Health Policy and Technology 10 (2021) 100543

Contents lists available at ScienceDirect

Health Policy and Technology

journal homepage: www.elsevier.com/locate/hlpt

Original Article

The implications of the California Consumer Privacy Act (CCPA) on healthcare organizations: Lessons learned from early compliance experiences

Pavankumar Mulgund [a,*], Banashri Pavankumar Mulgund [a,b], Raj Sharman [a,c], Raghvendra Singh [a,d]

[a] School of Management, University at Buffalo, United States
[b] LLB(Hons) UB School of Management, Unites States
[c] Professor School of Management, University at Buffalo, Unites States
[d] UB School of Management, University at Buffalo, Unites States

ARTICLE INFO

Keywords:
CCPA
HIPPA
Data privacy
Consumer health information

ABSTRACT

Objective: In 2018, California legislators passed the California Consumer Privacy Act (CCPA), a digital privacy regulation conferring consumers more control over their online personal information. CCPA is a significant regulation overseeing technology companies' data collection and usage practices in the United States. This article analyzes CCPA and its implications on healthcare organizations. We elaborate on the compliance challenges that have emerged due to the interplay of the CCPA with the Health Insurance Portability and Accountability Act (HIPAA) from legal and technical/operational perspectives.

Methods: Qualitative methods comprising semi-structured expert interviews, qualitative data coding, and analysis were used to explore the perceptions of the practitioners on various dimensions of the policy and to obtain insights from the field.

Results: Our findings indicated that California's healthcare organizations faced several legal and technological challenges in complying with CCPA. A lack of regulatory clarity and a low likelihood of enforcement emerged as two major themes of legal concern. Poor data discovery and inventory processes, lack of sophisticated digital infrastructure, the interaction between technology and privacy professionals, and the high cost of compliance emerged as significant technological hurdles to CCPA compliance.

Conclusions: Despite considerable ambiguity around the scope and jurisdiction of CCPA in the healthcare sector, healthcare organizations may be subject to CCPA, primarily when they collect personally identifiable information that is not protected health information. Such organizations may need to comply with both regulations. Furthermore, it is in their best interest to develop compliance plans proactively rather than being caught in the quandary of last-minute implementation or expensive litigation.

Public Interest SummaryInspired by GDPR and recognizing the need for a broader interpretation of privacy issues in USA California passed the California Consumer Privacy Act (CCPA). Although the regulation was created to cater to consumer industries such as ad tech, retail, and e-commerce, but it also impacts the healthcare sector in interesting ways. In this article, we examine the requirements of CCPA to understand its effect on different types of healthcare organizations. We elaborate on the interplay between the Health Insurance Portability and Accountability Act (HIPAA) and the CCPA. California's healthcare organizations faced several legal and technological challenges in complying with CCPA. A lack of regulatory clarity and low likelihood of enforcement emerged as two major themes of legal concern. Poor data discovery and inventory processes, lack of sophisticated digital infrastructure, the interaction between technology and privacy professionals, and the high cost of compliance emerged as significant technology and operational hurdles to CCPA compliance.

* Corresponding author at: Management Science and Systems, School of Management, University at Buffalo, 333 Jacobs Management Center, Buffalo, NY 14260-4000, Unites States.
E-mail address: pmulgund@buffalo.com (P. Mulgund).

https://doi.org/10.1016/j.hlpt.2021.100543

Available online 25 June 2021

Introduction

Digital privacy has assumed great significance, as web and mobile applications continue to collect and leverage online personal information to promote their business interests. However, unlike the European General Data Protection Regulation (GDPR) [1], the United States does not have one comprehensive data privacy regulation governing data collection and use [2]. Several federal and state regulations govern various sectors and types of personal information. For instance, considering the sensitivity of health information and the potentially catastrophic consequences of its breach, the protection of health information is governed by the Health Insurance Portability and Accountability Act (HIPAA). HIPAA ensures that the organization collecting and storing health information has the necessary processes and technology controls to protect health information. It also provides legal recourse to victims in the event of a breach [3]. However, such specific regulations are too narrow and quite limited.

Inspired by GDPR and recognizing the need for a broader interpretation of privacy issues, California passed the California Consumer Privacy Act (CCPA) [4]. It is a landmark regulation that will have a significant impact on the 40 million residents of the state of California and its 500,000 businesses, including the 10% of Fortune 1000 companies, which are some of the most profitable and cutting-edge technology firms [5]. Although the regulation was created to cater to consumer industries, such as ad tech, retail, and e-commerce, it impacts the healthcare sector in interesting ways [4,5]. In this article, we examine the requirements of CCPA to understand its effect on different types of healthcare organizations. We explore the legal and technological compliance challenges that emerge from the interplay between the HIPAA and the CCPA.

Background

The CCPA provides California citizens with a higher degree of control over their online personal information by providing rights over their online personal data and how companies use it. The act outlines certain restrictions and exemptions to specific data categories. The CCPA became effective on January 1, 2020, and organizations are expected to have data protection policies to comply with the new legislation [6].

CCPA applies to for-profit organizations doing business in California that collect and process consumers' personal information [7] if they meet at least one of the following criteria:

Annual gross revenue is greater than $25,000,000.

Engages in the purchase, sale, or transfer of personal information from more than 50,000 consumers, devices, or households.

Derives more than 50% of annual revenues from selling consumers' personal information [8].

The act defines 'consumer' [9] as any individual domiciled in California, including those living outside for temporary or transitional purposes. It also defines the term *personal information* [10] as information that can be reasonably linked, directly, or indirectly, to a consumer or household. Personal consumer information collected by the business can include the following [11]:

- Consumers' personal information—demographic, financial, digital
- Sources of personal information
- The purpose (business or commercial) of collecting or selling personal information
- Categories of third parties with which the business shares personal information
- Individual fields of information collected about the consumer

As presented in Fig. 1, CCPA describes various types of personal information. However, CCPA exempts publicly available information,

Protected Health Information	Non-Protected Health Information
• Names • Geocode - Zip code, city, county • All dates - admission, discharge, birth date • Phone Numbers • Fax Numbers • Electronic mail addresses • Social Security numbers • Medical record numbers • Health plan beneficiary numbers • Account Numbers • Certificate/License numbers • Vehicle identifiers and serial numbers, including license plate numbers • Device identifiers and serial numbers • Web Universal Resource Locators (URLs) • Internet Protocol (IP) address numbers • Biometric Identifiers including finger and voiceprints • Full face photographic images • Any other unique identifying number, characteristic	• postal address • unique personal identifier • online identifier • internet postal address • email address • account name • social security number • driver's license number • passport number • other similar identifiers • signature • Social security numbers • physical description • address • telephone number • passport number • insurance policy number • education • employment • employment history • bank account number • credit card number • debit card number • or any other financial information, medical information or health insurance information

Fig. 1. Classification of Personal Information *in CCPA*.

which is defined as "information that is lawfully made available from federal, state, or local government records but not if the purpose of data use is incompatible with its stated purpose" [12]. Protected health information collected by a covered entity governed by the Confidentiality of Medical Information Act and Health Insurance Portability and Accountability Act (HIPAA) is exempt from CCPA [13].

Furthermore, CCPA does not apply to nonprofits or California state and local governmental entities. Given the breadth of the CCPA's definition of business and consumer, companies across the US that collect user data and deploy cookies will be subject to compliance with the CCPA.

Consumers have been provided with several rights under CCPA, including the following:

- Disclosure [14] and access [15]

Collection, sale, or disclosure of consumers' personal information for a business purpose must be revealed to consumers [16]. A company collecting personal information should disclose the information collected in the last 12 months in response to a valid consumer request.

- Deletion

Businesses and their third-party service providers must delete the consumer's personal information collected in the last 12 months in response to a legitimate consumer request [17]. This includes the not only the personal information provided by the consumers, but also personal information collected from other sources.

- Nondiscrimination

Businesses must not discriminate against consumers who exercise any of their rights under CCPA. However, they may offer financial incentives to consumers to collect personal information with prior consent [18].

- Opt-out and website requirements

Businesses selling consumer personal information to other businesses and third-party organizations must notify consumers about the sale of their personal information and provide them with an option to opt-out. Businesses should also provide a 'Do not sell my personal information' [19] link on the website's home page to enable easy access to the 'opt-out' option. Companies should seek affirmative authorization from consumers between 13 and 16 years of age and parental consent for consumers below 13 [20].

- Privacy policy requirements

Businesses must describe their online privacy policy or any California-specific description of consumer privacy rights. The policy statement must be updated at least once a year [21].

Businesses that violate the rules specified in CCPA will be subject to an injunction. Further, they will be liable to pay the penalty not exceeding $2500 for each violation or $7500 for each deliberate violation [22].

Methods and materials

Sampling

We chose participants for interviews using purposive sampling to enable an in-depth exploration of both legal and technology implications. We shortlisted several experts from diverse areas, such as health law, digital privacy, and information systems security. Potential candidates were contacted with short recruitment messages and posts on the professional social networking platform 'LinkedIn.' From the shortlisted pool, we chose participants with substantial expertise in the intersection of digital privacy and information systems in the healthcare domain. Along with professional experience, every participant possessed expert-level certifications in digital privacy, information systems assurance, and healthcare information technology. There were no restrictions on the nature of their employment (consultant or employee) or the type of organization they worked for (management consulting, legal consulting, and technology service organizations). In total, we conducted 19 expert interviews. Table 1 provides the details of the participant's expertise.

Data collection through expert interviews

To facilitate smooth yet rigorous interviews with the experts, we created an interview guide. We pilot tested the interview questions with an expert researcher in information privacy, gathered relevant inputs, and updated the interview questions accordingly. Furthermore, based on the recommendations, the questions were framed in an unbiased tone [23]. The interview guide covered a range of topics related to our research aims. The interview questions are presented in Table 2.

Interviews were conducted virtually using Zoom and Google meetings between December 2019 and August 2020, with each session lasting between 60- and 90-min. Interviews were recorded upon consent, transcribed, and evaluated for accuracy before being analyzed. Personally, identifiable data were removed from transcriptions, and pseudonyms were used for participants. A team of three researchers (comprising the interviewer and two notetakers) interviewed the respondents and collected expert opinions. Interviewing as a team enabled better data collection, with one person facilitating the interview and the other two taking notes independently. This style of interviewing also helped aggregate the replies of the interviewees.

Data analysis

Employing the classic grounded theory approach to data analysis [24], we coded the data in three stages: open, axial, and selective coding, as presented in Fig. 2. In stage 1, we deconstructed interview transcripts into keywords and phrases called 'open codes.'

Subsequently, we grouped the keywords and phrases into ideas and concepts called 'axial codes.' Thereafter, these concepts were further grouped into higher-order themes or categories called 'selective codes.' The concepts and categories were continually refined by constantly

Table 1
Participant expertise.

Experience in years	
0–10	5
10–20	6
20–30	5
30–40	3
Organization Type	
Management Consulting	5
Technology Consulting	5
Health IT product organizations	4
Law firms	5
Job Titles	
Managing Director Founder	2
Director	5
Project/Engagement Manager	3
Lawyer/Counsel	5
Data Security/ Privacy Engineer	4
# of certifications held	
Data privacy-related:	11
CDPSE, CIPP, CIPT, CIPP-US, privacy law specialist, CDPO	
Information Security:	10
CISSP, CISA, CRISC, CISM	
Health IT-related:	3
CPHMIS, CAHMIS, HCISSP, CHTS, HIPAA	

Table 2
Expert interview guide.

1	What is your experience with information assurance, security, or regulatory compliance?
2	How are healthcare organizations affected by CCPA? What data is covered under CCPA, and what data is not?
3	How will CCPA apply to Protected Health Information (PHI) as defined by HIPAA?
4	How will CCPA apply to personally identifiable information that is not PHI? How does CCPA affect the de-identified data fields?
5	How does CCPA apply to companies that are not covered by HIPAA, like health and fitness app?
6	What healthcare data privacy issues are not well understood under CCPA?
7	What are some of the well understood data privacy issues under the ambit of CCPA?
8	What are some of the challenges that organizations face during the transition period?
9	How do companies ensure CCPA compliance for vendors?

comparing the new codes to existing codes. This process explored subtle differences and nuanced connections among the codes, enhancing their precision. Data collection and analysis were performed simultaneously, with insights from the data analysis guiding the choice of the next sample. Further, throughout the data collection and analysis, we recorded our reflections and critical insights in the form of memos that were integrated with the concepts and categories to arrive at our key findings. We illustrate the process of open coding with an example in Table 3.

We further grouped the open codes into higher-level concepts (axial codes), and using these concepts, categories (selective codes) were created. An example of mapping of open, axial, and selective codes is presented in Table 4.

We intertwined the data collection and analysis with the results of data analysis, informing and guiding our sample selection for interviews. We discuss the findings of this study in the following section.

Results

Given the focus of this study on legal and technical challenges of CCPA on healthcare organizations as perceived by professionals in the field, six different themes emerged from the analysis of interview data. Two legal themes that emerged were 1) lack of regulatory clarity and 2) the likelihood of its enforcement.

1 Lack of regulatory clarity

A broad range of healthcare organizations processing health data across the US and the world fall under the ambit of CCPA. Adopting a broad definition of personal information, CCPA carves out exceptions for specific purposes or types of well-regulated data. This approach has created ambiguity and led to situations in which the new requirements are inconsistent with prior regulations. Although the personal health

Table 3
An example open coding.

Transcript 1
"HIPAA is narrower in scope and is limited only to the protected health information. CCPA does not apply to PHI covered by HIPAA. Also, an important difference between HIPAA and a CCPA is that HIPPA does not permit the person who owns the data to limit the use of data for the express purpose only. CCPA, on the other hand, provides consumers that liberty. For example, health firms often sell protected patient information to third-party companies for advertising and other purposes for a fee. CCPA provides consumers with a means to control such use of data. However, there are areas that we are not entirely sure about, like vendor management, reporting, etc."

Transcript details	Open codes
HIPAA is narrower in scope and is limited only to the protected health information.	- Coverage of different data points
HIPPA does not permit the person who owns the data to limit the use of data for the express purpose only. CCPA, on the other hand, provides consumers with liberty.	- Data ownership differences - Greater granularity of permissions - Purpose-based access
For example, health firms often sell non-protected patient information to third-party companies for advertising and other purposes for a fee. CCPA provides consumers a means to control such use of data but HIPAA does not."	- Example highlighting differences
However, there are areas that we are not entirely certain like vendor management, reporting etc.	- Emphasizing the need for more information

Table 4
An example of mapping codes to concepts and categories.

Phase 1 (open coding)	Phase 2 (axial coding)	Phase 3 (selective coding)
Coverage of different data points	Jurisdictional scope	Regulatory clarity
Data ownership differences	Overlaps and complements between the two regulations	
Greater granularity of permissions to use data		
Purpose based access		
Data use transparency		
Emphasizing the need for more information	Missing details	
Unintended for healthcare organizations	Low priority in the enforcement of CCPA	Low likelihood of enforcement
No instance of enforcement		
Structured data sources	Inventory of Data sources	Challenges of data discovery and inventory
Unstructured data sources		
Nonproduction datasets		
Ghost databases		
Use of GRC tools	Difficulty of Data retrieval	
Unstructured data retrieval		
Incompatibility of Automatic tagging		

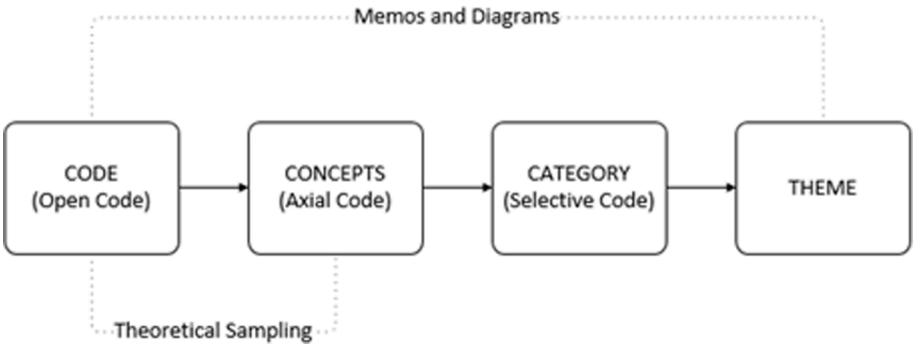

Fig. 2. Data collection and analysis process.

information covered under HIPAA is exempt from CCPA, several personally identifiable data elements collected by healthcare organizations are not PHI. Whether CCPA applies to such data is a common source of confusion.

CCPA explicitly exempts the following types of health information:

- Medical information, such as patient medical history and healthcare plan data covered under the Confidentiality of Medical Information Act (CMIA)
- PHI covered under the HIPAA. It is individually identifiable information related to the individual's physical or mental health or healthcare payment information.
- Clinical trial information and FDA requirements
- Aggregate consumer information or de-identified information

However, as illustrated by the transcript below, several types of data collected by HIPAA-compliant healthcare organizations potentially fall within the jurisdiction of the CCPA, but there is significant regulatory ambiguity around such data.

A lot of times, when you actually mention CCPA, it is applied in the absence of HIPAA. HIPAA does not really apply to Enterprise or B2B. So, the scope is very limited. I see companies they get confused because when we talk about collecting health information, whether they are subjected people. For instance, companies collecting temperature, footsteps, and activity trackers do not fall under HIPAA but are covered under CCPA.

Quote from a director of privacy and protection in a health IT product company with 15 years of experience and CIPP, CIPT certification

The following data points are some examples of such regulatory ambiguity:

- Employee data, except that which is owned by a covered entity as defined by HIPAA
- Non-PHI information of consumers collected by the covered entity
- Information received from non-HIPAA-covered entities by business associates
- Healthcare providers who do not engage in standard electronic transactions, such as cash pay services, as defined by HIPAA

Covered entities such as health plans, for instance, are increasingly leveraging non-PHI data, such as marital status, income, and television usage patterns, to assess patient risk for certain health conditions. Such use of data elements not traditionally classified as PHI by covered entities for making health-related assessments has blurred the difference between PHI as defined by HIPAA and personal information subject to CCPA, raising several regulatory concerns.

Another source of regulatory ambiguity stems from entities not covered by HIPAA or CMIA, such as clinical research organizations, biotechnology firms, wearables, fitness, and lifestyle apps, personal health record vendors, genetic test services, and assisted living facilities and services. The issue of jurisdiction of the CCPA on wearables and consumer health apps is especially common. Although wearable technologies and digital companies collect various personal healthcare data, including activity and sleep tracking, heart rates, blood glucose levels, menstrual cycles, and sexual activities, they are not covered under HIPAA, unless an HIPAA-covered entity is also involved. Therefore, such companies fall under the purview of the CCPA.

Further, the definition of '*sale* of data' is another point of confusion. The traditional definition of sale—the exchange of information for money—is covered under the CCPA. However, there is a need to interpret the broader definition of sales, such as data-sharing agreements between healthcare and non-healthcare organizations and data transfer with other agencies. The following interview transcript highlights this issue:

Yeah, so probably the biggest confusion is what actually constitutes the sale of data there. You know that you may not sell data. OK. However, you may have a, you know, you get a discount somewhere else for the data that you provide. And is that an in-kind contribution, and does that constitute a sale? That remains to be unknown. My company does not sell data. But I am sure that at some point, they will argue that no matter what, if you share data, that in some way you sell it.

Quote from data privacy and security attorney with 13 years of legal experience and CIPP-US certification

1 Likelihood of enforcement

There is some debate about the likelihood of the enforcement of CCPA in the context of healthcare organizations. On the one end, some privacy and legal professionals acknowledge that while CCPA could apply to data collected by HIPAA-compliant healthcare organizations, they also highlight the low likelihood of its enforcement. According to them, the act's primary objective was to bring digital consumer companies, ad tech, and retail organizations that collect a large volume of consumer data under its ambit. The healthcare organizations may not be a priority for enforcement agencies, but they could still be targets of expensive litigation by customers looking for non-compliant organizations[1]. The following excerpt highlights this issue:

In for-profit healthcare companies, when only personally identifiable information is captured, such as in customer relationship management or a marketing application, it is legally covered under CCPA. However, we do not believe it will be enforced. We are not seeing enforcement. It was not really who the law (CCPA) was targeted at.

Quote from a senior manager compliance and data privacy with 12 years of experience in regulatory compliance and CISM and CISSP certifications.

On the other hand, as presented in the excerpt below, some legal professionals believe that the likelihood of expensive litigation in healthcare is much higher because several law firms specialize in litigating healthcare organizations on data privacy and HIPAA-related breaches. For such firms, CCPA compliance will be a logical extension. Therefore, it is in the best interests of healthcare organizations to be proactively compliant.

Look at what has happened in the last few weeks. CCPA litigations are piling up. In my opinion, litigants will use CCPA to file cases on healthcare firms in the near term; in the longer term, it will depend on the verdicts of the first few cases.

Quote from a data privacy lawyer with 19 years of legal experience and CIPM certification

In addition to the two legal issues, the four emergent technology-related themes include 1) challenges of data discovery and inventory; 2) lack of sophisticated and robust digital infrastructure; 3) coordination between technical and privacy professionals; and 4) the high cost of compliance without an equitable ROI.

1 Challenges of data discovery and inventory

Making an inventory of all the consumers' data is the most complex technical and operational challenge that CCPA presents. In response to consumer requests, organizations should track and retrieve all consumer data. While it seems simple, discovering all consumer data is incredibly difficult to accomplish. The complexity arises because of the diversity of sources and types of data. Data is stored in several sources, including structured databases on cloud and local servers, but also on unstructured data files, such as PDFs, text files, spreadsheets, and images located in shared folders and individual computers. Some data may be stored as paper records. This challenge is most pronounced in healthcare organizations, where a large proportion of data is stored in unstructured data files and paper records. Prior studies note that nearly 80% of the clinical data generated by healthcare transactions is unstructured in nature and includes written text, radiological and X ray images, photos, pathology

[1] CCPA allows a private right of action only for certain cases of "data breaches".

slides, streaming device data, PDF files, faxes, and emails [25,26]. The following excerpts highlight this concern:

Where there are the most struggle, where they have the most difficult is not in putting up a consumer portal in asking for the request (DSAR) nor doing the basic audit tracking; it is the actual retrieval of consumer data itself. The reason that is so difficult is because it is both in structured as in relational databases such as Oracle, MY SQL could be in Mongo DB, in some type of database, and or it is sitting out in unstructured files in Word, Excel, PDFs, and finding that data is virtually impossible manually. When we have terabytes of data and we get an individual consumer's request for deletion, most of them (companies) fail there.

Quote from chief information security officer with health IT product company with 30 years of experience and CISSP and CISM certifications.

Many organizations also suffer from the existence of a large number of "Ghost Databases." On a daily basis, engineers often create and use production data dumps to test their code on staging and user acceptance test environments without any formal documentation. Such databases, over time, become good candidates for ghost databases, as noted in the following transcript:

Today, they have connectors into their core systems using API or SQL statements to those databases to retrieve the data. But those are very limited, and unfortunately, organizations have 100s, if not 1,000s, of other databases that they do not even know about.

Quote from senior privacy consultant with 8 years of experience and CIPT and CISSP certifications

1 A master data management system that provides a universal subject view of multiple data subjects, such as customers, employees, and vendors, could be a potential solution. However, most healthcare organizations are constrained in terms of the time and budget to invest in such systems.

Lack of sophisticated and robust digital infrastructure

Unlike consumer-facing digital companies, healthcare organizations usually do not possess a state-of-the art digital infrastructure. Healthcare organizations, being conservative consumers of information technology, have been slow to adopt the latest technologies, such as service-oriented architecture, cloud, and IOT. Furthermore, hospitals and healthcare agencies typically maintain their own "on-premise" data centers, whose technology infrastructure may not be sophisticated enough to adhere to this regulation. Even though several technology vendors have developed API components that assist in the automatic tagging of consumer data fields, making it easy to track and purge consumer data, healthcare organizations may not leverage these tools due to their limited ability to integrate with them, as highlighted by the transcript below:

Organizations that use conventional bare metal infrastructure or unstructured databases but are now migrating to the cloud or other new technology will face the challenges. Because these organizations do not have the ability to integrate with tools that can tag the data, they cannot run queries that allow them to purge all the data records easily.

A senior security and privacy engineer with 11 years of experience and CIPT and CISSP certifications.

1 Coordination between technology and privacy professionals

Most privacy officers are lawyers with experience in interpreting laws, but they often lack the training and experience to work with technology professionals. Similarly, IT professionals are beginning to realize that privacy professionals typically are not as technology-focused as cybersecurity and IT risk professionals. Managing expectations and ensuring meaningful communication between information system designers and privacy professionals remains a challenge. A minor change in expectations from the legal side could substantially impact the technological aspects of the project. On the other hand, IT engineers may not appreciate some of the regulatory nuances of the interplay between CCPA and HIPAA and may develop inadequate privacy controls. The following excerpt highlights this challenge.

Frankly, privacy people are not like cybersecurity people. They tend to be attorneys and do not understand how technology or complex databases work. Translating technical issues or concerns about data processes to them is a challenge Today. It is a solvable problem; however, it is still a problem today.

A director of product management with 11 years of experience in healthcare IT products and CPHIMS certification.

1 The high cost of compliance without an equitable ROI

The initial cost of compliance ranges from $50,000 at the lower segment to more than $2,000,000 at the top end. The cost of compliance is associated with the operational and information technology costs of implementing controls, training staff members, and developing improved record-keeping processes. The cost of compliance is much higher in hospitals and other health agencies that do not have a mature digital infrastructure. Furthermore, given the complexity of health information systems and the diversity of stakeholders, costs escalate in a healthcare enterprise without an equitable return on investment, as presented in the transcript below.

CCPA is an expensive undertaking for many organizations to comply with. Massive investments in newer technologies, operations, personnel, training, and audits need to be taken into account.

A founder and CEO of a health IT consulting firm with 22 years of experience

Discussion

Our study extends the line of research on data privacy regulations and their impact on healthcare organizations [27,28]. Much of the existing research on CCPA highlights its scope regarding eligibility criteria, exemptions, and penalties for non-compliant organizations. Some papers have also explored its implications for ad tech [29] and e-commerce organizations [30]. Prior work has also pointed to several categories of data collected by healthcare organizations that are not subject to HIPAA but are covered under CCPA [31]. Our study is unique as it offers a firsthand account of the legal and technical challenges involved in interpreting the regulation and developing privacy controls in the context of healthcare organizations as perceived by professionals in the field.

The vision of the CCPA is to provide consumers with greater control over their personal information and empower them to seek legal recourse in its breach and misuse. This vision transcends business domains and applies broadly to personal information. However, this regulation leads to some interesting and perhaps unintended interplay with HIPAA regulations in healthcare organizations. Therefore, it makes sense that regulatory ambiguity emerges as a frequent legal challenge. Furthermore, as other states, such as New York, Nevada, Virginia, Florida, Illinois, New Hampshire, and Washington, legislate their privacy regulations [32], issues relating to regulatory clarity will only become more complex. The interplay of these privacy regulations across states is an area for further research. We speculate that, as with the European Union GDPR, the US might at some point initiate a US-wide data privacy regulation; however, until that happens, there will be interesting regulatory challenges.

Furthermore, California privacy regulations are evolving and changing quickly. In November 2020, California passed the new data privacy bill called 'California Privacy Rights Act (CPRA),' which amends and expands the current CCPA. Several new changes have been proposed, including creating a new information category called sensitive personal information, changing CCPA scope, providing new rights to consumers, and establishing a government enforcement agency. Such rapid changes to privacy regulations have also led to some regulatory ambiguity.

Another common area of regulatory confusion revolves around the

wearable and mobile health applications industry. The data collected from these organizations were hitherto not subject to any regulatory compliance. However, with the legislation of the CCPA, data collected by mobile applications and wearable manufacturers potentially fall under its ambit. In addition, initiatives such as project Nightingale from Google, which intends to collect and process millions of patient records using AI and machine learning methods to make recommendations for improving patient outcomes, may be impacted by the CCPA. Further, the COVID-19 pandemic has exacerbated the situation, as various organizations are making enhanced use of technology to capture personal and health-related information, such as temperature scans, biometric data, location information, contact tracing, prior test results, antibody tests, and travel history, without establishing adequate data privacy safeguards. In particular, strong concerns have been expressed about specific contact tracing applications that did not meet privacy standards [33,34]. Although such practices have come under scrutiny, the issue of whether these data points are subject to the CCPA remains unclear. Further, our study also finds that, contrary to the expectations of industry leaders, the deadline for the CCPA enforcement has not been extended [35], making it necessary for businesses to develop compliance measures sooner than later.

From an implementation perspective, our study finds that the more visible components of CCPA compliance, such as building a website or setting up a helpline service for consumers to raise data access requests, are easy to accomplish. However, the task of ensuring an accurate inventory of all the consumer data collected and stored within the organization will be a challenging endeavor. Vendor management and collaboration issues between lawyers and IT teams surface as two other implementation challenges. Further, our study also notes that smaller healthcare organizations, especially those managing their on-premise data infrastructures, may not possess sophisticated technology infrastructure to deploy plug-and-play compliance engines, making them especially vulnerable to data breaches.

Limitations

As with any qualitative study, the interpretive nature of this study limits the generalizability of its results. However, because the primary objective is to explore the unintended challenges that the CCPA presents for HIPAA-compliant healthcare organizations, we provide a rich narrative from legal and technology perspectives. The readers are asked to exercise caution when assessing the transferability of this work to non-healthcare organizations. Furthermore, this study's results apply only to a small subset of healthcare organizations that fall under the purview of CCPA and HIPAA. Future studies could validate the findings of this work by leveraging other research methods. We hope that our work will provide an impetus for future studies in this area.

Conclusion

CCPA is a landmark regulation that provides consumers with greater control over their data. While it was regulated for digital consumer companies, online advertising, and retail industries, its definition is not confined to a particular industry. However, the institution of CCPA has led to some unintended effects on healthcare organizations. In this study, we present the challenges perceived by technology and legal teams. Amid all these challenges, it is prudent for these organizations to proactively comply with CCPA rather than getting involved in expensive legal battles. A clear understanding of their jurisdiction and exemptions will help organizations comply effectively. Further, studying the economic, technological, and operational effects of CCPA is vital to developing best compliance practices.

Funding

None

Ethical approval

Not required

Declaration of Competing Interest

None declared

Acknowledgement

We would like to thank the experts for consenting to participate in the interviews.

References

[1] Blanke JM. Protection for 'inferences drawn': a comparison between the general data protection regulation and the California consumer privacy act. Glob Privacy Law Rev 2020;1(2). https://doi.org/10.2139/ssrn.3518164. https://doi.org/.
[2] Solove DJ. A brief history of information privacy law. Proskauer on privacy. Practising Law Institute 2016. GWU Law School Public Law Research Paper No. 215.
[3] Baumer D, Earp JB, Payton FC. Privacy of medical records: IT implications of HIPAA. ACM SIGCAS Comput Soc 2000;30(4):40–7. https://doi.org/10.1145/572260.572261.
[4] Harding EL, Vanto JJ, Clark R, Hannah Ji L, Ainsworth SC. Understanding the scope and impact of the California consumer privacy act of 2018. J Data Prot Privacy 2019;2(3):234–53.
[5] Helveston MN. Reining in commercial exploitation of consumer data. Penn St L Rev 2018;123:667. https://elibrary.law.psu.edu/pslr/vol123/iss3/3.
[6] Saquella AJ. Personal data vulnerability: constitutional issues with the California Consumer Privacy Act. Jurimetrics 2020;60(2):215–45.
[7] Goldman E. An introduction to the California Consumer Privacy Act (CCPA). Santa Clara Univ; 2020. https://doi.org/10.2139/ssrn.3211013. *Legal Studies Research Paper*.https://doi.org/.
[8] California Civil Code. The California Consumer Privacy Act of 2018 Cal. Civ. Code § 1798.140(c)(1). Cal Civ Code § 1798.140(c)(2).
[9] California Civil Code. The California Consumer Privacy Act of 2018 Cal. Civ. Code 1798. 140(g).
[10] California Civil Code. The California Consumer Privacy Act of 2018 Cal. Civ. Code § 1798. 140(o)(1).
[11] California Civil Code. The California Consumer Privacy Act of 2018 Cal. Civ. Code § 1798. 80(e).
[12] California Civil Code. The California Consumer Privacy Act of 2018 Cal. Civ. Code § 1798.
[13] Rothstein MA, Tovino SA. California takes the lead on data privacy law. Hastings Cent Rep 2019;49(5):4–5. https://doi.org/10.1002/hast.1042.
[14] California Civil Code. The California Consumer Privacy Act of 2018. Cal. Civ. Code § 1798. 115.
[15] California Civil Code. The California Consumer Privacy Act of 2018. Cal. Civ. Code § 1798.100(d).
[16] California Civil Code. The California Consumer Privacy Act of 2018. Cal. Civ. Code § 1798.110.
[17] California Civil Code. The California Consumer Privacy Act of 2018. Cal. Civ § 1798.105.
[18] California Civil Code. The California Consumer Privacy Act of 2018. Cal. Civ § 1798.125(1).
[19] California Civil Code. The California Consumer Privacy Act of 2018. Cal. Civ. Code § 1798.135.
[20] California Civil Code. The California Consumer Privacy Act of 2018. Cal. Civ. Code § 1798.120(d).
[21] California Civil Code. The California Consumer Privacy Act of 2018. Cal. Civ. Code § 1798.130 (5).
[22] California Civil Code. The California Consumer Privacy Act of 2018.Cal. Civ. Code § 1798.155.
[23] Rowley J. Conducting research interviews. Manage Res Rev 2012;23. ISSN: 2040-8269.
[24] Kallio H, Pietilä AM, Johnson M, Kangasniemi M. Systematic methodological review: developing a framework for a qualitative semi-structured interview guide. J Adv Nurs 2016;72(12):2954–65. https://doi.org/10.1111/jan.13031.
[25] Augustine DP. Leveraging big data analytics and Hadoop in developing India's healthcare services. Int J Comput Appl 2014;89(16):44–50. Mar 26.
[26] Assale M, Dui LG, Cina A, Seveso A, Cabitza F. The revival of the notes field: leveraging the unstructured content in electronic health records. Front Med 2019 Apr 17;6:66.
[27] McGraw D, Mandl KD. Privacy protections to encourage use of health-relevant digital data in a learning health system. NPJ Digit Med 2021;4(1). https://doi.org/10.1038/s41746-020-00362-8. 1-1.
[28] Kwon J, Johnson ME. Health-care security strategies for data protection and regulatory compliance. J Manage Inf Syst 2013;30(2):41–66. https://doi.org/10.2753/MIS0742-1222300202.

[29] Maalouf M, Rozen M. CCPA reflections on the eve of enforcement and in the midst of a global pandemic. Comput Law Rev Int 2020;21(3):65–9. https://doi.org/10.9785/cri-2020-210302.
[30] Brazhnik, T. Cookies in e-commerce: balancing privacy and business. *SSRN* 2366262. 2013. https://doi.org/ 10.2139/ssrn.2366262.
[31] Harris R. Forging a path toward meaningful digital privacy: data monetization and the CCPA. Loyola Los Angeles Law Rev. 2020;54(1):197.
[32] Zachary RW, Andrew JS, Justin PW, Sarah AS. CCPA enforcement begins amid pandemic and regulatory uncertainty. Natl Law Rev 2020. XI:113 [.1], https://www.natlawreview.com/article/ccpa-enforcement-begins-amid-pandemic-and-regulatory-uncertainty (Accessed on April 19th, 2021).
[33] Bradford L, Aboy M, Liddell K. COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes. J Law Biosci 2020;7(1):lsaa034. https://doi.org/10.1093/jlb/lsaa034.
[34] Sowmiya B, Abhijith VS, Sudersan S, Sundar RS, Thangavel M, Varalakshmi P. A survey on security and privacy issues in contact tracing application of Covid-19. SN Comput Sci 2021;2(3). https://doi.org/10.1007/s42979-021-00520-z. 1-1.
[35] Robins M. American privacy law at the dawn of a new decade (and the CCPA and COVID-19): Overview and practitioner critique. Marquette Intell Prop Law Rev 2020.