Data Privacy/Ethics in Telemedicine

W231 Final Project

(Behind the Data: Humans and Values Course)

(August 10th- 2018)

By Anamika Sinha

Centuries ago, doctors were the sole guardians of information collected from their patients. Then, doctors organized themselves into institutions like hospitals, which then became the record keepers of patient information. Next, came insurance companies, who inserted themselves into the patient provider ecosystem resulting in patient information being shared across a trifecta of stakeholders. With advent of digital technologies we now have a fourth player in this ecosystem. Digital technologies have revolutionized electronic information sharing between patients and doctors that support and promote long-distance clinical health care, patient and professional health-related education, public health, as well as health administration. Telemedicine is one such medium for information sharing.

In this paper, I intend to look at telemedicine from the perspective of privacy and its implications on patients while taking into account the different stakeholders in this value chain. Before we dive deeper, let us **define** telemedicine. The early definition of telemedicine constituted a remote interaction between the doctor and patient. In 1978, Bennett and Associates[1] proposed a more inclusive definition of telemedicine, to encompass a wider area of telehealth including remote patient monitoring. More recently, The American Telemedicine Association[2] (ATA) defined telemedicine as " the use of medical information exchanged from one site to another via electronic communications to improve a patient's clinical health status. It includes a growing variety of applications and services using two-way video, email, smartphones, wireless tools and other forms of telecommunications technology". Modern day telemedicine can be broadly defined as remote diagnosis and treatment of patients by means of telecommunications

[1] "Telemedicine: A New Health Care Delivery System - Annual Reviews." Accessed August 2, 2018. https://www.annualreviews.org/doi/pdf/10.1146/annurev.publhealth.21.1.613.

[2] "Telemedicine or Telehealth - Definitions | Telehealth Alliance of Oregon." http://www.ortelehealth.org/content/telemedicine-or-telehealth-definitions. Accessed 5 Aug. 2018.

technology. With the help of telemedicine, doctors get access to more patient data. This data can be collected actively or passively and stored remotely. What differentiates telemedicine from various health tracker apps in the market is that the telemedicine platform is managed by a healthcare provider.

Modes of Telemedicine Consultation

There are primarily four[3] modes of telemedicine. The most simple and common mode involves live, interactive video conference consultation. In this mode, the doctor and the patient are actively engaged in real time, two-way exchange of information from different locations. The communication is facilitated via secure digital video conferencing enabled by a broadband connection. This remote interaction between patient and doctor may include sharing of images, voice and text. Providers use an inhouse app or an app like eVisit which is an iPhone app that claims to be a secure, HIPAA-compliant telehealth solution for patients and providers. There are companies like ‘American Well’ that are offering telemedicine providers platform in order to connect doctors and patients.

The second type of telemedicine can be defined as store-and-forward consultation. In this type of consultation, information is collected at a given time from the patient and evaluated remotely by the doctor at a future time. This could consist of a short one-time passive interaction facilitated by a specific mobile application from the provider.

A third type of telemedicine involves constant remote monitoring of a pre-diagnosed condition including alerting patients as well as doctors. Many mobile health providers have

[3] "Telemedicine and Telehealth | HealthIT.gov." Accessed August 2, 2018. https://www.healthit.gov/topic/health-it-initiatives/telemedicine-and-telehealth.

entered this space with apps like diabetes trackers. Furthermore, cell phone companies such as Apple and Samsung are increasing their offerings in this space by partnering with healthcare providers.

A fourth type of telemedicine involves mobile health technology whereby devices such as smartphones or portable monitoring sensors transmit information to providers, using dedicated application software (apps), which are downloaded onto devices. In this scenario, a patient with an undiagnosed condition may choose to share his data with his physician. In a recent initiative taken by Apple, known as the Apple Heart study, volunteers were recruited to use an app to monitor their heart health and their data was shared with Stanford doctors. In case of anomalies, users were notified and also given a free telemedicine consultation by the telemedicine provider company, American well. Apple is promoting these services along with integrated health care records by partnering with big name hospitals such as the John Hopkins Hospital, and the Los Angeles based Mount Sinai Hospital. Apple is also working with the insurance company, Aetna[4], to subsidize the cost of the Apple watch. Given the recent emergence of digital data in the field of telemedicine, policies governing the use of this technology are continually evolving.

Telemedicine Use Cases

Telemedicine is proving to fill an important void in healthcare. With a fast aging American baby boomers population, there is a greater need for easily accessible healthcare, especially for people with limited mobility. Furthermore, with the population growth on the decline, we have fewer young people caring for such aging individuals. For_older Americans, a

[4] "Apple Watch: Aetna Will Give Out Free Smartwatches Next ... - Fortune." 8 Nov. 2017, http://fortune.com/2017/11/08/free-apple-watch-aetna/. Accessed 6 Aug. 2018.

review of medical records,found that 38% of doctor visits, including 27% of Emergency Room (E.R.) visits could have been replaced with telemedicine.[5]With remote patient monitoring available with telemedicine, the aging population can get healthcare from the comfort of their home. On the other end of the spectrum, Telemedicine is also allowing doctors to work remotely. It is bridging the demand and supply gap for physicians. Due to the high cost of medical school and the high GPA and MCAT scores required to attend, the Association of American Medical Colleges predicts that by year 2025, the United States will face a shortage of between 46,000 and 90,000 physicians[6].

Telemedicine is also being adopted for other interesting use cases. One such example is its use by registered nurses in hundreds of schools across America. As reported in an article[7], telemedicine is helping students get to class faster thereby reducing the burden on the students' families. There are programs that send mobile telemedicine units to schools. These mobile units have high-resolution cameras, electronic diagnostic, and video conference equipment and a technician that can set up a remote consultation with a doctor. School nurses have reported huge success in getting timely intervention from doctors and ensuring that kids with challenging family backgrounds get timely medical attention. The mobile units also help in addressing privacy of the student patient. This can serve as a precursor to another healthcare issue where telemedicine has been a boon.

[5] "29 Statistics You Need To Know About Healthcare & Telemedicine." 1 Aug. 2017, https://www.fshealth.com/blog/29-statistics-about-telemedicine-healthcare. Accessed 5 Aug. 2018.

[6] "Doctor shortages: Here's the real culprit—commentary - CNBC.com." Accessed August 2, 2018. https://www.cnbc.com/2015/04/30/doctor-shortages-heres-the-real-culprit-commentary.html.

[7] "Telemedicine Reinvents the Visit to the School Nurse - WSJ." 25 May. 2018, https://www.wsj.com/articles/telemedicine-reinvents-the-visit-to-the-school-nurse-1527259188. Accessed 8 Aug. 2018.

This issue is behavioral health. About 42 million Americans have anxiety disorders, and more than 16 million suffer from major depression. Many hesitate to seek treatment because of the stigma involved and often times the symptoms are ignored. Telemedicine has offered a great avenue for such patients to seek medical help from the privacy of their homes[8], in addition to saving commute and wait time in the doctor's office. Furthermore, there have been collaborations to provide scarce resources to meet increased demand. One such collaboration is between Rutgers University Behavioral Health Care (UBHC) and New Jersey Medical School. They are offering online and phone-based consults to Essex County pediatricians through the Collaborative Behavioral Health Care Project – Essex Hub[9]. Access to child and adolescent psychiatrists is scarce. Some estimates have said that the field will be only 70 percent filled in two years. Telemedicine can bridge this gap, especially at a time where we have seen an increase in gun violence partially due to mental health issues.

Another health epidemic where telemedicine has proved useful is the opioid epidemic, which was recently declared as a national health emergency. Drug overdose deaths are rising in rural areas across our nation. In 2015, the overdose death rate for rural areas surpassed the death rate for urban or suburban areas[10]. These rural areas have a scarcity of specialists and often victims of opioid abuse are not in a position to go to a specialist's office because of societal pressures, other mental health issues, and monetary challenges. Telemedicine has been very helpful in getting resources to the victims. Furthermore, the Senate HELP committee passed the

[8] "How Telemedicine Is Changing Mental Health - eVisit." https://blog.evisit.com/how-telemedicine-is-changing-mental-health. Accessed 8 Aug. 2018.

[9] "Telehealth Targets a Niche in Mental Health Care for Urban Youths." 3 Jan. 2018, https://mhealthintelligence.com/news/telehealth-targets-a-niche-in-mental-health-care-for-urban-youths. Accessed 8 Aug. 2018.

[10] "Is Telemedicine a Remedy for Rural America's Opioid Epidemic ...." 15 Nov. 2017, https://psmag.com/news/telemedicine-is-no-cure-for-opioid-crisis. Accessed 5 Aug. 2018.

Opioid Crisis Act of 2018[11], which, among other provisions, outlines the importance of telemedicine use in the country's fight against the opioid epidemic.

We are also seeing new partnerships evolve between researchers and app developers resulting in use of telemedicine for diagnosis of conditions such as autism. An autism diagnosis[12] involves a complex process of observing a child in their natural setting over longer periods of time. One such partnership is between Apple's researchkit which has autism and beyond app, and researchers at Duke University. The Autism & Beyond app[13] uses the front-facing HD camera in iPhone, along with innovative machine learning algorithms for facial recognition, to analyze emotional reactions to videos in children as young as eighteen months. The app allows researchers to observe kids over long periods in their natural surroundings and also enables researchers to provide live remote consultation. Both patients and researchers seem to be benefitting from this exchange. For parents, an early diagnosis of autism as well as saving time by avoiding long lines at doctor's office is priceless.

In fact, Apple's product, Carekit, allows people to track their health information, and share with providers[14]. Apple is also entering the field of electronic health records by partnering with multiple big name providers. With technology stakeholders entering the ecosystem, the needle is moving forward in patient-facing technology and patient-generated health data.

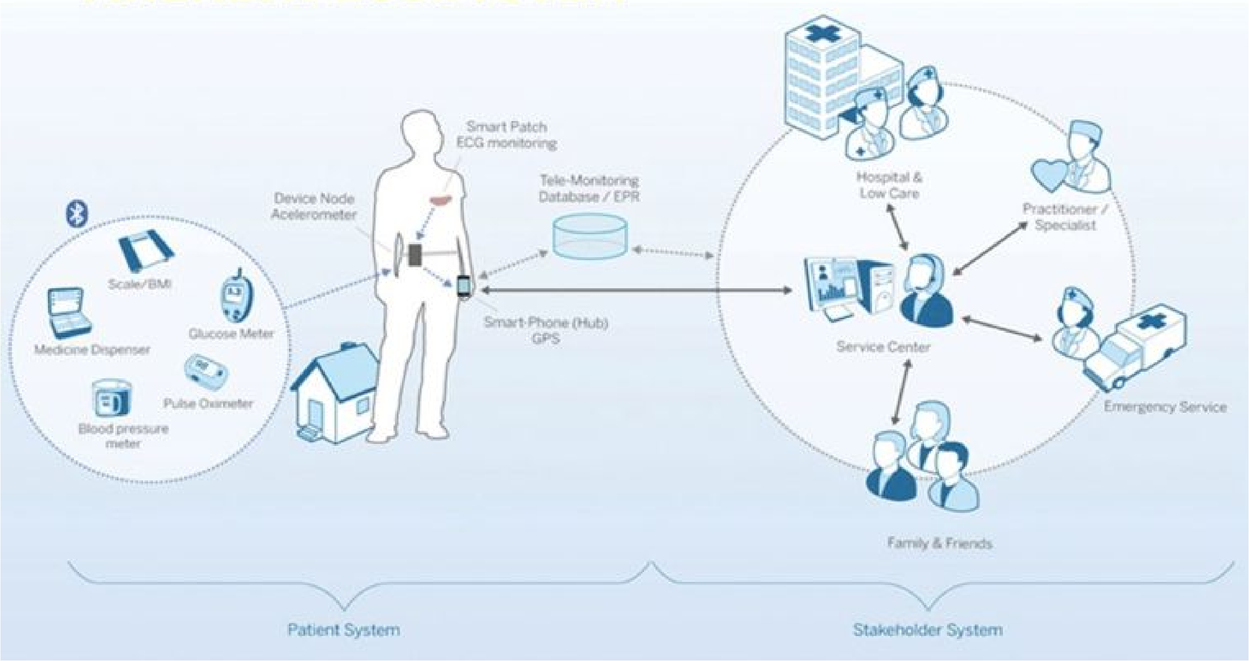
[11] "Senate finds telemedicine is crucial to opioid epidemic fight ...." 26 Apr. 2018, https://www.healthcareitnews.com/news/senate-finds-telemedicine-crucial-opioid-epidemic-fight. Accessed 8 Aug. 2018.

[12] "Could Telemedicine Work For Autism Therapy? Vanderbilt Experiments." http://www.chconline.org/resourcelibrary/could-telemedicine-work-for-autism-therapy-vanderbilt-experiments/. Accessed 8 Aug. 2018.

[13] "Using This New App Can Help Improve Early Detection and Screening ...." https://www.parents.com/health/special-needs-now/using-this-new-app-can-help-improve-early-detection-and-screening-for/. Accessed 8 Aug. 2018.

[14] "Apple CareKit should spark heightened privacy debate | ZDNet." 23 Mar. 2016, https://www.zdnet.com/article/apple-carekit-heightened-privacy-debate/. Accessed 8 Aug. 2018.

Information Flow and Associated Complexities



Source: https://www.mdtmag.com/article/2013/05/wireless-enabled-remote-patient-monitoring-solutions.

A telemedicine patient's health information is exchanged among multiple stakeholders across a wide network that leverages various communication technologies. This flow of information results in vulnerabilities and challenges at two levels- people and communication network. At the people level, outsourcing of certain telehealth-related functions, such as storage and maintenance of information to third parties further adds to the complexity. This means that it is not just the physician/provider who has access to or is storing the patient information, it’s also the software company that the provider has contracted with to maintain that electronic information. The second challenge for telemedicine is the communication network as it often involves transmission of protected health information over a digital network. The challenges get further magnified if we add third party apps that are increasingly being used as health trackers. These devices keep consumer information on their system in addition to sharing it with doctors on consent by patient. In summary, there are multiple players, network and digital platforms touching and often storing patient information.

Current Healthcare Privacy Protections, Regulations, and Standards

HIPAA[15] (Health Insurance Portability and Accountability Act of 1996) is the primary legislation in America that provides data privacy and security provisions for safeguarding medical information. This is the key protection in place for patient data. The Privacy Rule protects all *"individually identifiable health information"* held or transmitted by a covered entity, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information (PHI). As per HIPAA, there are no restrictions on the use or disclosure of de-identified health information."[14] De-identified health information neither identifies nor provides a reasonable basis to identify an individual.

As per HIPAA[16], "*When a breach does occur, all covered entities, including their Business Associates, are required to notify all affected individuals that their Protected Health Information has been exposed, whether it was due to a hacking incident, a lost laptop or smartphone, or any other device that contained unencrypted PHI.* "

[15] "Summary of the HIPAA Privacy Rule | HHS.gov." 28 Dec. 2000, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html. Accessed 10 Aug. 2018.

[16] "Summary of the HIPAA Breach Notification Rule - HIPAA Journal." 15 Mar. 2015, https://www.hipaajournal.com/summary-of-the-hipaa-breach-notification-rule-101/. Accessed 5 Aug. 2018.

HIPAA does not have specific requirements related to Telemedicine. Therefore, a telemedicine provider must only meet the HIPAA requirements, which does not differentiate between a remote and in person interaction between the doctor and patient.

In the Health Information Technology for Economic and Clinical Health (**HITECH**) Act of 2009[17], Congress extended HIPAA to “business associates,” entities that “create, receive, maintain, or transmit” identifiable health information to perform a function or service “on behalf of” a covered entity. A key provision of this standard is that a healthcare organization should only work with partners that are willing to sign a business associate agreement. This agreement obligates the third party hardware, as well as the software company which was used for the telemedicine services to maintain the same confidentiality required of the provider under HIPAA.

Federal law does not mandate”Informed Consent” from the patient before using telemedicine. However, at the state level, some states have passed laws that require informed consent use from the patient before using telemedicine.

In the February of 2015, the FDA issued guidance aimed at mobile medical app manufacturers and other interested parties, which stated the FDA’s intent to exercise enforcement discretion on mobile medical apps that pose a low risk to patients’ safety. Additionally, in the same time frame, the FDA also issued guidance stating that it would practice enforcement discretion on Mobile Device Data Systems(MDDS). MDDS is a device that is intended to transfer, store, convert, or display medical device data without controlling or altering

[17] "What is the HITECH Act - HIPAA Journal." https://www.hipaajournal.com/what-is-the-hitech-act/. Accessed 10 Aug. 2018.

the functions or parameters of any connected medical devices. An MDDS may include software, electronic or electrical hardware, modems, interfaces, and a communications portal.

There is also the FHIR [18](Fast Healthcare Interoperability Resources) specification, which is a technical standard for exchanging healthcare information electronically. This standard has a module on documentation and service to create and maintain security, integrity, and privacy.

Furthermore, some 167 bills related to telehealth/telemedicine are active in state legislatures this year, according to the Center for Connected Health Policy.

Specific Data Leakage and Privacy Issues

As we saw earlier, telemedicine has facilitated better access to healthcare and in some cases convenience for patients, but it has also introduced more complexity in an already complicated healthcare ecosystem. For example, telemedicine can create situations where patients and physicians may be in two different states. States have different privacy laws in addition to licensure requirements and this may require a provider to ensure that laws in both states are followed.

Another risk aggravated by telemedicine is ease of medical identity theft. Cyber criminals are increasingly targeting healthcare data that is rich in personally identifiable information. In a recent article by Reuters[19], it was mentioned that medical information is worth ten times more than credit card numbers on the black market. This value of medical data in black market has

[18] "Overview - FHIR v3.0.1 - HL7.org." https://www.hl7.org/fhir/overview.html. Accessed 10 Aug. 2018.
[19] "Your medical record is worth more to hackers than your credit card ...." 24 Sep. 2014, https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924. Accessed 9 Aug. 2018.

also been highlighted by privacy expert Larry Ponemon[20], founder of the Ponemon Institute. Hackers sell this data to fraudsters who use it to create fake IDs to buy medical equipment or drugs that can be resold, or they combine a patient number with a false provider number and file made-up claims with insurers, according to experts who have investigated cyber attacks on healthcare organizations. Unlike credit card theft, medical identity theft is often not immediately identified by a patient or their provider, allowing fraudsters more time to use such fake credentials.This type of identity theft has soared in recent years. which is why most medical practices now require patients to present an insurance card and a picture ID to confirm their identity at the time of service. With telemedicine, the patient is remote, making it much easier for someone to obtain treatment using a stolen medical identity.

Another challenge for telemedicine is that it often involves transmission of protected health information (PHI) over insecure connections. Providers are required to have transport encryption. So, while the network at the provider end is secure, there is nothing preventing patients from attending telemedicine appointments over a insecure Wi-Fi network in a local coffee shop, college students from connecting over a campus Wifi network, or patients in remote areas from connecting over a library Wifi network. And while consumers are becoming more conscious of security issues, not everyone has their home network properly secured. In summary, while the telemedicine service provider may have secured its network, an open unencrypted network at the patient's end will invite many avenues for cyberattacks.

Yet another challenge is with the downloading of files on mobile devices at the provider end. Not many providers go far enough to install remote wipe software on the mobile device to

[20] "Data Breaches Happening at Record Pace, Report Finds - NBC News." 24 Jul. 2017, https://www.nbcnews.com/business/consumer/data-breaches-happening-record-pace-report-finds-n785881. Accessed 9 Aug. 2018.

erase PHI. Challenges also arise in terms of patient understanding of scenarios of when they are covered by HIPAA. Currently, they are protected by HIPAA when they use devices initiated by the provider. With many health trackers in the market that allow a person to share health information with doctors, there's a good chance that their data is not covered by HIPAA and the naive consumer may not be aware of it.

Privacy issues also arise with remote monitoring systems that interface with the patient's body to detect safety issues or medical emergencies may inadvertently collect sensitive information about household activities. For instance, sensors intended to detect falls may also transmit information such as interactions with a spouse, religious activity, or indicate when no one is home.

The field of telemedicine has been proving so lucrative. Providers are rushing in to reap the monetary as well as immediate patient benefits without fully understanding the security implications. A study[21] revealed a lack of standardization in telemedicine security across all chronic illnesses included in the study. Furthermore, many telemedicine researchers seemed unfamiliar with the field of security in general. The study also revealed that in telemedicine related articles, authors designed their own protocols for communication without giving any proof of security.

While HIPAA protects identifiable patient data, there is no protection for de-identified patient data. This data is allowed to be sold to third party companies. Telemedicine, with its various modes of remote monitoring is on one hand helping patients but on the other hand is creating lot more digital imprints of patients habits. Deidentified patient data

[21] "Telemedicine Security: A Systematic Review - NCBI - NIH." 1 May. 2011, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3192643/. Accessed 5 Aug. 2018.

is already worth a lot in the secondary market. One example of a player in secondary market is pharmaceutical companies who are buying this data to figure out areas for investments, efficacy of drugs and much more. The detailed insights into a patient lives captured by telemedicine devices, is feeding a lot more information to the secondary market. If we combine this data with other sources available online, we can get into risky territory leading to re identification of an individual. In the words of Dr. Jonathan Wald, a Harvard Medical School instructor and expert on health data at the non-profit group RTI International,[22] "*It's very difficult to protect data from re-identification through most processes that are used to anonymize it. That is easy when it is a rare condition and there are a few other tidbits. It is getting easier and easier because of the amount of electronic publicly available data and the amount of analytic engines to turn through it.*"

Ethical Challenges with Telemedicine

There are some challenges on the ethical front as well. Since the first, second, and fourth scenarios of telemedicine mentioned earlier require the patient to have a digital device in the form of a computer, iPad, or smartphone, there is an exclusion bias based on affordability as well as ability to use these devices. The poorer sections of the society may not have access to digital

[22] "The Hidden Trade in Our Medical Data: Why We Should Worry ...." 11 Jan. 2017, https://www.scientificamerican.com/article/the-hidden-trade-in-our-medical-data-why-we-should-worry/. Accessed 9 Aug. 2018.

devices and also many elderly people are unaware of the security issues involved with telemedicine.

Another ethical concern that has been highlighted by the American Medical Association (AMA) is the significance of patient doctor relationship which has served as a foundation for trust in traditional medicine. In its guidelines, AMA emphasizes[23] that telemedicine is a supplement to “live visits” and should be used only in the context of an existing doctor-patient relationship. The World Medical Association also recommends having a prior relationship with the patient. The American Telemedicine Association(ATA) agrees that there should be an established doctor-patient relationship when using telemedicine, but also believes that it should be permissible to establish the relationship by video.

Furthermore, with third party apps like autism detectors (even when they are HIPAA compliant in order to be used by providers), doctors may not necessarily understand the algorithm and use it as a decision point. More transparency is required in order to lend credibility to these kinds of apps. This is further aggravated by any bias present in training data for these algorithms. These issues in machine learning remain opaque to doctors. The fourth scenario of telemedicine opens up a multitude of scenarios that are associated with use of apps that involve sharing data with doctors, even if the app is HIPAA compliant. For example, a diet tracker app sharing data with doctors can make its way to the patient’s electronic health record informing the insurance company of a person’s good or bad dietary habits leading to new forms of data that would not have been previously available to insurance companies. The ethical issues arise

[23] "Telehealth: The balance between access and ... - Medical Economics." 10 Dec. 2015, http://www.medicaleconomics.com/health-law-policy/telehealth-balance-between-access-and-ethics. Accessed 9 Aug. 2018.

because patients may share this data without realizing that it could end up in the hands of insurance companies who may use it to decide coverage and insurance rates.

When data breaches happen, who loses and who gains? When breaches occur, it is the patient who suffers most while the provider company can incur monetary and reputation loss. For the patient, the strain could be long term with worries about the health conditions being known to employers as well as insurance companies. Social stigma and other mental health issues can also add up. Just the mere fact of losing control over their health information can be very disturbing for many people.

Perspective of Privacy framework

I would like to begin this section with a fitting quote from one of the academic papers[24]. "Privacy is not just about patients' control over their information. It is better characterized in terms of norms that govern the flow of personal health information in a manner that promotes the values, ends, and purposes of the health care context."

A patient may be sharing information like mental health, substance abuse, or symptoms of life threatening situations. Such information is particularly sensitive and often associated with a stigma. Considering Nissenbaum's contextual privacy framework[25], where the patient is the sender of the information and the doctor is the recipient. The **context is patient welfare/treatment**. HIPAA puts in place a framework for patient privacy which guides the transmission principle. Telemedicine introduces a "medium of communication". If this medium

[24] "The Value and Importance of Health Information Privacy - NCBI - NIH." https://www.ncbi.nlm.nih.gov/books/NBK9579/. Accessed 9 Aug. 2018.
[25] "A Contextual Approach to Privacy Online - MIT Press Journals." 29 Sep. 2011, https://www.mitpressjournals.org/doi/10.1162/DAED_a_00113. Accessed 10 Aug. 2018.

is not compromised and the communication(network, systems and people), are governed by HIPAA, then the patient's privacy is not compromised if the data is just used for treatment. The contextual framework is violated when patient data is sold to third party companies for any purpose without asking for consent.

It is to be noted that the assumption of remote monitoring devices and apps complying with HIPAA is taken for granted if these devices/apps are introduced or provided to the patient by the provider. There are many self-standing apps like diabetes monitors or other nutrition apps as well as personal fitness devices such as Fitbit which are in the market that are used by people to self-monitor their health. These apps/devices are not governed by HIPAA and there is nothing preventing these companies to sell/use this data to maximize their gains.

Considering Benefits versus Privacy

In this section I will look at some studies that have looked at the cost benefit of telemedicine as well as some privacy and ethical issues with telemedicine that have ended at the court. I shall also look at the uniqueness of medical data privacy.

The US spends more money on healthcare than any other wealthy nation. But it hasn't resulted in better health. Telemedicine is a very small proportion of the healthcare diorama. According to analysis by global professional services company Towers Watson, telemedicine could potentially deliver more than $6 billion per year in health care savings to American companies by reducing the cost of healthcare[26]. As we move towards a value-based healthcare model, the role of telemedicine may increase significantly. A value based healthcare model is a

[26] "Current Telemedicine Technology Could Mean Big ... - Towers Watson." 11 Aug. 2014, https://www.towerswatson.com/en/Press/2014/08/current-telemedicine-technology-could-mean-big-savings. Accessed 10 Aug. 2018.

model where providers will be incentivized to keep patients healthy rather than being reimbursed on a volume of incidents. In order to keep patients healthy, the ability to monitor them when they are not in the doctor's office can provide great insights, sometimes even before the patient recognizes the symptoms. By using telemedicine, doctors work in a preventive mode rather than a reactive mode.

A study in 2015 which is titled, "Feasibility and Acute Care Utilization Outcomes of a Post-Acute Transitional Telemonitoring Program for Underserved Chronic Disease Patients"[27], investigated acute care utilization outcomes during the use of a 90-day transitional telemonitoring program for underserved COPD and heart failure patients. Patients were enrolled in the program between October, 2010 and August, 2012, and researchers measured rates of emergency department visits and all-cause readmission after 30, 90, and 180 days. The study found a 50% reduction in 30-day readmission and a 13-19% decrease in 180-day readmission among patients who received the telemonitoring intervention. Ultimately, they concluded that remote patient monitoring has the potential to reduce long-term acute care utilization.

Another study[28] in 2016 looked at the the costs and benefits of one large telemedicine Emergency Medical Services(EMS) initiative. In total, 5570 patients were treated over the first full 12 months with a telemedicine-enabled care model. The study found a 6.7% absolute reduction in potentially medically unnecessary Emergency department visits, and a 44-minute reduction in total ambulance back-in-service times. The average cost for a telemedicine patient

[27] "Feasibility and Acute Care Utilization Outcomes of a Post-Acute ... - NCBI." 8 May. 2015, https://www.ncbi.nlm.nih.gov/pubmed/25955129. Accessed 6 Aug. 2018.

[28] "Langabeer JR[au] - PubMed Result - NCBI." https://www.ncbi.nlm.nih.gov/entrez/query.fcgi?cmd=search&db=pubmed&term=Langabeer%20JR[au]&dispmax=50. Accessed 10 Aug. 2018.

was $167, which was a statistically significantly $103 less than the control group (*p* < .0001). The programme produced a $928,000 annual cost savings from the societal perspective, or $2468 cost savings per Emergency Department visit averted (benefit).

But **not all patients benefit from the cost savings** as much. Medicare, the largest health insurer for Americans across the United States, currently only covers the use of telemedicine in rural or medically underinsured areas and only when video conferencing is used, and Medicaid views telemedicine as a cost-effective alternative to the more traditional face-to-face physician/patient visit, but hasn't exactly jumped on board.

From the legal perspective, Telemedicine seems to have scored some victories. In a telemedicine battle in Texas[29] a judge issued a stay on regulations that would have rolled back the use of telemedicine in that state. The ruling stems from an ongoing case pitting the Texas Medical Board against Teladoc, a telemedicine provider. Earlier in the year the medical board created a rule that physicians must have established a face-to-face relationship with a patient to be able to prescribe medications. Teladoc–whose business is phone healthcare consultations for non-emergent conditions–fired back with an antitrust suit, claiming the regulation would hurt the telehealth industry and reduce access to the patients it serves. At its core, the lawsuit is an argument about the regulatory power of state medical boards, but it may also become a bellwether for determining the way telemedicine is used in the future.

In a 2015 Iowa court case[30], the court ruled in favor of administering a medication abortion remotely through video conferencing. The court said that putting such restrictrictions

[29] "Federal Court rules in favor of Teladoc, blocking Texas Medical Board ...." https://www.teladoc.com/news/2015/05/29/federal-court-rules-in-favor-of-teladoc/. Accessed 5 Aug. 2018.

[30] "Medication Abortion Through Telemedicine: Implications ... - NCBI - NIH." https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4780360/. Accessed 9 Aug. 2018.

places undue burden on a women's abortion rights especially in rural settings, where there a shortage of these services. While this has direct impact on women's abortion rights, the Court's decision also has broader implications for telemedicine, by limiting state boards of medicine's role regarding the restriction of politically controversial medical services when provided through telemedicine. The case also highlights that fairness in accessibility of healthcare services by all seemed to be a priority.

The Federal Trade Commission (FTC) is not hesitant to file complaints against companies that it believes fail to reasonably protect the security of consumers' personal data, including medical information. In August 2013[31] FTC filed a complaint against LabMD, Inc., alleging that the medical testing laboratory exposed the personal medical information of more than 9,000 consumers by placing the information on a peer-to-peer file-sharing network[32]. The filing followed the discovery of the personal information of several hundred consumers who used LabMD's services in the possession of identity thieves. In this case, as in an earlier case against a medical transcription firm that exposed personal medical information on the public Internet, FTC has acted to enforce HIPAA's security requirements

On the surface, it might appear that the healthcare context is similar to other privacy dilemmas in which individuals engage in a privacy calculus to evaluate the costs and benefits of disclosing personal information. Yet, arguably, the healthcare context is unique in at least two respects[33]: (1) the nature and variety of risks inherent in the compromise of sensitive health

[31] "Legal and Regulatory Considerations Associated with ... - NCBI - NIH." 14 Jan. 2015, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4377557/. Accessed 9 Aug. 2018.
[32] "Cases and Proceedings | Federal Trade ...." https://www.ftc.gov/enforcement/cases-proceedings. Accessed 10 Aug. 2018.
[33] "The Digitization of Healthcare: Boundary Risks, Emotion, and ...." 8 Apr. 2011, https://pubsonline.informs.org/doi/abs/10.1287/isre.1100.0335. Accessed 6 Aug. 2018.

information; and (2) the emotion linked to one's medical state. Prior research suggests that people tend to be more emotional and exhibit greater risk-seeking behavior when faced with a life–death choice than with problems in other life domains such as personal finances or public property[34]. Furthermore, patients care about what is done with their health data. They are more open to sharing their information if it is used for the welfare of other patients rather than used for maximizing gains for a pharmaceutical company or for commercial gains of insurance companies.[35]

Recommendations

Steps can be taken to mitigate some of the ethical, privacy as well as security issues highlighted in previous sections. Exclusion due to affordability can be addressed by providing subsidies for smartphones to qualifying sections of the population. Many states already have provisions for low income residents to get free cell phones as well as internet connectivity at a low cost.[36] This can be extended to cover smartphone to help alleviate the exclusion bias of low income population. A **privacy by design**[37] approach on telemedicine apps, remote monitoring devices and network devices can help with exclusion of elderly people who are not aware of security concerns. Such a privacy aware design will also ensure trust in the long term.

[34] "Emotion and the Framing of Risky Choice - Semantic Scholar." 8 Feb. 2008, http://faculty.wcas.northwestern.edu/~jnd260/pub/Druckman%20McDermott%20Political%20Behavior%202008.pdf. Accessed 10 Aug. 2018.

[35] "Whose Data Are They Anyway? Can a Patient Perspective Advance ...." https://www.nejm.org/doi/full/10.1056/NEJMp1704485. Accessed 9 Aug. 2018.

[36] "Free Cell Phones Lifeline and Link-Up - Accessible Cell Phones." http://www.etoengineering.com/freecellphones.htm. Accessed 9 Aug. 2018.

[37] "Towards a Privacy-Aware Qunatified Self Data Management ...." 10 Jun. 2018, https://www.researchgate.net/publication/325640055_Towards_a_Privacy-Aware_Qunatified_Self_Data_Management_Framework. Accessed 9 Aug. 2018.

Patients will benefit from a reignited dialogue on HIPAA about sharing of deidentified data. Healthcare technology has been reshaped a lot since HIPAA was passed. HIPAA was not designed to address the challenges that come with readily available public data online. As highlighted earlier, we can come very close to re-identifying a patient in rare medical conditions. Data scientists, telemedicine researchers and policy makers need to evaluate the modern days risks associated with releasing deidentified healthcare data.

In the domain of security, most providers incorporate network encryption. Data encryption where a files are encrypted and password protected can alleviate risk if the device with sensitive is lost or stolen. The encrypted file will be of no value when it ends up in the hands of wrong people. This is currently being done by some some but not all providers and definitely not as the patient end.

Blockchain technology[38]is proving to aid in patient privacy and security of shared data. The technology that provided a universal set of tools for cryptographic assurance of data integrity, standardized auditing, and formalized "contracts" for data access mainly in finance industry is starting to be used in healthcare. Organizations like Medicalchain are working to bring in the security of blockchain into electronic healthcare data[39] with the recent launching of telemedicine application.

Additionally, certification of third party telemedicine apps by cybersecurity experts can provide much needed trust and additional layer of security check. Currently health experts work

[38] "The Potential for Blockchain to Transform Electronic Health Records." 3 Mar. 2017, https://hbr.org/2017/03/the-potential-for-blockchain-to-transform-electronic-health-records. Accessed 9 Aug. 2018.

[39] "Medicalchain Announces Blockchain Enabled Telemedicine Application." https://medium.com/medicalchain/medicalchain-announces-blockchain-enabled-telemedicine-application-98858c5cd694. Accessed 9 Aug. 2018.

in silos to advance telemedicine with the goal of patient and provider benefits. While they exchange ideas with other health experts, cybersecurity experts also need to be part of the conversation. Collaboration between telemedicine researchers and security researchers can help in moving towards common industry security standards[40].

Finally, there is no substitute for effective patient education. Making patients aware of security issues with telemedicine and the vulnerable points will make them educated consumers and beneficiaries of the telemedicine revolution. However, the time for this education is not when the patient is in need of medical attention and focused on treatment and has a diminished ability to weigh risks. A better time would be in the form of public health messages when patients are in a better mental state to understand the risks and prepare themselves. In case a data breach happens, easy accessibility of simple steps that the victim can take to prevent long term harm can go a long way in helping patient concerns.

Conclusion

The rising cost, regulations, data privacy, and security issues with healthcare are pushing companies to form new partnerships. These alignments are ushering innovative methods to improve healthcare accessibility and cost. We are witnessing new alliances between technology companies and healthcare providers. If these partnerships focus primarily on patient welfare and dignity rather than just aiming to monetize patient information, then society can greatly benefit from telemedicine. But if the explosive growth of telemedicine is accompanied by an equivalent growth in medical data breaches and identity theft, then the industry risks to lose consumer

[40] "Telemedicine Security: A Systematic Review - NCBI - NIH." 1 May. 2011, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3192643/. Accessed 10 Aug. 2018.

trust. Therefore, telemedicine needs to succeed, cybersecurity experts need to play a key role in identifying risk areas that could lead to uniform industry security standards.

Telemedicine offerings need to go through a thorough risk analysis, be subject to the same privacy and security processes and policies as every other aspect of healthcare operations. Additionally, due to the treasure trove of data that telemedicine generates, the industry also needs to have a dialogue about the ability of HIPAA to protect patient privacy. There is an increasing threat of rouge entities using the growing volume of de-identified data along with wealth of public data already online to re-identify patients.

In summary, I truly believe that Telemedicine can disrupt the Healthcare industry much like Uber did to the taxi industry i.e. make it easy to access and affordable for the masses. But for all its promise, the prescription for telemedicine services requires us to proceed with prudence and discretion.