The Ethical Debate of Blackbaud's 2020 Data Breach

Mr. Traver Yates

Ethical and Legal Issues in the Professions: ETHC232

Professor Aprille Campbell

June 21, 2021

The Ethical Debate of Blackbaud's 2020 Data Breach

Introduction

What is the first thing that comes to mind when you think of confidentiality? Secrecy? Confidence? Trust? Mistrust? It really comes down to what experience a person has had with the subject matter as to what their perception may be. According to *Dictionary of Ethical and Legal Terms and Issues: The Essential Guide for Mental Health Professionals,* Confidentiality can be defined as "the requirement, with some exceptions that practitioners would not reveal to others the content of information communicated by the client to the." Confidentiality can come in several forms, from practitioner-client privileged communication, the duty to warn, and the responsibility to protect. The latter has exceptions, such as mandatory reporting laws, physical and sexual abuse, and exploitation or neglect. Many professions would have strict guidelines on how and when confidentiality must be upheld and procedures necessary if one of the previously mentioned exceptions were to apply to a situation (Sperry, 2006).

In this day and age, when technology not only surrounds us, but is also integrated it most of our day-to-day activities, confidentiality is more important than ever. We always have to stop and consider questions like, *should I enter my credit card information on this website? What permissions is this app really asking for? Why are they asking for my social security number?* More often than not, we shrug our shoulders and give consent or submit our information to whatever source is requesting it and we move on. However, what happens when there is a breach in confidentiality? What do we do when our trust is violated, and the domino effect of such a violation is felt for years to come? We like to think laws like HIPAA and HI-TECH protect our information, but what happens when the system fails? Who should be held responsible and made to pay the price? We cannot sacrifice our security and peace of mind because technology is at the

forefront of our existence. Confidentiality is more important than ever before, and the penalty for breaking this ethical code should decide with that importance in mind.

The Case

There are many times when confidentiality being violated gives off a ripple effect; the reverberations from which can be felt all over the world, and for years to come. In June 2020, it became public knowledge that the software vendor Blackbaud was the victim of a cyberattack. On May 20, 2020, the software vendor first began detecting an unauthorized login accessing their cloud system and on-site information systems. Cybersecurity specialists immediately began locking down the procedures and tracing the vulnerability. Interestingly enough, the cyber-attack was so sophisticated, it looked like legitimate customer activity. This made it easier from them to get past the corporation's intrusion detection systems, firewalls, and endpoint detection systems (Clolery, 2020).

Further investigation found that the attacks started as early as February 7, 2020, but were not discovered until May 20th (HealthITSecurity, 2020). Once the attack was discovered, Blackbaud started out working with internal and external cybersecurity specialists. They worked to block and patch the vulnerabilities the hackers were exploiting, and by doing so were able to prevent the hackers from further encrypting additional data on their systems (Szabo, 2020). The hackers ceased activities by June 3, 2020, allowing Blackbaud to transition their focus into assessing the extent of the damages to their systems and data (Clolery, 2020). Meanwhile, the cybercriminals continued contacting the company and requesting Bitcoin ransoms, which the company paid (Szabo, 2020).

Since the public release of Blackbaud hack, several class action lawsuits have been filed in several US court systems, including the US District Court of South Carolina, the US District

Court of Western District of Washington, and the California Central District Court. In addition, the list now includes the names of some of Blackbeard's largest clients, such as Inova Health Systems, Elon Medical Center, Roper St. Francis Healthcare, Northshore University Health Systems, Harvard University, and University of Kentucky HealthCare (HealthITSecurity, 2020). With Blackbaud clients in the United Kingdom, the Information Commissioners Office having 125 reports of UK-based businesses as victims (Clolery, 2020). The data breach compromised the confidentiality of medical records, personnel records, Social Security numbers, usernames and passwords, and bank account information (HealthITSecurity, 2020).

The Ethical Dilemma

While trying to make the best of a bad situation, Blackbaud worked at keeping the public in the loop and aware as developments in the investigation came to light. However, they still have been accused of several wrong doings in the way of confidentiality, and at the end of the day, that is where the company really failed its clients. This is a company that was entrusted with an immense amount of personal, private, and highly sensitive data that, in the wrong hands, can cause damage which could cost a single individual thousands of dollars in courts expenses to repair; and this breach has affected hundreds of thousands of individuals.

Blackbaud's has been accused of not training employees properly on security measures, failing to properly monitor their networks, and failing to implement appropriate security policies. There has also been mention of an unreasonable amount of oversight and excessive lapses in security measures. The lawsuits, including several cases against clients of Blackbaud, such as Randy Children's Hospital and other organizations, seek to recover damages, restitution, and relief on behalf of the data breach victims (HealthITSecurity, 2020).

The key ethical dilemma of the cases where Blackbaud's Information Systems were hacked in 2020 is the breach of confidentiality among hospitals, medical facilities, and other companies during the hack. Cases are being compiled as victim after victim prepares to sue Blackbaud for the invasion of their privacy, and the loss of extremely sensitive information. Which begs the question: Is Blackbaud really the culprit to be blamed, or should the fault fall solely on the hackers? Luckily, years of study have given way to a number of ethical theories that can help serve as a guide as we attempt to come to a verdict.

Application of Ethical Theory

Kantian Ethics

Immanuel Kant's theory is also known as the "Categorical Imperative." It basically says that morals, which some would say differ from person to person, apply to all. For some, this theory may bring back that "golden rule" we were all taught growing up, "Treat others the way you want to be treated." Interestingly enough, Kent's ethical theory also erases the double standard that divide ethnic groups, races, genders, and social classes. The way Kant saw it, we are all on a level, undivided, universal plain, and all reasonable human beings should be and are obliged by the same moral laws. Moral laws set the standard for decision making, and simply state that an immoral decision is an irrational one (Johnson & Cureton, 2004).

We can also draw parallels between the foundations of Kent's morals and some of the oldest parts in human history. The Christian community, for example, believe in The Ten Commandments, a set of rules which are believed to have been given to Moses by God (*Exodus 20 NKJV - - Bible Gateway*, n.d.). These Commandments lay the moral foundation for not only Christians but can even be seen as identical to the laws of many governments across the globe. We can also trace them to the moral laws which Kant believes would apply to all persons.

Where they differ is Christians believe that following these morals will lead to eternal life for your immortal soul. Kant simply sees any action that does not fall within morality as illogical and irrational. Of course, Kant's online biography, written by Tim Jankowiak, states "Kant also argued that his ethical theory requires *belief* in free will, God, and the immortality of the soul."

In the case of Blackbaud's lawsuits, Kant would more than likely weigh on the side of the hackers being at fault. The fault of Blackbaud's could be considered more of an accidental oversight. A costly one, yes, but an oversight all the same. The hackers on the other hand broke any moral law by stealing other's personal information and using it to acquire ransom. In Kant's view, what could be more irrational?

Consequentialism

Consequentialism is a theory that was developed and based on classic utilitarianism. This is a theory that we can find to be used multiple times throughout history and in current events. Consequentialism looks at the consequences of an action to determine the ethical standing of said action. Also put, "Consequentialism, as its name suggests, is simply the view that normative properties depend only on consequences" (Sinnott-Armstrong, 2003).

A good example of this can be found in a video from our second-week's lesson. Say a group of people are stuck in the cave, and one unlucky individual attempt to crawl out of the cave only to get stuck. Hence, trapping everyone else inside the cave. Since the poor guy is irreversibly jammed between the people and freedom, would it make since to sacrifice his life to save the lives of numerous others? The popular maxim that may be coming to mind is "sacrifice few for the sake of many." When consequentialism is applied to the above scenario, the answer is obvious (*Moral Philosophy - Deontology Vs Utilitarianism*, 2014).

On the subject of Blackbaud's data breach, the answer is not quite as clear. At first glance, we would believe the hackers would be at fault due to they were the ones *directly* responsible for the breach of confidentiality. However, does that mean the consequences lie solely with the unnamed criminals? Once we consider the fact that the breach would have never taken place had proper security checks and employee training been implemented, the consequentialist logic would have to place fault directly at the feet of Blackbaud's.

Virtue Ethics

Aristotle, one of the most well-known philosophers in history, is one of the holders of Virtue ethics, commonly known as Aristotle's ethics. This theory is defined as ethics that place their emphasis on the virtues and morale of a character. While other ethical theories, such as consequentialism, can take present virtues into consideration when deciding if a choice is ethical, virtues are the basis for Aristotle's theory (Hursthouse & Pettigrove, 2003). As written in the essay, *Advantages and Disadvantages of Virtue Ethics,* Aristotle believed that "virtues can be compared to skills and are acquired through proper upbringing." The philosopher also once listed and described some virtues, such as "courage, temperance, wittiness, friendliness, modesty, righteous, indignation, truthfulness, patience, ambition, magnanimity, magnificence, and liberality" (Suleman, 2019).

With that being said, if we look at the virtues—or vices—involved in the Blackbaud's data breach, we come to an interesting conclusion. On one side, we have a lazy corporation who neglected their responsibility to uphold confidentiality in regard to the data they were entrusted with protecting. On the other hand, we have greedy, unnamed, faceless hackers who stole other people's personal information for merely financial profit. Little, if any, morality can be found

within these too entities. However, it does not take much examination to find the cardinal vices that are involved (Suleman, 2019).

Envy and Sloth can both be seen here, and by both parties. With that in mind, it would be hard to rule which of the two Aristotle would agree was at fault. In fact, it would be simple to come to the conclusion that virtue ethics would name both parties at equal fault for their part in the breach.

Applying Ethical Theory to the Blackbaud Data Breach

Blackbaud's data breach had too many consequences to count. According to the consequentialism theory, the severity of the consequences of an action call into focus the ethical standpoint of that action. Truly, there were ethical flaws in both parties' actions within this situation. However, which are more far reaching? Which could have been prevented by the proper actions being taken by the other? By using the qualifications laid out in the consequentialism theory, it would be a simple process to decide upon the guilty party.

The Law and the Code of Ethics

Application of the Law

Blackbaud hosts thousands of clients and is responsible for innumerable data for users. The sensitivity of this data cannot be understated when considering that most of those clients include hospitals, doctor's offices, and other medical facilities. For those facilities that reside within the US, the information within Blackbaud is protected under HIPAA, or the Health Insurance Portability and Accountability Act of 1996. Likewise, those in the UK and Sweden are protected under GDPR, or the General Date Protection Regulation. Each have their own sets of rules and standards that are designed to guard patients from having their personal, sensitive information shared with unknown parties without their consent. Not only did the data breach

itself allow many HIPAA and GDPR infractions, but the lack of procedures and processes before, after, and even during the hack was as well.

In addition to the HIPAA and GDPR violations Blackbaud's is already having to answer for, users are also at risk for various issues including identity theft, along with incorrect reporting of credit, and information on things such as credit reports and insurance. While courts have sided in the past that "[w]here a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for fraudulent purposes…." (Wiseman & Fasoro, 2018). This is a long-term issue that may very well haunt Blackbaud's reputation for years to come.

One of the more notable infractions made by Blackbaud's was made at the very beginning, as soon as the breach of discovered. HIPAA states they must be notified as soon as the breach is discovered and GDPR require notification within 72 hours. Blackbaud's waited from May 14, 2020 (date of breach discovery) to July 16, 2020, before they publicly reported the breach to either entity. To break that down: Blackbaud's waited sixty-one days—1,464 hours—before they reported the breach.

Code of Ethics

There are also the violations to Blackbaud's own code of conduct to consider. Like all companies, Blackbaud has a code of conduct which is given to each employee at their time of hiring. Employees are expected to know and understand this code, as not following the guidelines and restrictions laid out in it can lead to a termination of employment. Two sections of their code specifically, "Computer Resources and Email" and "Confidentiality, Privacy, and Information Security," deal directly with how employees of the company are expected to treat sensitive information. They also indicate the proper procedure for how a suspected security

breach would be reported. Very strict regulations are in place which ensure employees know what they can and cannot access and for what reasons. They summarize this by simply stating, "if you do not have a business reason to access confidential information, you should not do so" ("Code of Business Conduct and Ethics of Blackbaud, Inc.," 2021).

With that being said, Blackbaud even ignored their own regulations when the breach occurred. Under Section 16 of the code, employees are advised that if they "become aware of or suspect a disclosure of confidential information, inappropriate handling of information or data, or a security breach that may have given someone within or outside of the Company unauthorized access to confidential information, you must report it immediately" ("Code of Business Conduct and Ethics of Blackbaud, Inc.," 2021). As stated in the previous paragraphs, they failed in this enormously. They also state, "safeguards must be put in place, maintained and observed to ensure that confidential information is not used, disclosed or released, intentionally or inadvertently, to someone else. You must follow all applicable laws, rules and regulations directed toward privacy and information security." Since claims have been filed accusing Blackbaud of neglecting its security measures, it is easy to conclude that their own code of conduct was not properly followed ("Code of Business Conduct and Ethics of Blackbaud, Inc.," 2021).

When looking at Blackbaud's code of conduct, however, one has to notice that prioritizing their customers privacy is not at the forefront. Not that the protection of company information should not be important, but perhaps if Blackbaud put more detailing into protection of client/customer information, as well as the procedures for possible security risks, this data breach could have been avoided.

Potential Solutions and Impacts

In May of 2020, a specialist at Blackbaud Inc. found unauthorized users were accessing company data within their self-hosted environment. While litigation for this situation is still currently in progress, several solutions could be considered to prevent similar situations from happening in the future. However, we must assume that each solution comes with its own sets of impacts and effects.

Employee Awareness

Since many companies solely focus on cyber-security as an information technology problem, they overlook the human element of their establishment. The reality is cyber-security is a company-wide issue, and it should be handled as such. Training employees on common issues about security is essential. One of the first topics that everyone focuses on is phishing and malware attacks. These attacks work to steal a user's credentials or other information, which can then be used to access otherwise restricted resources. In the year 2018, Accenture did a survey that found about 18% of healthcare employees would be willing to sell confidential data to unauthorized individuals; almost a quarter of the 18% stated that they knew someone who had sold sensitive information of this kind (Schute, 2018).

It stands to reason that environment needs to be created where security is brokered by levels of protection for the data and individuals. For a start, policies and guidelines for proper data handling would need to be put into place. Other security features could include locking down USB ports so data cannot be copied to removable drives, credential policies requiring users to passwords at regular intervals, setup and use of network activity monitors to detect and track irregular data traffic (Schute, 2018). Additionally, an individual or department should be assigned the duty to research the policies set forth by HIPPA and HITECH Acts and ensure that

the company follows those policies. That same individual or department would oversee employee training, printouts, and constant monitoring of the security and privacy policies. There should also be a method to allow employees anonymous ways to report data breaches and security compliance issues. Implementing just some of these solutions would help to secure the company's data and minimize the possibility of breaches involving employees more adequately.

Security Incident Response Plan

While we can fortify an organization to the highest standards, it is—in reality—impossible to completely prevent a data breach. With that in mind and all the necessary security protocols previously discussed, organizations also need to have a cybersecurity attack plan. A security plan lays out the methods, resources needed, chain of command, public notifications, and any third parties that need to be involved and their roles in the process. The plans begin with risk assessment and tailoring the policies for the organization, identifying the companies' vulnerabilities, and documenting the different types of data and systems which have been compromised. Based on the information discovered, please of response would be modified or put into place. This is often not a one response fits all scenario. First, the cyber-attack policy would specify the conditions in which an alarm should be sounded since every organization is different; a plan needs to indicate the point at which a flag should be raised. This includes the detection method, who all would be involved, both internal and external to the company, along with their roles. With the possible forms of detection laid out, employees will be able to execute the plan regularly or at any time which triggers an alert. From there if additional employees or outside resources should be contacted once an attack is found. With an invasion underway, responding quickly and documenting aspects is vital. The response is crucial to any attack, and so is understanding the possibility of additional incidents resulting from previous. Public notice is

essential to any reasonable investigation; developing a sense of transparency helps build trust internally and externally with the company. They have things, a draft of a public notice, a list of those to notify, such as appropriate authorities, news, individuals, and other organizations involved. Once all these steps have been evaluated, and those which need to be implemented are, intensive documentation can begin. This includes event logs, including step-by-step timelines of the incident, attack, when vulnerabilities were found, people notified, courses of action, and responses. Cyber-attacks will happen and continued monitoring and being vigilant to the possibility of attacks is a must. Practicing and training individuals on the security plan will help when an actual attack comes and continued external penetration testing of the company's assets and policies (Forming a Cyber Attack Response Plan - Cyberlock Defense, 2020).

Unacceptable Solutions

Many companies take the approach to not respond publicly to security and data breaches. While fearing the public repercussions and being tried in the public eye, the loss of revenue, and damage to the company's image. By not disclosing to the public the company's processes, who was involved, and the complete data breach analysis. This approach indirectly hurts the companies and individuals both; people tend to trust companies that allow more transparency within their policies and daily operations.

Some companies even take the stance of blaming other third parties, trying to make them responsible for the breach in the public's eyes. Reflecting the blame off them can only hurt the company's image by not taking responsibility for its lack of actions or duties in protecting one's data. By taking either of these routes and not coming forward when a breach happens or minimizing the event, people affected by the breach are at risk for identity fraud and other privacy issues and not even aware there was a breach in their privacy.

Blackbaud Inc. came forward once they had significant data surrounding the events and thoroughly analyze the extent of the data taken. This helped and hindered the investigation and notification process, giving a more prolonged period that the individual's data was publicly available without them knowing. However, once informed, they knew the extent and were able to make the public fully aware of it and the actions taken by the company, including the involvement of third parties and law enforcement. The complete analysis of the data breach has yet to be concluded and might continue for months. With accusations coming from the public, other businesses and government agencies neglect security policies and fail to properly monitor their networking and security equipment (HealthITSecurity, 2020). Multiple class-action lawsuits have been filed against Blackbaud Inc; those are still in the process of the courts, and outcomes are still out.

Decision

With all of this in mind, there is still a decision that needs to be made, a conclusion has to be drawn, and a guilty party must be named. Our ethical dilemma in this case is not simply how to rectify the situation Blackbaud's breach created, but to name who should be held responsible for the hack: the criminals who actually launched the attack and stole millions of bytes of sensitive data for the meager benefit of financial gain; or the corporation who, through a series of careless errors and lack of responsibility, dropped the proverbial ball and allowed the window of opportunity to be open for the hack to take place. This is a case that is currently still undergoing litigation in several places throughout the country—and the world—but we all know that guilty verdicts are decided across the dinner table. With that being said, the question remains: who should truly be held responsible, and what should be the consequences?

When evaluating the ethical dilemma behind the case of Blackbaud's data breach—the violation of confidentiality—a person may more than likely use the consequentialism theory. Yes, a crime was committed, and the individuals responsible should be punished for their crime. However, every action has an equal and opposite reaction. The laws of motion can be used in reference to actual actions in this case. Had it not been for the lack of training and proper security measures which should have been taken by Blackbaud's, it is possible the hack would not have been successful. The consequences for Blackbaud's action, or rather inaction, are far reaching, and have cost many their piece of mind, financial security, and even their jobs. This would mean, according to the consequentialism theory, Blackbaud's would be the party to shoulder a majority for the fault in this case.

In this modern age of the internet and technology, the fear of getting your private information stolen is very real. We place a significant amount of trust in companies that we shop with, get our healthcare from, and even pay our bill to. We sign forms and read fine print to make sure our information is safe because the consequences of stolen banking information, social security number, or even your address can be detrimental to your way of life. Not to mention, these are issues which can rarely, if ever, be fixed in a short amount of time.

A majority of the Blackbaud's clients are hospitals and medical facilities. These are places that hold a massive amount of sensitive data on hundreds of thousands, if not millions, of people at any given time. Have you or a family walked in a doctor's office within the last month? Have you noticed that sometimes the employees seem to know you as well as your own family? That is because of the extensive amount of information that is compiled within their system. Not only is it your medical history, but your demographic information, insurance information, billing

information, etc. Any one of those details in the wrong hands can send you and your family into a tailspin of headaches.

Of course, there is HIPAA, the Health Insurance Portability and Accountability Act. These are laws and regulation that are in place for any medical related facility created to give patients peace of mind that their information is not being shared with third parties without their consent or knowledge. It is basically a guidebook of confidentiality.

However, in a case like Blackbaud's data breach, there is little HIPAA can do to protect your information from an illegal action, such as a hack. That is where proper training of employees and personnel, security monitoring, firewall checks, etc. come into play. When contracts are signed with major data centers such as Blackbaud, contracts are signed and explained, and to put it simply, Blackbaud's violated confidentiality on a different level from the hackers because they betrayed the trust that placed in them. Not only did such a betrayal apply to their clients, but also, they also betrayed the millions of people whose information was stolen (Department of Health & Human Services USA, 2013).

As discussed previously, the consequences of Blackbaud's data breach are innumerable. If we judge this case based on the consequentialism theory, the severity of the consequences of an action call into focus the ethical standpoint of that action. And while both parties suffered severe lack of ethical decision making, one of them created the circumstances for the crime to take place by not upholding the basics of the IT ethical code: keep customer's data safe. It is true that a crime was committed, but ultimately Blackbaud's must take responsibility for their part in it all. They had a major breach in confidentiality, and this is something that must have consequences.

With no other way to put it, those consequences are going to come with dollar signs. Blackbaud's clients—and their clients—are going to need compensation. Having sensitive information stolen by a faceless criminal can have a heavy cost. The court fees alone to fight against identity theft can run easily into the tens of thousands of dollars, and it is not unreasonable to say that Blackbaud should foot the bill for such a situation—and any situation similar to it when that situation's cause can be traced back to the data breach. Such a penalty would definitely put a footnote in Blackbaud's future handbook to ensure proper protocols and employee training are never thought to be a waist of time or resources.

References

6 Ways to Prevent Cybersecurity Breaches. (2018, February 18). ComTech Computer Services, Inc.; ComTech Computer Services, Inc. https://www.comtech-networking.com/blog/item/596-6-ways-to-prevent-cybersecurity-breaches/

Athanassoulis, N. (n.d.). *Virtue Ethics | Internet Encyclopedia of Philosophy*. Internet Encyclopedia of Philosophy. https://iep.utm.edu/virtue/

Board Liability - Reduce Risk for Data Security Breaches. (n.d.). Legal.thomsonreuters.com. Retrieved June 2, 2021, from https://legal.thomsonreuters.com/en/insights/articles/board-liability-reduce-risk-for-data-security-breaches

CIVIL FOR RIGHTS YOUR HEALTH INFORMATION PRIVACY RIGHTS Know Who Has Seen It. (n.d.). Retrieved June 2, 2021, from https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/consumers/consumer_rights.pdf

Client Alert: Managing third party ransomware risk: Blackbaud. (2020, July 28). Cordery. https://www.corderycompliance.com/3rd-party-ransomware-risk-blackbaud/

Clolery, P. (Ed.). (2020, August 6). *The Hack of Blackbaud: Damage Is Still Being Assessed*. The NonProfit Times; NPT Publishing Group. https://www.thenonprofittimes.com/npt_articles/the-hack-of-blackbaud-damage-is-still-being-assessed/

Code of Business Conduct and Ethics of Blackbaud, Inc. (2021). In *Code of Business Conduct and Ethics of Blackbaud, Inc.* Blackbaud, Inc. https://investor.blackbaud.com/static-files/bf9c3696-073d-4ca2-b0e6-0128082792d5

Data Protection Law: An Overview. (2019). https://fas.org/sgp/crs/misc/R45631.pdf

Department of Health & Human Services USA. (2013). *OFFICE RIGHTS FOR CIVIL Privacy, Security, and Electronic Health Records 1 PRIVACY, SECURITY, AND ELECTRONIC HEALTH RECORDS*. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/consumers/privacy-security-electronic-records.pdf

Exodus 20 NKJV - - Bible Gateway. (n.d.). Www.biblegateway.com. Retrieved May 28, 2021, from https://www.biblegateway.com/passage/?search=Exodus%2020&version=NKJV

Forming a Cyber Attack Response Plan - Cyberlock Defense. (2020, August 25). Cyberlockdefense.com; Lockton Affinity, LLC. https://cyberlockdefense.com/2020/09/25/forming-a-cyber-attack-response-plan/

General Data Protection Regulation (GDPR). (2013). General Data Protection Regulation (GDPR). https://gdpr-info.eu/art-33-gdpr/

Art. 33 GDPR- Notification of a personal data breach to the supervisory authority

Good Cyber security Doesn't Try to Prevent Every Attack. (2016). *Business Mirror (Pakistan)*. Newspaper Source Plus. http://search.ebscohost.com/login.aspx?direct=true&db=n5h&AN=G90BBMI20161106.00040&site=ehostlive

Health Insurance Portability and Accountability (HIPAA) & HITECH Acts. (n.d.).

HealthITSecurity. (2020, September 30). *Blackbaud Confirms Hackers Stole Some SSNs, as Lawsuits Increase* (J. Davis, Ed.). HealthITSecurity. https://healthitsecurity.com/news/blackbaud-confirms-hackers-stole-some-ssns-as-lawsuits-increase

HIPAA Administrative Simplification Regulation Text. (2013). U.S. Department of Health and Human Services Office for Civil Rights.

HIPAA Compliance with Identity Verification. (2020). HIPAA Compliance and Identity Verification. https://www.smithmalek.com/hipaa-compliance-with-identity-verification/

HITECH Act Summary. (2009). Hipaasurvivalguide.com. http://www.hipaasurvivalguide.com/hitech-act-summary.php

Hursthouse, R., & Pettigrove, G. (2003, July 18). *Virtue Ethics (Stanford Encyclopedia of Philosophy)*. Stanford.edu. https://plato.stanford.edu/entries/ethics-virtue/

Jankowiak, T. (n.d.). *Kant, Immanuel | Internet Encyclopedia of Philosophy*. Internet Encyclopedia of Philosophy. https://iep.utm.edu/kantview/

Johnson, R., & Cureton, A. (2004, February 23). *Kant's Moral Philosophy (Stanford Encyclopedia of Philosophy)*. Stanford.edu. https://plato.stanford.edu/entries/kant-moral/

JOLT. (2016, December 2). *The Skeleton of a Data Breach: The Ethical and Legal Concerns*. Richmond Journal of Law and Technology. https://jolt.richmond.edu/2016/12/02/the-skeleton-of-a-data-breach-the-ethical-and-legal-concerns/

Keller (Ed.). (2020, February 27). *Risk Management Framework*. NIST. https://www.nist.gov/cyberframework/risk-management-framework

Kempfert, A., & Reed, B. (n.d.). *Health Care Reform In the United States: HITECH Act and HIPAA Privacy, Security, and Enforcement Issues †*.

Mazzoli, R., & Woitasen, D. (2021, June 1). *Health Insurance Portability and Accountability (HIPAA) & HITECH Acts - Microsoft Compliance*. Docs.microsoft.com. https://docs.microsoft.com/en-us/compliance/regulatory/offering-hipaa-hitech

Moral Philosophy - Deontology Vs Utilitarianism. (2014, February 20). Www.youtube.com. https://www.youtube.com/watch?v=aDMedWiZ_Iw

Found in Ethical and Legal Issues in the Professions, Week 2 Lesson. DeVry University.

OFFICE CIVIL RIGHTS FOR. (n.d.). https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/consumers/sharing-family-friends.pdf

Patricia Hogue Werhane, & R Edward Freeman. (1997). *The Blackwell encyclopedic dictionary of business ethics*. Blackwell Business.

Payne, S. (2014, November 24). *The Ethics of Cloud Computing*. Data Center Knowledge. https://www.datacenterknowledge.com/archives/2014/11/24/ethics-cloud-computing

Schute, D. A. (2018). Prevent cyber attacks: Don't overlook the human element. *Dermatology Times*, *39*(12), 68–68. Consumer Health CompleteEBSCOhost. http://search.ebscohost.com/login.aspx?direct=true&db=c9h&AN=133475908&site=ehostlive

Security Incident. (2020, August 29). Blackbaud. https://www.blackbaud.com/securityincident

Sharpe, C. C. (2001). *Telenursing: nursing practice in cyberspace*. Auburn House.

Sinnott-Armstrong, W. (2003). *Consequentialism*. Stanford.edu. https://plato.stanford.edu/entries/consequentialism/

Sperry, L. (2006). *Dictionary of ethical and legal terms and issues : the essential guide for mental health professionals*. Routledge.

Suleman. (2019, November 30). *Advantages and Disadvantages of Virtue Ethics | Pros & Cons | Bohatala*. Bohat ALA. https://bohatala.com/advantages-and-disadvantages-of-virtue-ethics/

Szabo, J. (2020, October 2). *How Did the Blackbaud Ransomware Attack Occur?* Top Class Actions. https://topclassactions.com/lawsuit-settlements/privacy/ransomware/blackbaud-ransomware-attack

The Definitive Guide to U.S. State Data Breach Laws. (n.d.). Retrieved June 2, 2021, from https://info.digitalguardian.com/rs/768-OQW-145/images/the-definitive-guide-to-us-state-data-breach-laws.pdf

Wiseman, L., & Fasoro, P. (2018, December 7). *Standing Issues in Data Breach Litigation: An Overview*. Inside Privacy. https://www.insideprivacy.com/data-security/data-breaches/standing-issues-in-data-breach-litigation-an-overview/