HEALTHCARE CYBERCRIME AND HARM CLASSIFICATION 2017
TMIT MODEL 03-08-17

This model provides and evidence based classification intended for use by healthcare leaders to support prevention of cyber-harm, preparedness in case of an incident, protection during an incident, and performance improvement after a harmful or potentially harmful event. The goal is to reduce the impact of cybercrime and cyber-harm on the people who are served and the people who serve at healthcare institutions.

Background:

- The frequency and severity of healthcare cybercrime and cyber-harm is expanding at such a great rate that best practices in management of these threats are lagging behind.
- A set of working definitions is helpful to classify the evidence and help provide focus to practitioners, researchers, and academics.
- The Texas Medical Institute of Technology (TMIT) has drawn on a National Research Test Bed of more than 3,100 healthcare institutions, more than 100 collaborative webinars, and a resource base of 500 subject matter experts to study threat safety issues and develop such models.

Research and Development:

- More Threat Safety Science Solutions research and development must be undertaken in the area of cybercrime and cyber-harm impacting the *Medical Identity* of patients and the *Professional Identity* of caregivers and academics. Cybercrime and cyber-harm both represent the personal property of individuals and the protection and validation of them directly impacts healthcare institutions.

Use:

- This model provides operational definitions. Grounded in legal vernacular and tied to evidence-based medicine, these definitions allow researchers and authors to have standardization in their work.
- As solutions in threat safety are developed in leadership, practices and technologies; they can be tied to a standardized uniform language that will periodically be updated as more is known.

Future:

- This classification will be periodically updated as the evidence in healthcare information technologies evolves. The law and what becomes defined as a crime naturally evolves later. The collaborative fusion of medicine, security, law enforcement, and legal disciplines provides improved opportunities to protect those we serve and those who serve.
- This classification will be updated quarterly or more frequently as necessary by Texas Medical Institute of Technology, Austin Texas. Contact Kyle Kemp at Kyle_Kemp@tmit1.org for questions.
- Suggested citation: TMIT Press. Healthcare Cybercrime and Harm Classification 2017. *TMIT Press.* 2017 Mar 8.

Healthcare Cybercrime Classification 2016			
Cybercrime or Cyber-harm	**Type**	**Definitions**	**Examples and Citations**
	Cybercrime, **Unethical Cyber-Behavior,** **And** **Cyber-harm**	**Cybercrime:** An act that harms individuals or organizations using computers, communication networks, and or the internet that the law makes punishable; the breach of a legal duty treated as the subject-matter of a criminal proceeding. * **Unethical Cyber-behavior:** An act that is not in conformity with moral norms or standards of professional conduct that may harm individuals or organizations using computers, communication networks, and or the internet can be considered Unethical Cyber-behavior. * **Cyber-harm:** An act undertaken by an individual or organization through the use of computers, communication networks, and or the internet that causes injury, loss, damage that is material or tangible detriment to and individual or organization. Cyber-harm may be a cybercrime when the law makes it punishable; the breach of a legal duty treated as the subject-matter of a criminal proceeding. * * *Thompson Reuters Black's Law Dictionary, 5th Edition* 1996	The use of digital technologies including computers, communications networks, and the internet are relatively recent developments and as such the law and common use of terminology is evolving. Certain legal definitions and terms in common use are helpful to understand the continuum of cyber-harm. The following definitions are taken from *Thompson Reuters Black's Law Dictionary, 5th Edition* 1996. They include: • **Crime:** An act that the law makes punishable; the breach of a legal duty treated as the subject-matter of a criminal proceeding. • **Computer Crime:** A crime involving the use of a computer, such as sabotaging or stealing electronically stored data. • **Unethical:** Not in conformity with moral norms or standards of professional conduct. • **Harm:** Injury, loss, damage; material or tangible detriment. • **Falsify:** To make deceptive; to counterfeit, forge, or misrepresent, to tamper with (a document, record, etc.) by interlineation, obliteration, or some other means. • **Falsifying a Record:** The crime of making false entries or otherwise tampering with a public record with the intent to deceive or to conceal wrongdoing. • **Fraud: 1.**A knowing misrepresentation or knowing concealment of a material fact made to induce another to act to his or her detriment. Fraud is usually a tort, but in some cases (esp. when the conduct is willful) it may be a crime. **2.** A reckless misrepresentation made without justified belief in its truth to induce another person to act. **3.** A tort arising from a knowing or reckless misrepresentation or concealment of material fact made to induce another to act to his or her detriment. **4.** Unconscionable dealing; esp., in contract law, the unfair use of the power arising out of the parties' relative positions and resulting in an unconscionable bargain. • **Counterfeit:** To unlawfully forge, copy, or imitate an item, esp. money or a negotiable instrument (such as a security or promissory note) or other officially issued item of value (such as a postage stamp or a food stamp), or to possess such an item without authorization and with the intent to deceive or defraud by presenting the item as genuine. *Thompson Reuters. Black's Law Dictionary, 5th Edition. West Publishing Co: 1996.* • **Libel:** A written or oral defamatory statement or representation that conveys an unjustly unfavorable impression by **1.** a statement or representation published without just cause and tending to expose another to public contempt **2.** defamation of a person by written or representational means **3.** the publication of blasphemous, treasonable, seditious, or obscene writings or pictures **4.** the act, tort, or crime of publishing such a libel http://www.merriam-webster.com/dictionary/libel • **Slander:** slander, n. (13c) A defamatory assertion expressed in a transitory form, esp. speech; esp., false and defamatory words that are said in reference to another, such as those charging criminal conduct, imputing a horrible or loathsome disease, alleging malfeasance or incompetence in reference to the person's professional responsibilities, or otherwise causing special damage to the person's reputation. • **Defamation: 1.** Malicious or groundless harm to the reputation or good name of another by the making of a false statement to a third person. If the alleged defamation involves a matter of public concern, the plaintiff is constitutionally required to prove both the statement's falsity and the defendant's fault. **2.** A false written or oral statement that damages another's reputation. • **Misconduct:** A dereliction of duty; unlawful, dishonest, or improper behavior, especially by someone in a position of authority or trust.

Healthcare Cybercrime Classification 2016			
Cybercrime or Cyber-harm	**Type**	**Definitions**	**Examples and Citations**
	Cybercrime, Unethical Cyber-Behavior, And Cyber-harm	**Cyber-harm, continued**	Other commonly used references outside of the legal domain are also helpful: • **Cybercrime:** Computer crime, or cybercrime, is crime that involves a computer and a network**.** Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)" Wikipedia " https://en.wikipedia.org/wiki/Cybercrime • **Cybercrime:** criminal activity (such as fraud, identity theft, or distribution of child pornography) committed electronically using a computer especially to illegally access, alter, or manipulate data (Merriam-Webster) CITE: http://www.merriam-webster.com/dictionary/cybercrime • **Cyber-attack:** Any type of offensive maneuver employed by individuals or whole organizations that targets computer information systems, infrastructures, computer networks, and/or personal computer devices by various means of malicious acts usually originating from an anonymous source that either steals, alters, or destroys a specified target by hacking into a susceptible system. These can be labeled as either a cyber campaign, cyberwarfare or cyberterrorism in different context. https://en.wikipedia.org/wiki/Cyber-attack
Identity Cybercrime or Cyber-harm	**Identity Breach**	**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. The actors who may undertake breach events are part of the *Cyber Threat Source Descriptions* used by the government and include: national governments, terrorists, industrial spies, organized crime groups, hacktivists, and hackers. Activities can include espionage, hacking, identity theft, crime, and terrorism. SEE: https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions	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. 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. Palermo E. 10 Worst Data Breaches of all Time. *Tom's Guide*. 2015 Feb 6. http://www.tomsguide.com/us/biggest-data-breaches,news-19083.html Legal definitions of "breach" are helpful to understand the nature of the term. The following definitions are taken from *Thompson Reuters Black's Law Dictionary, 5th Edition* 1996. They include: • **Breach of Confidence (legal definition): 1.** The disclosure of confidential information such as trade secrets or information that is privileged because of a relationship of trust, such as matters that a client shares in confidence with a legal representative **2.** A claim or lawsuit against someone who has received confidential information and then used or disclosed it in a manner contrary to the purpose for which it was originally disclosed (The information must not be in the public domain, must have been disclosed to the recipient in circumstances implying confidence, and must have been misused.) *Thompson Reuters. Black's Law Dictionary, 5th Edition. West Publishing Co: 1996.* • **Breach of Loyalty (legal definition):** An act that is detrimental to the interests of someone to whom a fiduciary duty is owed; esp., an act that furthers the actor's own interests or those of a competitor of the beneficiary. *Thompson Reuters. Black's Law Dictionary, 5th Edition. West Publishing Co: 1996.*

Healthcare Cybercrime Classification 2016			
Cybercrime or Cyber-harm	**Type**	**Definitions**	**Examples and Citations**
Identity Cybercrime	**Identity Theft**	**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.	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. 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. Palermo E. 10 Worst Data Breaches of all Time. *Tom's Guide*. 2015 Feb 6. http://www.tomsguide.com/us/biggest-data-breaches,news-19083.html Certain legal definitions are helpful to understand Identity Theft. The following definitions are taken from *Thompson Reuters Black's Law Dictionary, 5th Edition* 1996. They include: • **Cyber-theft:** The act of using an online computer service, such as one on the internet, to steal someone else's property or to interfere with someone else's use and enjoyment of property. • **Theft: 1.** The wrongful taking and removing of another's personal property with the intent of depriving the true owner of it; larceny. **2.** Broadly, any act or instance of stealing, including larceny, burglary, embezzlement, and false pretenses. *Thompson Reuters. Black's Law Dictionary, 5th Edition. West Publishing Co: 1996.*
	Identity Counterfeit	**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. Thieves who have obtained, stolen, or purchased financial and credit card information typically misrepresent themselves as another individual and obtain products, services, or turn the information into cash. Identity Counterfeit cybercrimes may be undertaken to defraud vendors when individuals create a new identity or assume the identity of someone else to illegally obtain value. When with the richness of medical information, is added to financial and credit card information, thieves can apply for more	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. Levin A. 5 Identity Theft Facts That Will Terrify You. *ABC News*: 2015 May 24. http://abcnews.go.com/Business/identity-theft-facts-terrify/story?id=31223144 The legal definition of "counterfeit" is helpful to understand an identity counterfeit cybercrime. The following definition is taken from *Thompson Reuters Black's Law Dictionary, 5th Edition* 1996: • **Counterfeit (legal definition):** To unlawfully forge, copy, or imitate an item, esp. money or a negotiable instrument (such as a security or promissory note) or other officially issued item of value (such as a postage stamp or a food stamp), or to possess such an item without authorization and with the intent to deceive or defraud by presenting the item as genuine. *Thompson Reuters. Black's Law Dictionary, 5th Edition. West Publishing Co: 1996.*

Healthcare Cybercrime Classification 2016			
Cybercrime or Cyber-harm	**Type**	**Definitions**	**Examples and Citations**
	Identity Counterfeit	credit, obtain significant spoils, and even submit fraudulent tax returns for direct reimbursement from the federal government. They can create great damage to the unsuspecting public.	
Identity Cybercrime	**Identity Contamination and Vandalism**	**Identity Contamination:** 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. As soon as such 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. **Identity Vandalism:** When an individual, individuals, or organizations harm the personal identity of individual using computers, communication networks, or the internet, the damage may be described as Identity Vandalism. This may be perpetrated by disgruntled former employees, competitors, and people who perceived they have been wronged want to harm someone else.	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. Pascual A. 2015 Identity Fraud: Protecting Vulnerable Populations *U.S. Department of Justice, Javelin Strategy & Research*. 2015 Mar 2. The definition of "contamination" and legal definition of "vandalism" are helpful to understand the nature of cybercrimes in this area. • **Contamination** is a process of contaminating: a state of being contaminated. To Contaminate is to soil, stain, corrupt, or infect by contact or association, to make inferior or impure by admixture, to make unfit for use by the introduction of unwholesome or undesirable elements **http://www.merriam-webster.com/dictionary/contamination** • **Vandalism*: 1.** Willful or ignorant destruction of public or private property, especially of artistic, architectural, or literary treasures. **2.** The actions or attitudes of one who maliciously or ignorantly destroys or disfigures public or private property; active hostility to anything that is venerable or beautiful.* Legal definition of "vandalism" is taken from *Thompson Reuters Black's Law Dictionary, 5th Edition* 1996.
	Medical Identity Breach	**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. Like personal identity breach including financial data, medical identity breach can occur through the same actors defined in the government's Cyber Threat Source Descriptions and include: national governments, terrorists, industrial spies,	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. Source: 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

Healthcare Cybercrime Classification 2016			
Cybercrime or Cyber-harm	**Type**	**Definitions**	**Examples and Citations**
		organized crime groups, hacktivists, and hackers. Activities can include espionage, hacking, identity theft, crime, and terrorism. SEE: https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions	
Medical Identity Cybercrime	**Medical Identity Theft**	**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. Thieves who have obtained, stolen, or purchased medical identity information will also likely obtain financial and credit card information. As with personal or financial identity theft, thieves who use the information can misrepresent themselves as the victim and obtain products, services, or turn the information into cash. .	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. Although criminal attacks are 5 Munro D. Data Breaches In Healthcare Totaled Over 112 Million Records In 2015. *Forbes:* 2015 Dec 31. *http://www.forbes.com/sites/danmunro/2015/12/31/data-breaches-in-healthcare-total-over-112-million-records-in-2015/#59ca18307fd5* 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?sid=TV2:3o5EMagob 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 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. 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** • "Almost half of medical identity theft (47%) occurs when a family member takes a relative's health insurance card or other ID—or when people knowingly share their health information or IDs with someone they know." • "In the Anthem hack of 2015, about 70 million records were reportedly stolen." • "An estimated 2.3 million cases [of medical identity theft] identified in 2014, a number that's up almost 22 percent from the year before." Source: Andrews M. The Rise of Medical Identity Theft. Consumer Reports. 2016 Aug 25. Available at: http://www.consumerreports.org/medical-identity-theft/medical-identity-theft/
Medical Identity Cybercrime	**Medical Identity Counterfeit**	**Medical Identity 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	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 hospitals of services. Amazingly, numerous individuals have even undergone complex surgical procedures requiring many days of hospitalization

Healthcare Cybercrime Classification 2016			
Cybercrime or Cyber-harm	**Type**	**Definitions**	**Examples and Citations**
	Medical Identity Counterfeit	unethical behavior may be described as Medical Identity Counterfeit. Thieves who have stolen or purchased financial and credit card information can combine it with the richness of medical information and can apply for credit, submit tax returns, obtain products, services, or turn the information into cash. This can create enormous harm and loss to unsuspecting patients and families.	using stolen identities including organ transplants and even elective surgery such as penile implant procedures. 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 Identity Contamination, Harm, and Vandalism	**Medical Identity Contamination:** 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. Once enough information is obtained that can be used to convert personal and medical information to the benefit of thieves, they are on the way to contaminating the credit, financial records, and causing harm that may be irreparable.	Sixty-five percent of medical identity theft victims in the 2015 Ponemon Institute report had to pay an average of $13,453.38 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 imposters. 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. 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. 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?sid=TV2:3o5EMagob In 2016 there were 55 breaches in the Medical/Healthcare category. 15,426,015 records were exposed, and these breaches comprised 36.2% of all 2016 data breaches. Identity Theft Resource Center. 2016 Data Breach Category Summary. IDT911. 2016 Dec 13. Page 4 (page 5 of PDF). http://www.idtheftcenter.org/images/breach/2016/DataBreachReport_2016.pdf
	Healthcare Professional Identity Breach	**Healthcare Professional Identity Breach:** A cyber-attack using computers, communication networks, or the internet to gain unauthorized access to a healthcare professional's professional information without known or apparent use of the data is Professional Identity Breach. It is unknown	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. 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.

Healthcare Cybercrime Classification 2016			
Cybercrime or Cyber-harm	**Type**	**Definitions**	**Examples and Citations**
Healthcare Professional Identity Cybercrime		how many pure professional identity breach and theft occurrences have happened and are happening.	According to KPMG in a 2015 report, 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 cyber security: Increasing threats require increased capabilities. New York (NY): KPMG LLP; 2015.] Available at http://advisory.kpmg.us/content/dam/kpmg-advisory/PDFs/ManagementConsulting/2015/KPMG-2015-Cyber-Healthcare-Survey.pdf.]
	Healthcare Professional Identity Theft	**Professional Identity Theft:** A cybercrime whereby the healthcare professional 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. Healthcare professional identity breach of information systems must occur or professional identity information must be acquired through hardware that is accessed without breaching healthcare information systems. When thieves couple healthcare professional provider identity information with payer numbers, the combination can be used to submit fraudulent claims to insurers. Such claims are on the rise.	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. 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 . 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.
Healthcare Professional Identity Cybercrime	**Healthcare Professional Identity Counterfeit**	**Identity Counterfeit:** When an individual or organization unlawfully forge, copy, or imitate the healthcare professional identity of an individual using computers, communications networks, or the internet; the cybercrime may be described as Professional Identity Counterfeit. Non-caregivers can use a real caregiver's professional identity information and deliver care, write prescriptions, and order tests which are paid for by healthcare payers. Individuals with illegal or unethical intent may create counterfeit credentials in order to advance their professional careers. With the advent of the internet, professional counterfeit of invented identities is easier.	William Hamman, an airline pilot 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 fraud. His fraudulent intent was discovered 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. 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. 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. [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.] [[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

Healthcare Cybercrime Classification 2016			
Cybercrime or Cyber-harm	**Type**	**Definitions**	**Examples and Citations**
Healthcare	**Healthcare Professional Identity Counterfeit**	**Identity Counterfeit, continued**	doctor. ABCNews.go.com website 2010 Dec 15. Available at http://abcnews.go.com/Health/MindMoodNews/fake-cardiologist-william-hamman-duped-real-doctors/story?id=12395288.] Another example is of a 18-year-old who not only masqueraded as a doctor, but even convinced an investor to develop a full-blown clinic by providing computer-generated transcripts and credentials. 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 . 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.]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/.
	Healthcare Professional Identity Contamination, Harm, and Vandalism:	**Professional Identity Contamination:** The professional identity of legitimate healthcare professionals can be both intentionally and unintentionally harmed by their employers, collaborators, colleagues, and competitors using computers, communication networks, and the internet. The instigators may be within the institution where the healthcare professional is employed/ affiliated or outside them. The internet has provided a force multiplier to the harm of such contamination because it is permanent, searchable, and promotes replication without authentication. Intentional harm may be perpetrated by disgruntled former employees, competitors, and people who perceived they have been wronged want to harm someone else. Unintentional distribution of false or defamatory information about a healthcare professional may be undertaken and generate unintentional harm when those who copy or cite information are unaware that it is false or misleading.	Examples of intentional harm to a professional identity include: • Clinical Trials Misconduct • Fraudulent Healthcare Publication • Sham Peer Review • Healthcare Workplace Bullying • Academic Cyberbullying • Healthcare Journalism Fraud • Website Fraud and Vandalism Certain legal and general definitions and citations are helpful to address Healthcare Professional Identity Contamination, Harm, and Vandalism: • **Fraud:** Fraud may be defined as wrongful or criminal deception intended to result in financial or personal gain. This can occur when someone edits another person's biography on a website such as Wikipedia. • **The FFP Model of U.S. Office of Integrity:** The definition of unethical behavior of the "FFP" (fabrication, falsification, and plagiarism) model put forth by the United States Office of Integrity has applicability to cybercrimes of a person or thing intended to deceive others, typically by unjustifiably claiming or being credited with accomplishments or qualities. • **Libel:** To meet the Supreme Court's definition of libel involving a public figure, a quotation must not only be made up or materially altered. It must also defame the person quoted, and damage his or her reputation or livelihood https://www.google.com/#q=Liebel+definition • **Defamation:** The communication of a false statement that harms the reputation of an individual person, business, product, group, government, religion, or nation. (LeRoy Miller, Roger (2011). Business Law Today: The Essentials. United States: South-Western Cengage Learning. p. 127. ISBN 1-133-19135-5).

Healthcare Cybercrime Classification 2016			
Cybercrime or Cyber-harm	**Type**	**Definitions**	**Examples and Citations**
Healthcare Professional Identity Cybercrime	**Healthcare Professional Identity Contamination, Harm, and Vandalism:**	**Clinical Trials Misconduct:** Misconduct related to clinical trials and contamination of the resulting publications is Clinical Trials Misconduct. The FDA is very well aware of such misconduct. 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 . 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
		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. It uses the definition of unethical behavior of the "FFP" (fabrication, falsification, and plagiarism) model put forth by the United States Office of Integrity to define fraud.	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 . 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. Sarwar U, Nicolaou M. Fraud and deceit in medical research. J Res Med Sci. 2012 Nov; 17(11): 1077–1081.
Healthcare Professional Identity Cybercr Healthcare Professional Identity Cybercrime		**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. Both the process of clinical peer review of a caregiver's behavior and peer review of publications can be corrupted process. *Physician Exec* 2008; 34: 24-29 [PMID: 19456073] CITE: https://en.wikipedia.org/wiki/Sham_peer_review#cite_note-AMA-2	Sham clinical peer review is thought to represent 10-15% of peer review events. 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. 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] Pfifferling JH, Meyer DN, Wang CJ. Sham peer review: perversions of a powerful 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." 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

Healthcare Cybercrime Classification 2016			
Cybercrime or Cyber-harm	**Type**	**Definitions**	**Examples and Citations**
		Sham Peer Review, continued	▪ 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 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.]
Healthcare Professional Identity Cybercrime	**Healthcare Professional Identity Contamination, Harm, and Vandalism:**	**Healthcare Workplace Bullying:** Bullying occurs when a real or perceived imbalance of power is used to impact another individual or organization. Bullying may not be classically described as a crime, however it is increasingly being found to be a precipitating factor. Cyberbullying occurs when a computer, communication network, or the internet is used to generate impact on an individual or institution.	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. In the Joint Commission 2016 *Bullying has no place in healthcare* report, it recognized five categories of workplace violence: US Government Accountability Office. Workplace Safety And Health: Additional Efforts Needed to Help Protect Health Care Workers from Workplace Violence. *GAO*. 2016 Mar. According to the 2016 report by the Joint Commission, workplace bullying (also referred to as lateral or horizontal violence) is repeated, health-harming mistreatment of one or more persons (the targets) by one or more perpetrators. *Bullying is abusive conduct that takes one or more of the following forms:* • *Verbal abuse* • *Threatening, intimidating or humiliating behaviors (including nonverbal)* • *Work interference – sabotage – which prevents work from getting done3* *There are five recognized categories of workplace violence:4* • *Threat to professional status (public humiliation)* • *Threat to personal standing (name calling, insults, teasing)* • *Isolation (withholding information)* • *Overwork (impossible deadlines)* • *Destabilization (failing to give credit where credit is due)* *In the scientific literature, several types of bullying have been studied: intimidation, harassment, victimization, aggression, emotional abuse, and psychological harassment or mistreatment at workplace, among others.5* 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 Workplace Bullying Institute. The Healthy Workplace Campaign. Healthy Workplace Bill website (accessed May 14, 2016) Rayner C and Hoel H. A summary review of literature relating to workplace bullying. Journal of Community & Applied Social Psychology, 1997;7:181-191 The publicized case of Kimberly Hiatt, a highly recognized nurse who made a wholly inadvertent

Healthcare Cybercrime Classification 2016			
Cybercrime or Cyber-harm	**Type**	**Definitions**	**Examples and Citations**
Healthcare Professional Identity Cybercrime	**Healthcare Professional Identity Contamination, Harm, and Vandalism:**	**Healthcare Workplace Bullying, continued**	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 . 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 ? 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 . Aleccia J. Nurse's suicide highlights twin tragedies of medical errors. NBCNews.com: 2011 Jun 27. http://www.nbcnews.com/id/43529641/ns/health-health_care/t/nurses-suicide-highlights-twin-tragedies-medical-errors/ 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.
		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. **Cyberbullying (legal definition)*:** The abuse, coercion, harassment, or threatening of another person through electronic media *Thompson Reuters. Black's Law Dictionary, 5th Edition. West Publishing Co: 1996.* *	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. 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. The dissemination through the internet was broad and deep and there was no real opportunity to right the wrong. Christensen CM, Grossman JH et al. *The Innovator's Prescription: A Disruptive Solution for Health Care.* McGraw-Hill Education: 2008 Dec 25. 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 Bennett D. Clayton Christensen Responds to New Yorker Takedown of 'Disruptive Innovation'. *Bloomberg*. 2014 Jun 21. http://www.bloomberg.com/news/articles/2014-06-20/clayton-christensen-responds-to-new-yorker-takedown-of-disruptive-innovation
		Healthcare Journalism Fraud: Under the guise of journalistic integrity, sources may purposefully cause intentional	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

Healthcare Cybercrime Classification 2016			
Cybercrime or Cyber-harm	**Type**	**Definitions**	**Examples and Citations**
Healthcare Professional Identity Cybercrime	**Healthcare Professional Identity Contamination, Harm, and Vandalism:**	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. The U.S. Office of Integrity definition of unethical behavior of the "FFP" (fabrication, falsification, and plagiarism) model has applicability to healthcare journalism.	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. 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/ [1]No Authors Listed]. Qualitygate: The Quality Movement's First Scandal. *Southwest Journal of Pulmonary and Critical Care*. 2014 Feb 24. http://www.swjpcc.com/editorial/2014/2/24/qualitygate-the-quality-movements-first-scandal.html [1] Forbes Fact Check Review Report, 2016 http://www.safetyleaders.org/disclosures/Forbes%20Fact%20Check%20Review%20Report%202016.pdf
		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. Vandalism is the action involving deliberate destruction of or damage to public or private property. The terms fraud, vandalism, libel, slander, and defamation all have new impact due to the enormous distribution generated through this free global resource. The definition of unethical behavior of the "FFP" (fabrication, falsification, and plagiarism) model put forth by the United States Office of Integrity has applicability to cybercrimes and cyber-harm intended to deceive others.	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*. 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. [No authors listed.] "Vandalism on Wikipedia." *Wikipedia.com*. Web. Available at https://en.wikipedia.org/wiki/Vandalism_on_Wikipedia According to Wikipedia, "fraud is deliberate deception to secure unfair or unlawful gain, or to deprive a victim of a legal right. Fraud itself can be a civil wrong (i.e., a fraud victim may sue the fraud perpetrator to avoid the fraud and/or recover monetary compensation), a criminal wrong (i.e., a fraud perpetrator may be prosecuted and imprisoned by governmental authorities) or it may cause no loss of money, property or legal right but still be an element of another civil or criminal wrong. Citation: "Legal Dictionary: fraud". Law.com. Retrieved 2016-01-27.The purpose of fraud may be monetary gain or other benefits, such as obtaining a driver's license or qualifying for a mortgage by way of false statements. Citation: "Basic Legal Concepts". Journal of Accountancy. Retrieved 2013-12-18 Certain legal definitions and terms from sources other than Wikipedia in common use are helpful to understand the continuum of cyber-harm and cybercrime. They include: • **Fraud: 1.**A knowing misrepresentation or knowing concealment of a material fact made to induce another to act to his or her detriment. . Fraud is usually a tort, but in some cases (esp. when the conduct is willful) it may be a crime. **2.** A reckless misrepresentation made without justified belief in its truth to induce another person to act. **3.** A tort arising from a knowing or reckless misrepresentation or concealment of material fact made to induce another to act to his or her detriment. **4.** Unconscionable dealing; esp., in contract law, the unfair use of the

Healthcare Cybercrime Classification 2016			
Cybercrime or Cyber-harm	**Type**	**Definitions**	**Examples and Citations**
	Healthcare Professional Identity Contamination, Harm, and Vandalism:	**Website Fraud and Vandalism, continued**	power arising out of the parties' relative positions and resulting in an unconscionable bargain* • **Libel:** A written or oral defamatory statement or representation that conveys an unjustly unfavorable impression by **1.** a statement or representation published without just cause and tending to expose another to public contempt **2.** defamation of a person by written or representational means **3.** the publication of blasphemous, treasonable, seditious, or obscene writings or pictures **4.** the act, tort, or crime of publishing such a libel http://www.merriam-webster.com/dictionary/libel Libel is an important concept. To meet the Supreme Court's definition of libel involving a public figure, a quotation must not only be made up or materially altered. It must also defame the person quoted, and damage his or her reputation or livelihood https://www.google.com/#q=Liebel+definition • **Slander:** slander, n. (13c) A defamatory assertion expressed in a transitory form, esp. speech; esp., false and defamatory words that are said in reference to another, such as those charging criminal conduct, imputing a horrible or loathsome disease, alleging malfeasance or incompetence in reference to the person's professional responsibilities, or otherwise causing special damage to the person's reputation.* • **Defamation: 1**. Malicious or groundless harm to the reputation or good name of another by the making of a false statement to a third person. If the alleged defamation involves a matter of public concern, the plaintiff is constitutionally required to prove both the statement's falsity and the defendant's fault. **2.** A false written or oral statement that damages another's reputation.* * *Thompson Reuters. Black's Law Dictionary, 5th Edition. West Publishing Co: 1996.*