/story?id=31223144
14. Pascual A. 2015 Identity Fraud: Protecting Vulnerable Populations. *U.S. Department of Justice, Javelin Strategy & Research.* 2015 Mar 2.
15. Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data. *Ponemon Institute LLC*. May 2016. http://lpa.idexpertscorp.com/acton/attachment/6200/f-04aa/1/-/-/-/-/Resources%20-%20Sixth%20Annual%20Benchmark%20Study%20on%20Privacy%20and%20Security%20of%20Healthcare%20Data%20.pdf
16. Fair Credit Reporting Act: 15 U.S.C Section 1681. 2012 Sep. https://www.consumer.ftc.gov/articles/pdf-0111-fair-credit-reporting-act.pdf
17. Javelin. 13.1 million identity fraud victims but less stolen in 2015, according to Javelin. Press release. Pleasanton (CA): *Javelin Strategy & Research.* 2016 Feb 2. Available at https://www.javelinstrategy.com/press-release/131-million-identity-fraud-victims-less-stolen-2015-according-javelin
18. Munro D. Data Breaches In Healthcare Totaled Over 112 Million Records In 2015. *Forbes.* 2015 Dec 31. https://www.forbes.com/sites/danmunro/2015/12/31/data-breaches-in-healthcare-total-over-112-million-records-in-2015/#4634f28a7b07

19. Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data. *Ponemon Institute LLC*. May 2016. http://lpa.idexpertscorp.com/acton/attachment/6200/f-04aa/1/-/-/-/-/Resources%20-%20Sixth%20Annual%20Benchmark%20Study%20on%20Privacy%20and%20Security%20of%20Healthcare%20Data%20.pdf

20. Winton R. Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating. *Los Angeles Times.* 2016 Feb 18. http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html

21. Ornstein C. Celebrities' Medical Records Tempt Hospital Workers To Snoop. *NPR*. 2015 Dec 10. http://www.npr.org/sections/health-shots/2015/12/10/458939656/celebrities-medical-records-tempt-hospital-workers-to-snoop

22. Armour S. How identity theft sticks you with hospital bills. The *Wall Street Journal* 2015 Aug 7. Available at http://www.wsj.com/articles/how-identity-theft-sticks-you-with-hospital-bills-1438966007

23. Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data. *Ponemon Institute LLC.* May 2016. http://lpa.idexpertscorp.com/acton/attachment/6200/f-04aa/1/-/-/-/-/Resources%20-%20Sixth%20Annual%20Benchmark%20Study%20on%20Privacy%20and%20Security%20of%20Healthcare%20Data%20.pdf

24. Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data. *Ponemon Institute LLC.* May 2015. http://medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_Theft_Study1.pdf

25. Pollack D. Is medical identity theft really a problem? *ID Experts website.* 2015 Aug 17. Available at https://www2.idexpertscorp.com/blog/single/is-medical-identity-theft-really-a-problem

26. Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data. *Ponemon Institute LLC*. May 2015. http://medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_Theft_Study1.pdf

27. Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data. *Ponemon Institute LLC.* May 2015. http://medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_Theft_Study1.pdf

28. Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data. *Ponemon Institute LLC.* May 2015. http://medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_Theft_Study1.pdf

29. Hitler A, Murphy J (trans.). *Mein Kampf.* London: Hurst and Blackett; 1943. Available at http://greatwar.nl/books/meinkampf/meinkampf.pdf

30. KPMG. 81% of healthcare organizations have been compromised by cyber-attacks in past 2 years: KPMG survey. Press Release. New York (NY): *KPMG LLP*. 2015 Aug 26. Available at http://bit.ly/1LzhkTK [Bell G, Ebert M. Health care and cy-ber security: Increasing threats require increased capabilities. New York (NY): KPMG LLP; 2015.] Available at http://www.kpmg-institutes.com/institutes/healthcare-life-sciences-institute/articles/2015/08/health-care-and-cyber-security.html

31. [No authors listed.] Catch Me If You Can. *Wikipedia.com*. Web. Available at https://en.wikipedia.org/wiki/Catch_Me_If_You_Can

32. CSLEA. Operation Safe Medicine: Our CSLEA members at work. Sacramento (CA). *California Statewide Law Enforcement Association*. 2012 Nov 13.

33. Mosbergen D. Accused fake 'teen doctor' Malachi Love-Robinson arrested again. *HuffPost Crime website.* 2016 Mar 3. Available at http://www.huffingtonpost.com/entry/malachi-love-robinson-arrested-again_us_56d7e0b2e4b0000de4036dc7

34. Acevedo J, Netto J. 18-year-old arrested for pretending to be a doctor, police say. *CNN.com.* 2016 Feb 17. Available at http://www.cnn.com/2016/02/17/health/florida-palm-beach-teen-doctor-arrest/

35. Marchione M. Fake doctor Duped Hospitals, Universities, AMA. *NBCNews.com website.* 2010 Dec 12. Available at http://www.nbcnews.com/id/40630166/ns/health-health_care/#.VuHfib8sBXt

36. [No authors listed.] "William Hamman." *Wikipedia.com*. Web. Available at https://en.wikipedia.org/wiki/William_Hamman [Carolla K, ABC News Medical Unit. Cardiologists 'shocked' that William Hamman passed himself off as doctor. *ABCNews*.go.com website 2010 Dec 15. Available at https://abcnews.go.com/Health/MindMoodNews/fake-cardiologist-william-hamman-duped-real-doctors/story?id=12395288

37. Seife C. Research misconduct identified by the US Food and Drug Administration: out of sight, out of mind, out of the peer-reviewed literature. *JAMA*. 2015 Apr. http://www.ncbi.nlm.nih.gov/pubmed/25664866

38. Sarwar U, Nicolaou M. Fraud and deceit in medical research. *J Res Med Sci.* 2012 Nov; 17(11): 1077–1081.

39. Fang FC, Steen RG et al. Misconduct accounts for the majority of retracted scientific publications. Proceedings of the *National Academy of Sciences of the United States of America.* 2012 Sep 6. Source: http://www.pnas.org/content/109/42/17028.full

40. Parmley WW. Clinical peer review or competitive hatchet job. *J Am Coll Cardiol.* 2000; 36: 1-2 [DOI: 10.1016/S0735-1097(00)01032-9]

41. Pfifferling JH, Meyer DN, Wang CJ. Sham peer review: perversions of a powerful process. *Physician Exec.* 2008; 34: 24-29 [PMID: 19456073]: *Wikpedia* on Sham Peer Review: https://en.wikipedia.org/wiki/Sham_peer_review#cite_note-AMA-2

42. Goldberg BA. The peer review privilege: a law in search of a valid policy. *Am J Law Med.* 1984; 10: 151-167 [PMID: 6528878]

43. [No authors listed.] "Clinical peer review." *Wikipedia.com*. Web. Available at https://en.wikipedia.org/wiki/Clinical_peer_review [Edwards MT, Benjamin EM. The process of peer review in U.S. hospitals. *Journal of Clinical Outcomes Management.* 2009 Oct;16(10):461-7.] Available at http://www.turner-white.com/pdf/jcom_oct09_peer.pdf

44. [No authors listed.] "Peer review." *Merriam-Webster.com*. Web. Available at https://www.merriam-webster.com/dictionary/peer%20review

45. Huntoon LR. Tactics characteristic of sham peer review. Journal of American Physicians and Surgeons 14(3);2009 Fall. Available at www.jpands.org/vol14no3/huntoon.pdf

46. US Government Accountability Office. Workplace Safety And Health: Additional Efforts Needed to Help Protect Health Care Workers from Workplace Violence. *GAO.* 2016 Mar.

47. Quick Safety: Bullying Has No Place In Healthcare. *Joint Commission:* 2016 Jun.
Source: https://www.jointcommission.org/assets/1/23/Quick_Safety_Issue_24_June_2016.pdf

48. Aleccia J. Nurse's suicide highlights twin tragedies of medi-cal errors. *NBCNews.com.* 2011 Jun 27. Source: http://www.nbcnews.com/id/43529641/ns/health-health_care/t/nurses-suicide-highlights-twin-tragedies-medical-errors

49. Denham CR. TRUST: The 5 Rights of the Second Victim. *J Patient Saf.* 2007 June. Source: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.516.157&rep=rep1&type=pdf
Leape L. Who's to Blame? J Patient Safety, April 2010 Volume 36 Number 4.

50. Wu A. Medical error: the second victim. The doctor who makes mistakes needs help too. *BMJ.* 2000;320:726Y727.

51. Christensen CM, Grossman JH et al. *The Innovator's Prescription: A Disruptive Solution for Health Care*. McGraw-Hill Education: 2008 Dec 25.

52. Lepore J. The Disruption Machine, what the gospel of innovation gets wrong. *The New Yorker*. 2014 Jun 23. http://www.newyorker.com/magazine/2014/06/23/the-disruption-machine

53. Bennett D. Clayton Christensen Responds to New Yorker Takedown of 'Disruptive Innovation'. *Bloomberg*. 2014 Jun 21. Source: https://www.bloomberg.com/news/articles/2014-06-20/clayton-christensen-responds-to-new-yorker-takedown-of-disruptive-innovation

54. Millenson M. The Money, the MD and a $12 Million Patient Safety Scandal. *Forbes*. 2014 Mar 8. http://www.forbes.com/sites/michaelmillenson/2014/02/14/the-money-the-md-and-a-12-million-patient-safety-scandal/

55. No Authors Listed]. Qualitygate: The Quality Movement's First Scandal. *Southwest Journal of Pulmonary and Critical Care.* 2014 Feb 24.
http://www.swjpcc.com/editorials/2014/2/24/qualitygate-the-quality-movements-first-scandal.html

56. Forbes Fact Check Review Report, 2016 http://safetyleaders.org/disclosures/Forbes%20Fact%20Check%20Review%20Report%202016.pdf

57. [No authors listed.] "Vandalism on Wikipedia." *Wikipedia.com*. Web. Available at https://en.wikipedia.org/wiki/Vandalism

58. Plan and Prepare for Disasters, *DHS/FEMA*. Source: https://www.dhs.gov/topic/plan-and-prepare-disasters

59. Plan and Prepare for Disasters, *DHS/FEMA*. https://www.dhs.gov/plan-and-prepare-disasters

60. Institute for Healthcare Improvement website: http://www.ihi.org/Pages/default.aspx

61. Institute for Healthcare Improvement website: http://www.ihi.org/Pages/default.aspx