eDiscovery Challenges in Healthcare

Secure and Effective Management of Data in the Healthcare Industry

Sundar Krishnan, Narasimha Shashidhar

Sam Houston State University, Huntsville, TX, USA. Ph: (936) 294-1591
E-mail: {*karpoor, skrishnan*}*@shsu.edu*

ORCID ID: 0000-0003-4360-1300, 0000-0002-4877-158X
Research Paper Received: 17.05.2019 Revised: 21.06.2019 Accepted: 29.06.2019

Abstract—In today's digital age, medical litigation often involves Healthcare data and medical devices. Electronic discovery is a process involving legal parties on a case to preserve, collect, review, and exchange electronic information for the purpose of using it as evidence in the case. With the growth of information in electronic format across the globe, litigations involving Healthcare can get challenging especially with the advent of smart Healthcare devices. In this paper, the authors explore the challenges faced during the eDiscovery process involving Healthcare data, systems and devices. The authors propose incorporating industry best practices towards effective management of the eDiscovery process in the Healthcare Industry.

Keywords—Data Security, Privacy, eDiscovery, Digital Evidence, Electronic Discovery Reference Model (EDRM), Electronic Stored Information (ESI), Healthcare, Legal, Digital Forensics

1. Introduction

Electronic Discovery (also known as e-discovery, e discovery, or eDiscovery) is the contemporary concept of the traditional pre-trial discovery process during which legal counsels exchange copies of documents from the opposing party in anticipation of finding valuable evidence to assist with their side of the legal case. Electronic Discovery Reference Model (EDRM) [1] is a conceptual framework of the eDiscovery process that outlines standards for the recovery and discovery of digital data. EDRM consists of nine steps namely; Identification, Preservation, Collection, Processing, Review, Analysis, Production and Presentation.The scope of eDiscovery process relates to evidence of nearly all electronic devices especially those that are connected to the company or home network or the Internet such as personal computers, wearable devices, mobile phones, IoT, computer networks, industrial automation, medical equipment, etc. Stories about the search and identification for "smoking gun" documents – usually e-mail and instant messaging – has become a staple of the news media in many industries [2]. Healthcare providers have been little involved in such news stories, however, noteworthy cases have started coming from allied industries like insurance carriers, medical device manufactures and pharmaceuticals [2]. It is predicted that this situation will change someday and will probably catch the vulnerable Healthcare providers in a blind. If the recent eDiscovery cases are of any indication,

Healthcare providers and their business associates are especially big targets for eDiscovery. Healthcare service providers, insurers, researchers, medical device manufacturers and medical technology enthusiasts are in the continuous process of enhancing Healthcare with the latest technology like mobility, Artificial Intelligence (AI) and robotics. This has yielded some cutting-edge developments, such as, medical robots, tele-medicine, wearable devices and portable platforms that were once only portrayed in fiction settings like the star-wars movies. Such developments in technology has yielded great user feedback and acceptance making this a lucrative market. While automation is welcome, litigation can get cumbersome if the legal world is not in-step with technology. With the American Recovery and Reinvestment Act of 2009, Healthcare providers were mandated to implement the use of electronic health records (EHR) by 2014 leading to a paperless world. User acceptance of all the technological enhancements has also contributed to the drive to automate. Sometimes, in situations like a medical malpractice cases or an agency mandated audit, the forensic capabilities of tools and investigative skills can be a nightmare due to complicated skill matrix needed to undertake such an exercise. Moreover, technology in devices also assists in multi-language support contributing to the investigation complexity.

In a dispute, extensive cooperation is required among litigation parties, their counsel and other stakeholders as to; 1) What information exists, 2) Is it relevant 3) Where it exists 4) Is worth extracting 5) Can it be extracted in a targeted and meaningful way while maintaining it's integrity and 6) Can it be explained within the context of the case. For example, medical records in diagnostic and monitoring equipment contains the patient information and medical information. In addition to device metadata, it also contains metadata (logs) about how and when the patient was treated, when and what medical information was written, when it was accessed by whom, and when it was transmitted, opened, read, printed, commented or edited [3]. Unlike the huge volume of emails and document that are traditionally the bulk of eDiscovery, in the above example, device metadata, possible residual patient data and transaction logs may be hidden or embedded, encoded and in proprietary formats. Litigation parties must constantly decide if such data is pertinent to their case and worth the extraction effort.

In this paper, the goal of the authors is to catalog various challenges that can occur in the legal-healthcare market due to the growth of medical devices, increased automation of medical systems, consolidation of various databases and proliferation of Internet-of-Things (IoT) in the Healthcare industry. The authors suggest best practices that might overcome these challenges.

2. Literature Review

In the healthcare litigation world, eDiscovery can be encountered in cases like medical malpractice, criminal, civil and financial lawsuits, incident breaches, drug frauds, dubious research, insurance claims, enactment of Healthcare regulations, etc. In each of these cases, the whole EDRM process is undertaken by the legal stakeholders. The legal profession and community have a dedicated branch of practice and personnel focused entirely on Healthcare lawsuits. A ton of related work on eDiscovery can be found in the legal blogs, court dockets and legal-medical news bulletins wherein multiple legal cases are discussed. For a successful eDiscovery process in Healthcare, evidence should be identified, collected and preserved. Darnell et al. [4] in "Forensic Science in Healthcare" highlight the need for preserving the on-scene evidence by first

responders in Healthcare. Crime-scene preservation is key to successful evidence gathering with possible tampering. Khan et al. [5] discuss the forthcoming legal challenges in Mobile Health Technology's Impact on the medical profession. As medical devices acquire mobility features, legal issues can arise due to evidence acquisition and preservation as users may tamper with the device. eDiscovery challenges are just not local to the US Healthcare market. Kunsten et al. [6] focus on Ontario, Canada to describe the trends and analysis of Trials and Appeals in the medical malpractice. A literature gap exists in documenting various challenges that legal analysts may face in the Healthcare industry. In this paper, the authors outline these challenges and propose best practices.

3. Healthcare litigations

Across the globe, Healthcare is a busy industry when it comes to litigations. Legal disputes can cover a wide variety of issues and there are plenty of lawsuits being filed for various reasons. These disputes can be challenging given the degree of medical automation and digital data they present. Below are a few examples of the types of litigations related to Healthcare.

- ➢ Regulatory disputes or Criminal investigations or qui tam suits for accusations of violation of the Stark Act, False Claims Act, or other state and federal laws
- ➢ Reimbursement litigation and ERISA violations
- ➢ Disputes about drug trials - preparation, surveys, testing and outcomes
- ➢ Employment discrimination
- ➢ Employment contracts and provisions like non-competition, non-disclosure and non-solicitation
- ➢ Disputes with staff privileges and credentialing
- ➢ Partnership disputes between providers
- ➢ Bankruptcies
- ➢ Trademark and copyright
- ➢ Disputes between Insurer(s) and Provider(s)
- ➢ HIPAA violations
- ➢ Unfair competition and tortious interference by competitors
- ➢ Data breaches
- ➢ False Data for grants
- ➢ Embezzlement
- ➢ Malpractice

A recent litigation trend survey states that organizations are facing more regulatory proceedings and arbitrations while trying to manage cyber-risk and data protection [7]. Often Hospital class action lawsuits arise from the hospital's unauthorized disclosure of Patient Health Information (PHI). Data breach litigation is now in the spotlight and performing eDiscovery in such situations can be complex given the unknowns of the data loss and impact. For example; within 24 hours after health insurer Anthem's announcement of a data breach involving hackers stealing the data of as many as 80 million of its current and former customers, the company was hit with lawsuits over the cyber-incident. Of the millions impacted, only 19.1 million members of the class-action lawsuit were able to demonstrate that their personal information was stored in the data center that was attacked by hackers [8]. With the onset of personal mobile medical devices and IoT enabled Healthcare devices, data breaches originating from such devices can be a challenge for litigation. Many websites are dedicated on the Internet for the latest Healthcare lawsuits and settlements [9], [10].

4. Healthcare data universe

Healthcare data can assume many forms; from the fax/paper documents to electronic patient records. The authors try to group Healthcare data into distinct types and identify possible electronic storage locations.

Corporate IT Healthcare data falls into the below types [11], [12];

- ➢ Operational data
- ➢ Real time data - Networks and monitoring systems like HVAC
- ➢ Machine data - machine data is the digital exhaust created by the systems, technologies and
- ➢ infrastructure powering modern businesses
- ➢ Structured corporate data - data related to financial transactions, sales, inventory management and manufacturing production resulting in structured data
- ➢ Unstructured repetitive corporate data
- ➢ Unstructured non-repetitive corporate data like emails, Healthcare records, warranty claims, corporate contracts, call center interchanges, marketing responses
- ➢ Business Customers data
- ➢ Audit data
- ➢ Intellectual Property
- ➢ Dark data
- ➢ Unverified outdated data
- ➢ High-dimensional data
- ➢ Insurance data
- ➢ Business data across Geos

For corporate data, eDiscovery starts from the beginning with logging, copying, and indexing information from various information repositories. While querying and indexing simplifies the search process, narrowing search variables to generate accurate reports can be challenging due to the volume of data. Departing employees take with them valuable information about business practices, clientèle, and operations [13]. Following an organizational approved exit process, ensures that all such information is transitioned and handled appropriately when an employee exits the workplace is crucial with e-discovery. With the dependence on social media, employees should be careful with their organization's social image and the business should encourage their clients and partners to do so the same, with the knowledge that data on social media may come back to bite them as a lawsuit. Furthermore, avoid spoliation on social media as it can be easy to discover when litigation is anticipated or ongoing.

Clinical data is a common resource for Healthcare and medical research and is stored electronically. Clinical data is either collected during the course of ongoing patient care or as part of a formal clinical trial program. Clinical data falls into six major types and typical data location for storage as below [14].

- ➢ Electronic health records.
- ➢ Administrative data.
- ➢ Claims and Encounter data.
- ➢ Patient / Disease data and registries.
- ➢ Health surveys.
- ➢ Clinical trials, research and knowledge data.

In eDiscovery, all the above types of clinical data may be needed during audits or litigation. The location of such data can complicate the extraction and stretch timelines. Clinical (and pharmaceutical) trials can involve a large number of similar documents completed by participants that implies a lot of OCRed text. Such trials may involve many decades of research around the efficacy of a particular drug and involve many historical documents that were originally created on paper [15].

5. The Current State of challenges

In 2006, electronically stored information (ESI) in eDiscovery was introduced in the amended Federal Rules of Civil Procedure. During this time, EHRs in Healthcare was becoming an industry standard. While eDiscovery has rapidly evolved at the federal level, the same cannot be said at the state court level, where we find most medical malpractice litigation.

eDiscovery is often associated with legal procedures but is also a required step during audits and post-cyber incident investigations. As Healthcare moves towards embracing technology, eDiscovery increases in complexity. A heatmap table of challenges during the EDRM stages as outlined in Figure: 1. Below are the challenges discussed in detail in relation to the eDiscovery process.

5.1. Big Data

In the case of Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521 (7th Cir. 2018) [16], residents of Naperville were concerned about the volume of data from home appliances gathered by the smart readers being deployed by the city replacing traditional energy meters on its grid. The Seventh Circuit court found that the collection of smart meter data without consent from residents' homes constituted a "search" under the Fourth Amendment considering the potential privacy impact on the residents. Healthcare electronic data too can be enormous given the number of digital systems and patients that the entity deals with. From an estimate of clinical data generation viewpoint, the data storage needs can be upwards of 19 Terabytes per annum [17]. Managing and storing such volumes of data each day can be a nightmare. Often data is improperly classified and tagged or at worse never classified. Sifting through such volumes of data from backups and archives for eDiscovery can take days. Sometimes, data is either infrequent or completely not backed-up from medical systems due to various reasons like criticality or tier classification of the system by IT. From Figure- 1, managing big data can be a challenge during the identification, preservation, collection, processing and destruction phases. eDiscovery and support teams need analytical tools & software like Reativity [18] and Proofpoint [19], to get a better insight into their information. As described by Ivo Dinov in "Volume and Value of Big Healthcare Data" [20], there are four directions that could significantly impact the process of extracting information from big Healthcare data, translating that information to knowledge, and deriving appropriate actions. The author also identifies Information hoarding (e.g., heterogeneous health care systems unwilling to share clinical data about patients they have in common, health insurers unwilling to reveal, providers' reimbursement rates, computational scientist limiting access to powerful new resources, etc.) as a catalyst for the decay in data value of many interesting Big Healthcare datasets. Such challenges of big Healthcare data cause further complexities for legal and audit teams during eDiscovery. Healthcare entities must outline a data specific policy and deploy a Master Data Management (MDM) governance program that details business goals, process and procedures. The MDM program should define and identify data locations, address audit challenges, scrub and shape data, technology needs, policies, etc. all with the aim to improve data trustworthiness. At the same time, electronic data collection, processing and sale details have to be adequately and fully communicated to the patients to avoid legal issues.

5.2. EHR and Automation

Healthcare in the United States has a remarkable transition from paper to Electronic Health Record

(EHR) systems in the past decades making them a ubiquitous part of the healthcare digital landscape. A EHR system is a patient-centered digital data set that replacing the paper-chart to document observations, measurements, acts, and events in the course of evaluating, advising, or treating a patient [21], [22]. The terms ”Electronic Medical Record” (EMR) and “Electronic Health Record” (EHR) have discrete meanings that can sometimes cause confusion. An EMR contains the medical and clinical data gathered in one provider’s office, while an EHR includes more comprehensive patient information [23]. EHRs serve as a double edge sword and can trigger or prevent malpractice lawsuits. With many EHR systems to choose from, Healthcare providers, researchers and medical device manufacturers tend to cater to the maximum EHR products. This coupled with EHR deployment challenges, often lead to these systems being in poor security compliance. To complicate further, EHR systems are not always compatible with each other making them information-silos that can be difficult for the eDiscovery team to correlate. Also, individual practices have access to a Healthcare system’s EHR and maintaining their office access is a challenge. EHR systems may be well designed during initial deployment but tend to become obsolete over time with various maintenance challenges. From Figure- 1, EHR and automation can be challenging during the collection and preservation phases as the quantity of data can be huge depending on the case scope. A healthcare provider may use more than one EHR leading to further complications. Often the business needs and pressure overrule smart thinking towards deployment design architecture. Also, both sides in the litigation need to be cognizant of the EHR software’s transactional capabilities and reporting capabilities [24]. In a medical malpractice case, Borum v. Smith et al., No. 4:2017cv00017 - Document 31 (W.D. Ky. 2017) [25], a federal magistrate judge in Kentucky ordered the healthcare provider to allow the plaintiff to perform an on-site inspection of the provider’s EMR and provide the plaintiff with an audit trail of the electronic records in native format. Such litigation allows for additional scrutiny of the EHR and increases the scope of discovery burdening the legal teams. In a study [26] of 66 EHR-related litigation claims from July 2014 through December 2016, 50 percent of these claims were caused by system factors such as failure of drug or clinical decision support alerts and 58 percent of claims were caused by users such as copying and pasting progress notes. This highlights the need for EHR systems to integrate machine learning techniques to minimize system and user errors as increased system testing and numerous EHR user trainings can still result in errors. With proper design, scalability, managed integrations and workflows with other systems, incorporating security, good training and other routine precautions, EHR systems can be easily managed reducing litigation.

5.3. Logging and Retention

Adequate logs and their retention is dependent on a range of factors ranging from system features, retention capabilities to the organization’s practices. Electronic Records, system logs, database backups, email archiving, etc. if not retained for defined periods of time, can introduce complications during eDiscovery. Medical records (EHR) retention period varies from state to state in the United States depending on the category of data, patient condition and provider [27]. Artigliere et al. [21] discuss ways to manage EHR during eDiscovery and highlight the misconception by legal support that all relevant EHR actions log associated auditable events to support discovery queries for every step of originating, updating, or viewing EHRs. While routine IT systems like servers, network infrastructure, appli-

cations (software) and databases log some level of data, logs of medical devices are often inaccessible to a centralized log aggregation and management system (SIEM). Insufficient levels of logging, and reduced life of logs due to overwrites (poor archival design) further complicate investigations. Similarly, metadata contained on these devices are seldom backed up as part of routine maintenance. Medical data transactions between pharmacies, Healthcare providers, imaging consultants, research labs, billing services, transcriptionists, etc. make it difficult to track such electronic communications. Healthcare entities can help reduce eDiscovery costs by getting rid of Redundant, Obsolete and Trivial (ROT) data. Often retention process is overlooked until the cost of storage is an issue. From Figure- 1, logging, tracking and retention activities can be a challenge during the governance, identification and destruction phases. Often logs are prematurely deleted by systems or suffer from poor retention oversight as they are not at par with raw data which enjoys greater attention. Following a regular and robust audit process can help in efficient retrievals of data and fine-tuning the long-term health record retention strategy. On average estimate in 2011, 1,000 pages have been preserved for every page entered as an exhibit – too often, too much unnecessary data has been preserved and drawn into eDiscovery [28]. From a study in 2010, it is estimated that discovery costs can range from $5,000 to $30,000 per gigabyte [28]. While merely increasing the volume of logs is not advocated, increasing the quality of logs is recommended. A log integration system can help with tracking and monitoring of log information. Defining and implementing data-retention policies are key to successful audits and litigation.

5.4. Digital Forensics, Security and Privacy

With increasing volume of electronic information in the Healthcare industry being stored coupled with declining storage costs, there is a continuous increase in the demand for forensically sound digital investigations that can be presented in legal proceedings and in corporate settings. Be it for forensic recovery of emails or data, forensics during eDiscovery can be a nightmare if not properly conducted. Use of skilled forensicians, certified laboratories, recognized industry standards and industry-leading hardware and software is recommended when extracting data in a forensically sound manner across electronic devices including medical, wearable and medical IoT devices. Security and privacy of a patient's health information — whether it is stored on paper or electronically - is often a top priority for patients, Healthcare providers, professionals and the government. Most Healthcare providers follow the federal Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule (Privacy Rule) that outlines a baseline for the protection of Protected Health Information (PHI). According to a study conducted by two physicians at Massachusetts General Hospital Center for Quantitative Health, there has been a 70% increase in Healthcare data breaches between 2010 and 2017 [29]. Data breach perpetrators often span across countries. With every data breach, investigations follow and eDiscovery of the impacted systems and data stores is part of post-mortem exercises whether on-premises at the vendor or at the law offices. With ever-tightening privacy regulations across states and countries, eDiscovery is a growing challenge and perpetrator's right to privacy is also to be accounted for. Data affected in the breach is often protected health information (PHI) and clean-up activities can sometimes be futile as the stolen data is often traded in the dark-web or dumped in cloud bins. Since this stolen data

is part of the evidence, documenting and tracking of such data is also a nightmare. Sometimes targeted entities simply notify the impacted population of a breach and pay fines to avoid legal and eDiscovery expenses. From Figure- 1, managing security and privacy can be a challenge across all the phases of EDRM. This shows the extent to which this challenge is on the minds of eDiscovery practitioners.

5.5. Medical Internet of Things (IoT)

Medical devices are increasingly getting smarter and networked. Some of them can be classified under the IoT umbrella like a portable hand-held ultrasound, home genetics tests, personal patient monitors, personal infusion pumps, etc. that connected to a tablet or Smartphone. Since they roam between wireless networks, they leave behind breadcrumbs or residual data on these networks. From Figure-1, proper disposal of such devices is a challenge as they are often discarded without much thought about residual data that they may still hold. Such devices seem to also suffer from logging, authentication and general security hygiene that complicates eDiscovery when the need arises. The market for these devices is increasing and this is only going to add to the existing eDiscovery complexities.

5.6. Wearable Devices

Lifestyle trackers, fitness trackers, smart clothing, etc. fall under the wearables umbrella. These devices have grown from simple pedo tracking, wearable therapeutic devices and calorie burning features to disposable wearable patches collecting data points off sweat and skin glands. These devices support various languages, integrate with the cloud and offer minimal logging often stored in the cloud. Few legal cases have cropped-up thus far, but in McLellan et al. v. Fitbit, Inc. [30] and a recent Canadian case [31] show that data from wearables is poised to become even more insightful for courts given their wealth of user data. Such cases also introduce other players like analytics processing companies who crunch wearable data for the legal teams. From Figure- 1, identification, collection, destruction can be a challenge. They can be challenging during production and presentation especially when striving for a near-native presentation format. For example, presenting selected data from a fitness tracker in a courtroom can be a challenge especially when trying to preset it within the frame of the device for maximum impact. Data forensics for eDiscovery from such devices suffer from cloud challenges, translation annoyance and minimal onboard storage. From the growth in the industry, the future of wearables for forensic evidence seems to further complicate such devices since it would involve human DNA on disposable wearables.

5.7. Communications and Telemedicine

As technology advances, communication and side discussions around patient care or medications, often happen over text messaging, image and video sharing, various instant messaging tools or specific vendor solutions. While some of this communications can be logged or recorded a lot just cannot be retrieved for eDiscovery analysis due to the poor design and implementations of these communication systems by IT at the Healthcare facilities. Unfortunately, IT teams do not allocate much attention to these systems apart from securing them. Telemedicine can be explained as the remote delivery of healthcare services, such as health assessments, medical images or physician consultations over the telecommunications infrastructure that can sometimes comprise mobile networks and mobile devices.From Figure- 1, identification, collection and processing can be a challenge as communica-

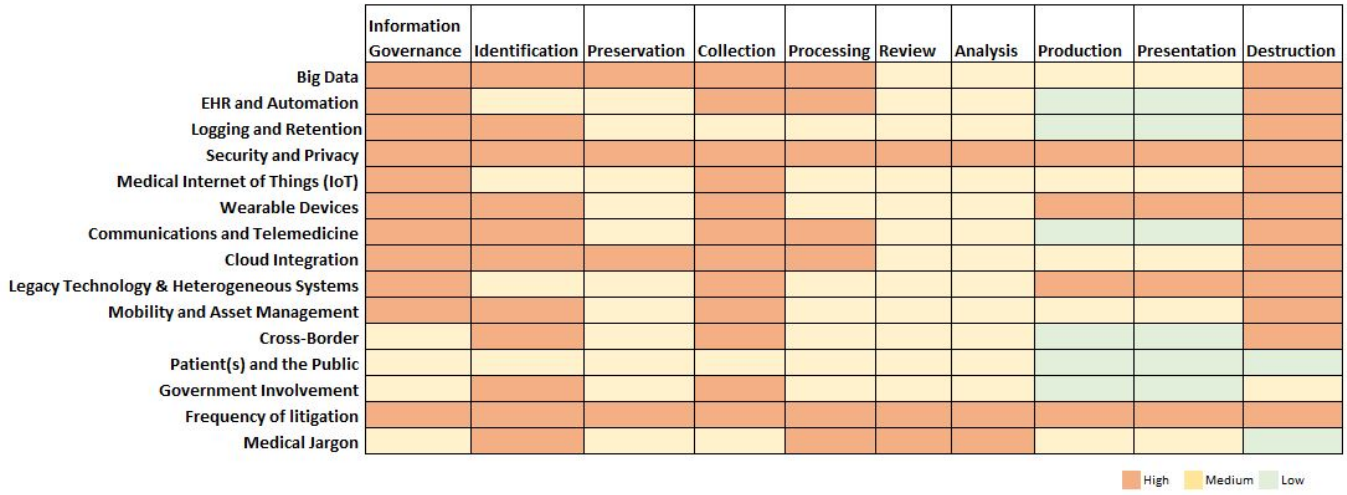

Fig. 1: Heat Map of Healthcare challenges in relation to EDRM stages from a digital perspective.

tions data can be disjoint and stored on devices or the cloud. Increasingly telemedicine has embraced the cloud complicating discovery. Medical transcription services often use the cloud for storage and any forensic examinations on such storage have proven a challenge due to cloud related geographical complexities and privacy. While communications is key to the business, adequate logging and implementing The National Institute of Standards and Technology (NIST) tele-medicine best practices [32] is recommended for a start.

5.8. Could Integration

About 91% of Healthcare practices use cloud-based services, yet 47% are not confident in their security posture due to manual workflow processes [33]. Healthcare industry is increasingly embracing the cloud for few of their systems. It is easy to get absorbed by the Cloud product offerings, but, is difficult to get out of them considering the data that would remain behind on the cloud systems [34]. From Figure- 1, identification, collection and processing can be a challenge as access to data can be limited by the legal contracts between the Healthcare provider and the cloud service provider. Unless, it is decided to copy the cloud data into local storage (post identification), mechanisms may need to be put in place to secure and preserve this data in it's original cloud storage. Legal issues are abound with Cloud services as data and infrastructure is often not owned by the user [35]. Healthcare vendors have been increasingly dependent on the Cloud due to cost benefits and the solution mobility. Cloud integration also poses challenges for eDiscovery due to international data processing regulations like EU's General Data Protection Regulation (GDPR), Japan's Act on the Protection of Personal Information (APPI) and China's new Cybersecurity Law. The rise of solutions like Office 365, DropBox, Github, AWS, etc. make it even harder for data retrieval during eDiscovery. Healthcare entities should deploy Cloud specific policies and standards along with employing Cloud best practices [36], [37]. Access to cloud services should be regulated by an experienced and dedicated technical team within the organization IT or as an outsourced service.

5.9. Legacy Technology and Heterogeneous Systems

The Healthcare market is still functioning internally and with external providers using antiquated technologies such as the fax, private automatic branch exchange (PABX), mainframes, legacy EHR systems. Data files containing sensitive data are still shared with business partners and internally on CDs, USB media sometimes without encryption. The focus is more on business continuity than technology growth. Such systems lack in-depth logging and archiving making it harder to collect forensic evidence. Such technology also contributes to the skill pool required to undertake forensic investigations. From Figure- 1, collection can be a challenge, especially from disjoint legacy systems. Production and presentation can also be challenging if the intent is to present this data in a near-native format. The authors suggest slowly replacing legacy technology with today's technology.

5.10. Mobility and Asset Management

The rise of mobile devices in the healthcare industry has made a dramatic impact in lowering the barriers to Healthcare access as well as gives patients the responsibility for their personal health. Findings of the 2017 Executive Mobility Report shows that companies face daunting technical e-discovery challenges even if their employees turn in their personal mobile devices for an investigation as discovering data on mobile devices can be difficult. This challenge applies to the Healthcare industry as well [38]. Bring Your Own Device (BYOD) like Smartphones and tablets are becoming the primary device for Physicians, Nursing staff and patients. Patient health monitoring and management is increasingly delivered through Smartphone apps. Mobile devices also include wearables, patient monitors, and other connected medical devices that communicate data over a network. However, staying agile and secure while managing mobility is a continuous challenge for the Healthcare industry. From Figure-1, collection and destruction of data from mobile devices can be a challenge if the Healthcare entity has not deployed adequate mechanisms on these devices. Often their inventory is poorly managed and tracking them can be difficult. Patient Health data may be stored on these devices or transmitted over poorly secure channels back to the provider or monitoring staff. Vendors can sometimes lag in patching vulnerabilities. The future of Healthcare IT is focusing on patient-directed data exchange, Internet of Things (IoT), and telemedicine [39], [40]. Litigations involving mobile devices can be a challenge as network transmissions may be involved in the case, forensic data extraction from these devices may be needed and fourth amendment implications need to be considered [41]. Healthcare entities like most other enterprises suffer from effective Asset management. Simple asset tracking and management tools can greatly assist along with dedicated staff. The authors suggest implementing NIST best practices [42], [43], [44] while managing mobile assets.

5.11. Cross-Border

Given today's international data privacy landscape, a discovery request or data demand across state and international borders can present a variety of challenges for organizations that are global [45]. States that border one another often have patients traveling across borders seeking medical care In KIMBERLY MONTAÑO v. ELDO FREZZA [46], the New Mexico Supreme court ruled that a Texas surgeon cannot be sued for medical malpractice in a case filed in New Mexico. Similarly, with the growth in global tourism and medical tourism,

malpractice cases and arbitration can be complicated while navigating local laws. With the stepping-up of international privacy laws, the collection stage of the eDiscovery process can be complicated as many of these laws are untested across courts beyond their jurisdiction. Data collection by law may need to be handled locally [3]. Guidelines [47], published by the E-Discovery Working Group of the New York City Bar Association, serve as a reminder of the challenges that New York State legal practitioners face when documents within the scope of a client's discovery obligations reside in a foreign jurisdiction. In such cases, foreign laws can prohibit transferring those same documents to the United States. As organizations tend to grow with mergers and acquisitions they need to be compliant with local laws and conduct periodic due diligence and risk analysis for ligation scenarios. Figure- 1 highlights this challenge as local laws can interfere when collecting data across borders. Similarly, destruction of this data can also be subject to their local laws and regulations. Being aware of cross-border legislations, working with local entities and staying abreast with the local happenings are some of the best ways to overcome this challenge.

5.12. Patient(s) and The Public

Litigation involving minor(s), emotional/mentally-impaired/aggrieved/agitated patient(s), death of individual(s) or when facing public outrage can be challenging for eDiscovery teams. Performing eDiscovery in such situations can itself be pressuring given that the litigant may not be in a competent state to assist their legal counsel. In such situations, it is imperative to have a clear understanding of issues to avoid further exposure to liability. Thomas et al. [48] focus on a list of topics and concerns based on actual court cases to highlight the high-risk medico-legal issues concerning an agitated patient so that liability can be avoided. Persistent media coverage and a growing public perception can be a challenge when litigation involves a jury. In such cases, arbitration may be an option as it produces a swifter resolution to disputes with due compensation for either party. Figure- 1 highlights this challenge. Participation of surrogates or counselors or social workers during eDiscovery interactions with such patients and being cognitive to their situation can ease eDiscovery effort to a large extent. Appropriate training of eDiscovery staff on handling such situations may also be considered.

5.13. Goverment Involvement

In addition to dealing with routine litigation, many healthcare organizations may be involved in state or federal government investigations involving certain jurisdictions, medication recalls, services provided or faulty medical devices. Such government requests can be very broad, making it imperative for the eDiscovery team to get detailed information to narrow the scope of the investigation, the goals of collection, duration of the collection period and deadlines [49]. Figure- 1 highlights identification and collection stages as challenging given the scope and limitations of the government-led investigations. Timely awareness of government-mandated investigations and their scope can better assist with overcoming this challenge.

5.14. Frequency of Litigation

The Healthcare industry is a target for litigations as it largely deals with people. Almost all health care providers have been through a litigation cycle and should be prepared with dedicated and skilled personnel. It is important to have a proven and repeatable eDiscovery process that's tailored to the or-

ganization's needs and requirements [49]. Employees and data custodians have to be similarly trained to avoid unpreparedness and blunders. Increased frequency of litigations triggers numerous EDRM cycles for each legal case. Figure- 1 highlights the toll that a Healthcare entity often undergoes due to the countless litigations that it has to handle all year round. Healthcare entities should routinely train their legal support teams and adequately staff them to overcome this challenge.

5.15. Medical Jargon, Transcription and Billing

The Healthcare industry deals with a ton of medical terminology. For a legal mind, medical procedures, equipment/device functionality, medical terminologies, disease descriptions, pharmacy terms, etc. can be a challenge. Legal teams need to engage with subject-matter experts (SME) in such situations and may impact eDiscovery costs. The healthcare market generates huge volumes of audio and video data catering to the medical transcription industry. Most Medical Transcriptionists work from home, or other locations outside the provider facility thereby necessitating complete audit trails to facilitate eDiscovery. With the growth of cloud technology, documents and medical records will be stored on cloud-based systems, making them easily accessible for outsourced transcription from any part of the globe. Provider's legal counsel should help write and review the outsourced Medical Transcription Service Organization (MTSO) contract(s) to include provisions and mechanisms for ease in eDiscovery should there be a need for one. Many legal cases relate to the billing of services rendered. Fraudulent health care providers cost-benefit plans and health insurers hundreds of billions of dollars annually. Fraudulent claims, reimbursement disputes, and incorrect provider billing can be better addressed by legal teams using sophisticated knowledge of medical coding systems and claim-form submissions. Figure- 1 highlights this challenge during identification, processing, review and analysis stages of eDiscovery.

6. Conclusion

eDiscovery trends around medical litigation continue to evolve depending on the complexity of cases. Electronic Medical Records (EMR), increased automation and mobility increasingly present challenges that both the legal and Healthcare communities must be aware of. Healthcare providers' in-house legal counsel, audit teams, Medical/Clinical security, IT Governance and IT Security teams should work in a cohesive way to be prepared for litigation challenges. Incorporating machine learning to assist with analytics can make eDiscovery workload more manageable by assisting with searches, indexing, deep-analysis, analytics, and sorting. A data management policy, retention policy and accompanying standards are needed at an organizational level. Management of EHR includes assembling representatives from legal, compliance, governance and IT early in the data retention process so that every aspect of data management and retention requirements is included in the organization's long-term plan. Since data revolves around patient care, it is imperative to design Healthcare systems and devices with eDiscovery best practices keeping in mind default logging, archiving and log preservation techniques. Accommodation for forensic collection of data and secured storage may be necessary at all levels of system design and deployment. Without such considerations, a great deal of cooperation is required among parties, their counsel, patients, regulators and stakeholders in a dispute (audit or post-incidents) as to what and where information (data) exists?, is it appropriately tagged?, can it be extracted in a targeted and

meaningful way?, is it worth extracting?, and can it be explained based on the context from which it was extracted? A Healthcare market player needs to continuously monitor litigation risk and frequently conduct an assessment of their readiness to comply with e-discovery requests.

Acknowledgments

The authors would like to thank the forensics lab at the Cyber Forensics Intelligence Center, Sam Houston State University for allowing the use of lab resources.

References

[1] "EDRM Model — EDRM." [Online]. Available: https://www.edrm.net/frameworks-and-standards/edrm-model/

[2] S. Giordano, "It's all e-discovery — Healthcare IT News," 2010. [Online]. Available: https://www.healthcareitnews.com/news/it's-all-e-discovery/

[3] "How eDiscovery Teams can Help You with Cross-Border Investigations," 2018. [Online]. Available: http://blog.specialcounsel.com/ediscovery/cross-border-ediscovery/

[4] C. Darnell, *Forensic Science in Healthcare*. CRC Press, feb 2011. [Online]. Available: https://www.taylorfrancis.com/books/9781439844915

[5] F. Khan, "The 'Uberization' of Healthcare: The Forthcoming Legal Storm Over Mobile Health Technology's Impact on the Medical Profession," may 2016. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2773786

[6] E. S. Knutsen, "The Medical Malpractice Landscape in Ontario: Facts, Trends and Analysis of Trials and Appeals," aug 2017. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3023607

[7] "2018 Litigation Trends Annual Survey." [Online]. Available: https://www.nortonrosefulbright.com/-/media/files/nrf/nrfweb/imported/20181105--2018-litigation-trends-annual-survey-pdf.pdf

[8] "Court Approves Anthem $115 Million Data Breach Settlement," 2018. [Online]. Available: https://www.hipaajournal.com/court-approves-anthem-115-million-data-breach-settlement/

[9] "Legal & Regulatory Issues." [Online]. Available: https://www.beckershospitalreview.com/legal-regulatory-issues.html

[10] "Health : Law360 : Legal News & Analysis." [Online]. Available: https://www.law360.com/health

[11] B. Inmon, "Classification of Corporate Data by Bill Inmon - BeyeNETWORK," 2014. [Online]. Available: http://www.b-eye-network.com/view/17251

[12] A. Bridgewater, "The 13 Types Of Data," 2018. [Online]. Available: https://www.forbes.com/sites/adrianbridgwater/2018/07/05/the-13-types-of-data/#70d949b63362

[13] K. Stucklin, "Tips for Successful Application of E-Discovery." [Online]. Available: https://ce.uci.edu/areas/legal/ediscovery/tips.aspx

[14] J. Rich, "Library Guides: Data Resources in the Health Sciences: Clinical Data." [Online]. Available: http://guides.lib.uw.edu/hsl/data/findclin

[15] S. Pierson, "How to Simplify 3 Common Types of eDiscovery & Document Review — Blog — Relativity," 2016. [Online]. Available: https://www.relativity.com/blog/how-to-simplify-3-common-types-of-e-discovery-and-document-review/

[16] "Naperville Smart Meter Awareness v. City of Naperville," 2018. [Online]. Available: http://media.ca7.uscourts.gov/cgi-bin/rssExec.pl?Submit=Display&Path=Y2018/D08-16/C:16-3766:J:Kanne:aut:T:fnOp:N:2203659:S:0

[17] J. Halamka, "Life as a Healthcare CIO: The Cost of Storing Patient Records," 2011. [Online]. Available: http://geekdoctor.blogspot.com/2011/04/cost-of-storing-patient-records.html

[18] "eDiscovery Analytics — eDiscovery Software — Relativity." [Online]. Available: https://www.relativity.com/ediscovery-software/analytics/

[19] "E-discovery Software & Data Analytics — Proofpoint." [Online]. Available: https://www.proofpoint.com/us/products/ediscovery-analytics

[20] I. D. Dinov, "Volume and Value of Big Healthcare Data." *J. Med. Stat. informatics*, vol. 4, 2016. [Online]. Available: http://www.ncbi.nlm.nih.gov/pubmed/26998309http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=PMC4795481

[21] R. Artigliere, C. P. Brouillard, R. D. Gelzer, K. Reich, and S. Teppler, "Diagnosing and Treating Legal Ailmentsof theElectronic Health Record:Toward an Efficient andTrustworthy ProcessforInformation Discovery and Release," *Sedona Conf.*, 2017. [Online]. Available: https://engage.ahima.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=16ceb9c5-5929-451f-b3cd-191fbb50b775

[22] "What is an electronic health record (EHR)? — HealthIT.gov." [Online]. Available: https://www.healthit.gov/faq/what-electronic-health-record-ehr

[23] "EMR vs EHR – What is the Difference? — Health IT Buzz." [Online]. Available: https://www.healthit.gov/buzz-blog/electronic-health-and-medical-records/emr-vs-ehr-difference

[24] E. Gumz, "5 eDiscovery Trends in the Healthcare Industry," 2017. [Online]. Available: https://www.hanzo.co/blog/5-ediscovery-trends-in-the-healthcare-industry

[25] "Borum v. Smith et al, No. 4:2017cv00017 -

Document 31 (W.D. Ky. 2017)," 2017. [Online]. Available: https://law.justia.com/cases/federal/district-courts/kentucky/kywdce/4:2017cv00017/101673/31/

[26] "Electronic Health Record Closed Claims Study," Tech. Rep., 2017. [Online]. Available: https://www.thedoctors.com/siteassets/pdfs/risk-management/closed-claims-studies/11220_ccs_ehr_1017_single-page_fr4_sg.pdf

[27] "Medical Record Retention Required of Health Care Providers: 50 State Comparison — Health Information & the Law," 2016. [Online]. Available: http://www.healthinfolaw.org/comparative-analysis/medical-record-retention-required-health-care-providers-50-state-comparison

[28] Warner Norcross & Judd, "Six Tips to Stop eDiscovery from Breaking the Bank in Healthcare Record Retention — HIMSS," 2015. [Online]. Available: https://www.himss.org/news/six-tips-stop-ediscovery-breaking-bank-healthcare-record-retention

[29] "Study Reveals 70% Increase in Healthcare Data Breaches Between 2010 and 2017," 2018. [Online]. Available: https://www.hipaajournal.com/study-reveals-70-increase-in-healthcare-data-breaches-between-2010-and-2017/

[30] "McLellan et al v. Fitbit, Inc." 2016. [Online]. Available: https://f.datasrvr.com/fr1/218/54618/Fitbit.pdf

[31] P. Olson, "Fitbit Data Now Being Used In The Courtroom," 2014. [Online]. Available: https://www.forbes.com/sites/parmyolson/2014/11/16/fitbit-data-court-room-personal-injury-claim/#40ac38707379

[32] "Securing Telehealth Remote Patient Monitoring EcoSystem - Draft," 2018. [Online]. Available: https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/hit-th-project-description-draft.pdf

[33] R. Hammer, "30 Healthcare Statistics That Keep Hospital Executives Up At Night," 2016. [Online]. Available: https://getreferralmd.com/2016/08/30-healthcare-statistics-keep-hospital-executives-night/

[34] A. Barsocchini and S. Maccherola, "3 Challenges to Data Collection in the Cloud," 2017. [Online]. Available: https://accessdata.com/blog/3-challenges-to-data-collection-in-the-cloud/

[35] S. Krishnan and L. Chen, "Legal Concerns and Challenges in Cloud Computing," in *2nd Int. Symp. Digit. Forensics Secur. (ISDFS 2014)*, 2014. [Online]. Available: https://arxiv.org/abs/1905.10868

[36] "NIST Cloud Computing Standards Roadmap." [Online]. Available: https://www.nist.gov/sites/default/files/documents/itl/cloud/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf

[37] "Guidelines on Security and Privacy in Public Cloud Computing." [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

[38] "2017 Executive Enterprise Mobility Report," *CITO Res.*, 2017. [Online]. Available: https://go.apperian.com/rs/300-EOJ-215/images/Apperian2017ExecutiveEnterpriseMobilityReport_FinalDraft_20170419.pdf

[39] J. Halamka, "Life as a Healthcare CIO: Remote Patient Monitoring and Self-Responsibility," 2019. [Online]. Available: http://geekdoctor.blogspot.com/2019/02/remote-patient-monitoring-and-self.html

[40] P. Cerrato, J. Halamka, P. Cerrato, and J. Halamka, "Innovations in mHealth, Part 2: Electronic Health Record–Linked Apps, Remote Patient Monitoring, and the Internet of Things," *Transform. Power Mob. Med.*, pp. 17–40, jan 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9780128149232000027

[41] H. Allen and D. Herman, "Challenges of Mobile Devices, BYOD and eDiscovery - Law Technology Today," 2014. [Online]. Available: https://www.lawtechnologytoday.org/2014/09/challenges-of-mobile-devices-byod-and-ediscovery/

[42] "Securing Electronic Health Records on Mobile Devices," 2018. [Online]. Available: https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-ehr-nist-sp1800-1.pdf

[43] "Guidelines for Managing the Security of Mobile Devices in the Enterprise," 2013. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf

[44] "Mobile Device Security," 2019. [Online]. Available: https://www.nccoe.nist.gov/sites/default/files/library/sp1800/mds-nist-sp1800-4b.pdf

[45] "Cross-Border eDiscovery Challenges — Deloitte US." [Online]. Available: https://www2.deloitte.com/us/en/pages/advisory/articles/discovery-insights-cross-border-ediscovery.html#

[46] "KIMBERLY MONTAÑO v. ELDO FREZZA," 2017. [Online]. Available: https://caselaw.findlaw.com/nm-supreme-court/1852690.html

[47] "Cross-Border E-Discovery: Navigating Foreign Data Privacy Laws and Blocking Statutes in U.S. Litigation — Member & Career Services — NYC Bar," 2018. [Online]. Available: https://www.nycbar.org/member-and-career-services/committees/reports-listing/reports/detail/cross-border-e-discovery-navigating-foreign-data-privacy-laws-and-blocking-statutes-in-us-litigation

[48] J. Thomas and G. Moore, "Medical-legal Issues in the Agitated Patient: Cases and Caveats." *West. J. Emerg. Med.*, vol. 14, no. 5, pp. 559–65, sep 2013. [Online]. Available: http://www.ncbi.nlm.nih.gov/pubmed/24106559http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=PMC3789925

[49] B. Schwartz, "Mitigating eDiscovery challenges in the healthcare industry," 2019. [Online]. Available: http://www.healthcarebusinesstech.com/mitigating-ediscovery-challenges-in-the-healthcare-industry/