AHLA

VOLUME 18 ISSUE 2 October 2018

HIT News

A Publication of the American Health Lawyers Association
Health Information and Technology Practice Group

Table of Contents

California Consumer Privacy Act of 2018 Promises to Change the Nature of Privacy Rights in the United States

Adam H. Greene
Davis Wright Tremaine LLP
Washington, DC

On June 28, 2018, California passed the California Consumer Privacy Act of 2018 (CCPA), arguably the most comprehensive privacy law in the country.[1] The effective date is January 1, 2020, but the time is now for entities to begin the analysis of whether the law will apply and, if so, how they will need to revise their privacy programs. The following discusses the background of the CCPA, to what extent it will apply to health care entities, and what will be required for compliance.

A Rush to Change the Face of Privacy Law

In contrast to many other developed countries, the U.S. does not have a comprehensive privacy law. We have various sectorial laws, such as the Health Insurance Portability and Accountability Act (HIPAA)[2] in health care, the Gramm-Leach-Bliley Act[3] governing financial institutions, and the Family Educational Rights and Privacy Act governing educational institutions.[4] The Privacy Act of 1974 governs federal agencies.[5] States have various privacy laws governing medical records, sensitive conditions, state agencies, and breach notification. The closest the country has come to a comprehensive privacy law is Section 5 of the Federal Trade Commission (FTC) Act, which broadly prohibits unfair and deceptive trade practices.[6] The FTC has interpreted the Act to require reasonable privacy and security practices, although even this authority generally does not apply to nonprofit entities.[7] In the U.S., it is quite possible for an entity, such as a nonprofit that is not in a regulated sector, to fall outside of any federal or state privacy laws.

In contrast, the EU has the General Data Protection Regulation (GDPR), effective May 25, 2018.[8] The GDPR provides EU residents broad privacy rights with respect to their personal information, such as certain consent rights and a "right to be forgotten." As the compliance date approached,

PRIVACY POLICY

many U.S. organizations with sufficient ties to EU residents overhauled their privacy compliance programs to comply with GDPR.

As U.S. businesses were struggling to comply with GDPR's broad privacy requirements, an unlikely trio in California introduced a ballot to provide California residents even greater privacy rights.[9] The trio consisted of a real estate developer, who personally contributed millions of dollars to the effort, a financial industry executive, and a Central Intelligence Agency analyst. Their ballot initiative, titled the California Consumer Privacy Act of 2018, would provide California residents with rights to learn what personal information businesses were collecting, the right to opt out of the sale of personal information, and substantial penalties for noncompliance.[10] The initiative's backers state that they collected approximately 629,000 California residents' signatures to place the measure on the ballot.[11]

Facing the likelihood of the ballot measure passing, and amid vocal concerns from industry about its impact, two California legislators struck a deal with the initiative's backers.[12] The backers would withdraw the ballot initiative prior to the June 28, 2018 deadline for withdrawal of such an initiative, if the California legislature enacted a similar proposed bill by that date. This deal led to a scramble to enact the most comprehensive privacy statute in U.S. history within a week, and without any meaningful opportunity for debate. The result: a statute that will have a huge impact on how personal information is maintained and disclosed in California; that will impact the rest of the country; and that many believe has significant flaws to be addressed in the coming year.

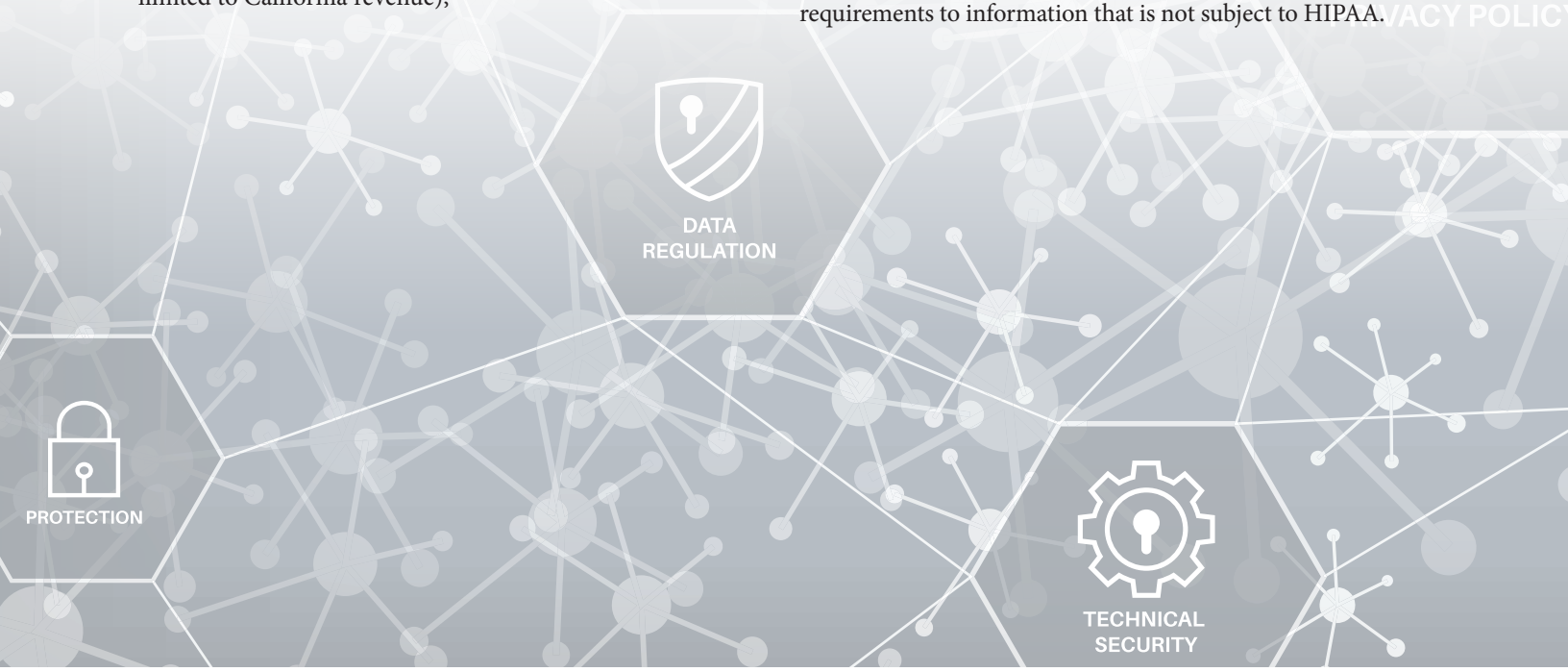
Who the CCPA Does and Does Not Govern in Health Care

The CCPA governs any "business" that does business in California and meets any of the following three criteria:

- Has annual gross revenue of more than $25 million (not limited to California revenue);
- Annually buys, receives for commercial purposes, sells, or shares for commercial purposes the personal information of 50,000 or more California residents, their households, or devices; or
- Derives 50% or more of its annual revenues from selling California residents' personal information.[13]

Of note, the CCPA does not encompass nonprofits. In that sense, the U.S. still does not have a truly comprehensive privacy law at the federal or state level. Accordingly, many health care entities, ranging from most hospital systems to some of the largest California health plans, fall outside of the statute.

The CCPA also has certain health care exemptions. It excludes protected health information that is collected by a HIPAA covered entity.[14] It incorporates HIPAA's definitions of "protected health information" and "covered entity," but originally failed to mention business associates. Since passage of the CCPA, however, the California legislature has passed amendments that also exempt protected health information that is collected by a business associate, although the amendments were awaiting the Governor's signature as of the writing of this article.[15] Additionally, for a HIPAA covered entity, the CCPA would apply to California residents' information that is not protected health information (e.g., information about website visitors who are not patients, visitors to gift shops and parking garages, etc.), assuming that the covered entity is a for-profit entity. The amendments (that await the Governor's signature) will exempt all "patient information" of a HIPAA covered entity, but only to the extent that the covered entity maintains patient information in the same manner as protected health information.[16] This change likely will have limited impact, however, since it still does not exempt information that is not "patient information," and because it only exempts patient information that is protected in the same manner as protected health information, whereas covered entities likely do not apply HIPAA requirements to information that is not subject to HIPAA.



The CCPA's health care exemption also excluded "health information" that is governed by the Confidentiality of Medical Information Act (CMIA). The provision then stated that "medical information" has the same definition as set forth in the CMIA. The reference to "health information" here was likely a mistake, as the CMIA governs "medical information," rather than "health information."[17] The amendment awaiting the Governor's signature will fix this drafting error, solely referring to "medical information" in reference to the CMIA. This provision means that for-profit health care entities in California that are not governed by HIPAA (e.g., a health care provider that does not electronically conduct transactions with health plans) arguably will need to comply with CCPA with respect to non-medical information (e.g., website visitors, gift shop and parking garage visitors, etc.), unless the information is "patient information" that is maintained in the same manner as medical information. In light of case law holding that demographic information of patients that does not reveal medical history, diagnosis, or care is not "medical information," the CCPA arguably governs for-profit organizations' patient demographic information of California residents, unless the information is subject to HIPAA and the HIPAA exemption, or unless the organization maintains such non-medical information in the same manner as medical information.[18] If you find these exemptions very confusing to navigate, rest assured that you are not alone.

What Information Is Governed?

The CCPA will govern "personal information" of California residents. But the definition of "personal information" is far broader than that which is found in California's information security and breach notification laws (or any other state's breach notification law, for that matter).[19] The CCPA broadly defines "personal information" as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." It includes direct identifiers such as name or Social Security number, but also less commonly-regulated identifiers such as Internet Protocol addresses, biometric information, and geolocation information. It includes professional or employment-related information. Befitting the initiative backer's focus on technology companies, "personal information" includes purchase histories and consumer profiles that are created based on inferences (e.g., an inference that an individual has certain political leanings based on the news sites the individual most frequents). Further, the definition of "personal information" is not limited to online information, but rather includes information gathered offline as well. The definition of "personal information" also excludes publicly available information.

There is some debate about whether "personal information" governs employee information. The CCPA generally refers to "consumers," which suggests that it is focused on commerce and is not intended to encompass employee information. But the definition of "consumer" broadly encompasses "a natural person who is a California resident," which seemingly encompasses a business' California employees.[20] The fact that "personal information" explicitly includes "employment-related" information seems to further support the view that the law encompasses a business' employee information.

CCPA does not restrict a business' ability to use, retain, sell, or disclose deidentified or aggregate information.[21] "Deidentified information" is defined differently than under HIPAA. Under CCPA, "deidentified information" cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that the business has: (i) implemented technical safeguards that prohibit reidentification of the consumer; (ii) implemented business processes that specifically prohibit reidentification of the information; (iii) implemented business processes to prevent inadvertent release of deidentified information; and (iv) makes no attempt to reidentify de-identified information.[22] Accordingly, CCPA does not require HIPAA's "expert determina-

tion" or "safe harbor" methods of de-identification, but instead requires additional safeguards for deidentified information as compared to HIPAA.[23]

The CCPA's Requirements

While CCPA is different than GDPR in a large number of respects, it is the closest U.S. law in terms of its broad definition of "personal information" and the breadth of rights it provides to consumers. If a for-profit entity is governed by the CCPA, then the business will need to understand its data flows to be able to respond to consumer requests for information about disclosures and for deletion of records. More specifically, the CCPA will require:

- **Right of Deletion.** A California resident will have a right to request that a for-profit business delete any personal information about the resident that the business has collected.[24] This deletion right, however, includes a number of significant exceptions; such as if the business deems it necessary to maintain the personal information in order to "use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information."[25]
- **Right to Information about Collection and Disclosures.** A California resident will have a right to request that the business inform the resident of: (i) the categories of personal information it has collected about the resident; (ii) the categories of sources from which the personal information is collected; (iii) the business or commercial purpose for collecting or selling personal information; (iv) the categories of third parties to whom personal information is disclosed; and (v) the specific pieces of personal information the business has collected about the resident.[26]
- **Online Privacy Policy.** The business must have an online privacy policy that informs California residents of their right to deletion of their personal information.[27] The policy also must state whether or not the business sells California residents' personal information or discloses such information for business purposes and, if so, the categories of personal information it has sold or disclosed for business purposes.[28] The policy also must include a list of categories of personal information that the business has collected about California residents in the preceding 12 months, such as whether it has collected identifiers (e.g., name, Social Security number, etc.), commercial information (such as products or services purchased), biometric information, Internet activity (e.g., browsing or search history), or inferences about consumers (e.g., likes, dislikes, political preferences, etc.).[29]
- **Sale of Personal Information or Disclosure for Business Purposes.** A California resident will have the right to request that a business that sells the resident's personal information, or that discloses it for a business purpose, disclose: (i) the categories of personal information that the business collected about the resident; (ii) the categories of personal information that the business sold, and the categories of third parties to whom it was sold; and (iii) the categories of personal information that the business disclosed about the resident for a business purpose.[30]
- **Opt Out of Sale of Personal Information.** A for-profit business that sells personal information will need to include a clear and conspicuous link on its home page titled "Do Not Sell My Information."[31] By clicking on this link or otherwise submitting a request, a California resident will have the right to opt out of the sale of the resident's personal information.[32] Furthermore, if a business has actual knowledge that a resident is 16 years old or younger, then the business will need to receive the affirmative opt in from the resident (if age 13 to 16) or the parent or guardian (if younger than 13) for the sale of personal information.[33]
- **Anti-Discrimination.** A business cannot discriminate against a California resident based on the resident exercising CCPA rights, including by charging differently for a product or service (e.g., making a health care app free unless the consumer opts out of sale of personal information).[34] A business may, however, provide a financial incentive to a California resident tied to collection, sale, or deletion of personal information.

Penalties for Violating the CCPA

What may be the biggest impact of the CCPA are the penalties. First, the law provides a private right of action for victims of breaches under California's existing breach notification law, even if they do not suffer harm.[35] This is limited to breaches of "personal information" as the term is defined more narrowly under a pre-existing information security law,[36] rather than the broader definition in CCPA. California residents can recover between $100 and $750, per individual and per incident, if their unencrypted personal information is subject to unauthorized access and exfiltration, theft, or disclosure due to a business' failure to implement and maintain reasonable security procedures and practices. Accordingly, if a single breach incident involves the theft of 100,000 California's residents' records, you can expect a class action suit for $75 million to follow shortly.

In the past, a significant obstacle to such a suit would be proving whether the information was actually used in a harmful manner. Under the CCPA, that will no longer be necessary. This is familiar ground for California health care entities, who face similar penalties of up to $1,000 per person for violating CMIA, without the plaintiffs needing to demonstrate harm (which has resulted in multi-billion dollar class action suits). Now other businesses in California are in a similar situation, with the floodgates for class action suits likely opening wider. The CCPA does provide that, before initiating suit, a California resident must provide 30-day notice and an opportunity to cure any violation if cure is possible, but it is not clear how cure will be possible if information has been exfiltrated or otherwise stolen.

Second, the California Attorney General can impose civil penalties of up to $7,500 for any knowing violation of the CCPA, such as a failure to timely respond to an individual's request for dele-

tion or for a deficient online privacy policy.[37] As with the private right of action, businesses have 30 days to cure violations, but it is not clear whether discontinuing a practice that violates the CCPA constitutes a "cure" of prior violations.

Next Steps

The effective date for CCPA is January 1, 2020. This may seem very distant, but so did the compliance dates for HIPAA and GDPR at one time. As with those laws, compliance with the CCPA is going to be a significant project that will take many months of planning and execution. Health care entities should consider the following steps now:

- Determine whether they are entirely exempt from CCPA, such as because they are nonprofit;
- If covered by the CCPA, consider whether some information is exempt, such as protected health information that is subject to HIPAA (if a covered entity) or medical information that is subject to CMIA;
- For information that remains subject to CCPA, map out information flows of personal information to be able to identify what information is collected, from whom, to whom it is disclosed, when it can be deleted at a consumer's request, and when it is sold or disclosed for business purposes;
- Begin building processes to respond to California resident requests, such as requests for deletion, disclosure of information, or opt out of sale of personal information;
- Begin to plan changes to your online privacy policy, including addition of significantly more detail on how information is collected and disclosed, and information about new CCPA rights; and
- Batten down the hatches around information security, such as through thorough risk assessment and management and extensive use of encryption, as an information security breach after 2020 may be far more costly due to increased class action litigation risks.

Finally, stay tuned for changes to CCPA. There is widespread recognition that, due to the legislative rush, the statute has significant room for improvement. There is a high likelihood of amendments. The CCPA also is creating renewed efforts for federal privacy legislation that, if enacted, could preempt CCPA and other state laws.

---

1 Assem. Bill 375, 2017-2018, ch. 55, 2018 Cal. Stat., https://leginfo.legislature.ca.gov/faces/billPdf.xhtml?bill_id=201720180AB375&version=20170AB-37591CHP (to be codified at Cal. Civ. Code §§ 1798.100 to .198) (hereafter "CCPA").

2 The Administrative Simplification subtitle of the Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health Act and otherwise, and its implementing regulations at 45 C.F.R. parts 160 to 164 (collectively, "HIPAA").

3 15 U.S.C. §§ 6801- 6803; 16 C.F.R. pt. 313.

4 20 U.S.C. § 1232g; 34 C.F.R. pt. 99.

5 5 U.S.C. § 552a.

6 15 U.S.C. § 45.

7 The Federal Trade Commission recently requested that Congress grant the agency more authority over data privacy and security, as well as explicit authority over nonprofit entities and common carriers. *See FTC Testifies before House Energy and Commerce Subcommittee about Agency's Work to Protect Consumers, Promote Competition, and Maximize Resources,* FTC, www.ftc.gov/news-events/press-releases/2018/07/ftc-testifies-house-energy-commerce-subcommittee-about-agencys (July 18, 2018).

8 Commission Regulation 2016/679, EU General Data Protection Regulation 2016/619, 2016 O.J. (L. 119).

9 Daisuke Wakabayashi, *Silicon Valley Faces Regulatory Fight on Its Home Turf,* N.Y. Times, May 13, 2018, https://www.nytimes.com/2018/05/13/business/california-data-privacy-ballot-measure.html.

10 California Consumer Privacy Act of 2018 (ballot initiative submitted to California Office of the Attorney General), Nov. 17, 2017, https://oag.ca.gov/system/files/initiatives/pdfs/17-0039%20%28Consumer%20Privacy%20V2%29.pdf (accessed July 20, 2018).

11 Californians for Consumer Privacy, *California Consumer Privacy* Act, https://www.caprivacy.org/ (accessed July 20, 2018).

12 *Lawmakers reach deal on privacy bill if initiative is withdrawn,* Cal. News Publishers Ass'n, June 22, 2018, https://cnpa.com/lawmakers-reach-deal-on-privacy-bill-if-initiative-is-withdrawn/ (accessed July 30, 2018).

13 CCPA at Cal. Civ. Code § 1798.140 (definition of "business").

14 CCPA at Cal. Civ. Code § 1798.145(c).

15 Sen. Bill 1121, 2017-2018, at Sec. 10 (to be codified at Cal. Civ. Code § 1798.145(c)(1)(A)).

16 Sen. Bill 1121, 2017-2018, at Sec. 10 (to be codified at Cal. Civ. Code § 1798.145(c)(1)(B))

17 Cal. Civ. Code § 56.05.

18 *Eisenhower Med. Ctr. v. Super. Ct. (Malanche),* 226 Cal.App.4th 430 (2014) (holding that "medical information" does not encompass demographic or numeric information that does not reveal medical history, diagnosis, or care.

19 CCPA at Cal. Civ. Code § 1798.140(o) (definition of "personal information"); cf. Cal. Civ. Code §§ 1798.81.5 and .82(h) (definitions of "personal information" in California's information security law and one of California's breach notification laws).

20 CCPA at Cal. Civ. Code § 1798.140(g) (definition of "consumer").

21 CCPA at Cal. Civ. Code § 1798.145(a)(5).

22 CCPA at Cal. Civ. Code § 1798.140(h).

23 45 C.F.R. § 164.514(b)(1) ("expert determination" method of de-identification) and (2) ("safe harbor" method of de-identification).

24 CCPA at Cal. Civ. Code § 1798.105(a).

25 CCPA at Cal. Civ. Code § 1798.105(d)(9).

26 CCPA at Cal. Civ. Code § 1798.110.

27 CCPA at Cal. Civ. Code §§ 1798.105(b) and .130(a)(5)(A).

28 CCPA at Cal. Civ. Code §§ 1798.115(c) and .130(a)(5)(C).

29 CCPA at Cal. Civ. Code §§ 1798.110(c) and .130(a)(5)(B).

30 CCPA at Cal. Civ. Code § 1798.115(a).

31 CCPA at Cal. Civ. Code § 1798.135(a)(1).

32 CCPA at Cal. Civ. Code § 1798.120(a).

33 CCPA at Cal. Civ. Code § 1798.120(d).

34 CCPA at Cal. Civ. Code § 1798.125(a).

35 CCPA at Cal. Civ. Code § 1798.150(a).

36 Cal. Civ. Code § 1798.81.5.

37 CCPA at Cal. Civ. Code § 1798.155.

Editor's Column

Gerard M. Nussbaum
Zarach Associates LLC
Chicago, IL

Welcome to the October 2018 issue of *HIT News*. This issue showcases the breadth of areas covered by the Health Information and Technology Practice Group (HIT PG), including Adam Greene's article on the new California consumer privacy law; an article on the key interrelationships between information security agreements with vendors and managing privacy and data security risks, by Alex Davenport and Shelley Thomas; and an introduction to connected medical devices by Bill Berglund. We thank all of the authors for their contributions!

These contributions show the strength and involvement of the HIT PG Affinity Groups (AGs), as these articles were developed and brought forward through our AGs (Digital Health, Tech Licensing and Intellectual Property, and Privacy and Cybersecurity Risk, Compliance and Enforcement). If you are not already familiar with the activities of these three AGs, I encourage you to not only find out, but get involved!

We are always interested in articles, suggestions for publications, and volunteers to share their knowledge and expertise with their peers. Please reach out to me at Gerard@zarachassociates.com with any suggestions, questions, or interest in participating. If you have a topic, that is great; if you are interested in participating, we can match you up with others who share your interests. Don't wait until the New Year to make a resolution to become more actively involved in the HIT PG—do it now! I look forward to hearing from you.

Best,
Gerard

Using Information Security Agreements to Manage Privacy and Data Security Risks in Vendor Relationships

Alex Davenport
Shelley Thomas
Bass Berry & Sims PLC
Nashville, TN

Health care organizations routinely engage third-party vendors to provide information technology (IT) related services. These third-party vendors help the organization lower costs, improve efficiencies, and bolster capabilities. However, the outsourcing of hosting, maintaining, and securing sensitive data, including protected health information (PHI), increases the risk of a data or security breach and gives the health care organization less control over the security measures used to prevent the breach and response plans implemented to mitigate it. In today's world, where data breaches have become more of the norm rather than occasional outliers, vendor outsourcing relationships should be subject to stricter scrutiny to ensure that the vendors are taking the appropriate steps to comply with applicable laws and the health care organization's own policies, procedures, and expectations as it relates to data and network security.

Vendors often promote their high standards for privacy and data security in their marketing pitches and materials, but fail to document those when it comes time to execute the actual agreement—leaving the data owner with little visibility into the vendor's actual practices and no remedy or recourse if those standards are not upheld. An effective tool and contracting strategy to combat those issues is an information security agreement (ISA).This article sets forth guidelines for developing and integrating ISAs into your contracting practices to ensure adequate protection of your organization's critical business processes and information technology assets.

What legal and business considerations should your organization contemplate before developing an Information Security Agreement?

ISAs should be drafted and designed to ensure that vendors protect your organization's data and systems in a manner that: (i) meets or exceeds your organization's own practices; (ii) adheres to your organization's policies and procedures; and (iii) complies with applicable laws, regulations, and industry standards. An ISA is not a one-size-fits-all document. Instead, there are several legal and business considerations your organization should take into account before defining your organization's privacy and data security requirements in an ISA, including:

- The size, scope, and type of your business and other services or activities.

- Your information collection and use practices, including the amount and types of personal and other sensitive data your organization maintains and stores.
- The need to secure both patient and employee personal information.
- Specific applicable legal requirements and industry standards, such as:
  - The Health Insurance Portability and Accountability Act (HIPAA);
  - The Health Information Technology for Economic and Clinical Health Act (HITECH);
  - The National Institute of Standards Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity, which provides various globally-recognized and accepted standards and best practices used as a minimum standard of care for many organizations;
  - State-specific statutes and regulations; and
  - International laws and regulations. For example, if your organization handles personal information (i) of non-U.S. residents or (ii) plans to transfer personal information to or from the U.S., your organization may be subject to data security or privacy laws in other jurisdictions. Privacy laws vary significantly, and can be more stringent outside of the U.S., especially in the European Union.[1]

What standard provisions should be included in an Information Security Agreement?

An ISA should define and obligate vendors to meet a minimum standard of care for privacy and data security. Your organization's minimum standard of care should include administrative, logical, technical, and physical security requirements that each vendor shall maintain to protect the availability, confidentiality, and integrity of all data made available by your organization. Although the requirements outlined below represent "standard" provisions typically found in an ISA, it is important to note that the list below is not exhaustive and should be used by your organization as a starting point when drafting (or re-visiting and updating) your ISA.

- **Access Controls.** Define access controls that limit vendors' access to your organization's data, networks, and IT systems.
  - Limit vendors access to your organization's IT systems and use of your data solely to the extent required to perform the services agreed upon, unless your organization specifically grants written authorization.
  - Prohibit vendors from disclosing your organization's data to third parties except as specifically authorized in writing by your organization (including to subcontractors).
  - Require vendors to logically and physically separate your organization's data from vendors' other customers' data.
- **Vendor Personnel.** Document specific privacy and data security obligations for vendors' personnel and other third party service providers.

- Require vendors to contractually obligate its subcontractors or other service providers to the same security standards set forth in the ISA and to engage in the management and oversight necessary to ensure compliance by third parties.
- Require vendors to perform background investigations on all personnel performing services or otherwise having access to your organization's data and contractually obligate vendors' subcontractors to do the same. Prohibit personnel who have a criminal conviction involving a dishonest act (e.g., fraud, theft, embezzlement) from performing services and accessing your data.

- **Physical Security Requirements.** Require physical security protocols that obligate vendors to maintain industry standard controls on physical infrastructure and facilities where your organization's data is handled or accessed.
  - Require vendors to maintain specific controls and procedures over facilities where data is received, processed, filed, or stored and where your network is accessed, including without limitation appropriate alarm systems, card access systems, visitor access procedures, and security guards to prevent damage and unauthorized access.
  - Require secure storage of physical files, workstations, and devices (e.g., mobile phones).
- **System and Network Security.** Define requirements for vendors' adoption of policies and procedures to prevent and monitor unauthorized access, misuse, or modification of vendors' networks and systems and enforce requirements through your organization's audit right and reporting requirements (further discussed below).
  - Require vendors to implement firewalls, restrict network traffic, properly segment vendors' network, and maintain anti-virus software, configuration management, and patch management.
  - Require industry standard practices for intrusion detection and prevention systems to detect inappropriate, incorrect, or anomalous activity and establish and follow operational procedures to stop or mitigate any potential attack or attempted attack.
  - Ensure the encryption of data (consistent with validated cryptography standards as specified in NIST or other standards) at all times during storage and transmission.
- **Back-up; Business Continuity and Disaster Recovery (BCDR).** Require vendors to develop and maintain procedures to resume operations following a security incident and to reduce the risk of data loss. Organizations typically request BCDR plans in their RFP as a diligence point.
  - If applicable, require vendors to back-up your organization's data; and recover destroyed, corrupted, lost, misused or damaged data within specific timeframes and assurances of off-site data storage.

— Require vendors to maintain and provide their written BCDR plans in accordance with industry standards and to promptly notify your organization of a business interruption that activates vendors' BCDR plan. Plans should include recovery time objectives and recovery point objectives.

- **Secure Destruction of Data.** Specify protocols for secure destruction of data to ensure data is destroyed or rendered in a manner where the data is completely unreadable so it cannot be accessed or used for unauthorized purposes.
- **Software.** Document requirements specific to software used or developed by vendors.
  - — Require vendors to test common vulnerabilities identified by the Open Web Application Security Project (OWASP) (e.g., Structured Query Language (SQL) injection attacks) in connection with developing upgrading or testing software before delivering to your organization.
  - — Prohibit vendors from storing, maintaining, hosting, transmitting to or permitting the presence of your organization's data outside of the United States without your organization's prior written consent.
- **Audits and Reporting.** Establish audit and reporting procedures.
  - — Include audit rights that provide the ability to assess and review vendors' privacy and data security practices. Common methods include:
    - direct vendor audits or assessments performed by your organization or its contractors;
    - self-assessments performed by vendors at minimum intervals;
    - independent third party audits, assessments, or certifications; or
    - a combination of methods based on timing and risks.
  - — There are several different types of third party audits, assessments, or certifications your organization may use to assess vendors' security requirements. Many organizations choose more than one of the following methods depending on the level of risk under the agreement.
    - *Service Organization Control (SOC) Reports*. Audits are based on American Institute of Certified Public Accountants (AICPA) standards, and provide information about vendors' internal controls.
      - – AICPA SOC 1 reporting covers vendors' activities affecting your organization's internal controls over financial reporting; and
      - – AICPA SOC 2 reporting focuses on vendors' privacy and data security controls.
    - *ISO 27001 certification*. Certifications provide assurance that vendors' information security management program complies with internationally recognized, ISO standards.
    - *General privacy and data security*. Many organizations may find assessments such as those performed against the NIST Cybersecurity Framework useful.
    - *Sector-Specific privacy and data security*. Sector-specific standards and best practices also provide good measures for particular industry needs, in addition to regulatory compliance reviews. For example, the Health Information Trust (HITRUST) Alliance, an independent health care industry group, has established the HITRUST Common Security Framework and a set of related assessment programs.
- **Risk Allocation Provisions.** Address risk allocation, specifically to account for a data breach or other security incident. Typical risk allocation provisions contain:
  - — Indemnification obligations;
  - — Data breach obligations, including specific security incident reporting and response requirements. The reporting requirements often mimic the requirements established in the BAA;
  - — Cyber insurance requirements, including specific limits required for vendors' policies; and
  - — Cost allocation for regulatory penalties or other liabilities related to vendors' failure to meet privacy and data security requirements, data breaches, or other security incidents. These are generally heavily negotiated provisions and, depending on caps on types of costs, generally range somewhere between unlimited down to the amounts of vendors' cyber insurance coverage.

Conclusion

As the health care industry continues to offer outsourced solutions to help other organizations increase administrative efficiencies and reduce health care costs, an ISA is a vital contracting tool that your organization can easily create by mimicking its current information security practices and applicable laws and industry standards. Since vendors typically enact and follow data security and privacy practices as a means of doing business with customers, most vendors are generally accepting of ISAs without the need to heavily negotiate their provisions (assuming vendors are maintaining industry standard practices). In fact, negotiations can illuminate gaps in security and technical diligence that may not have been previously identified as the vendor reacts to the requirements in the ISA. In short, developing an ISA for your organization is an efficient and effective mechanism to (i) provide a concrete way to diligence and document information security compliance; (ii) secure data (arguably its most important asset); and (iii) mitigate risk in using outsourced information technology providers.

1 *See* the General Data Protection Regulation (GDPR)(EU) 2016/679.

Connected Medical Devices: What Attorneys Need to Know

William H. Berglund
Tucker Ellis LLP
Cleveland, OH

Connected medical devices increasingly serve a vital role in improving the health and well-being of patients in all care settings. Connected devices have the potential to make patient care safer and more effective, yet, these devices can also pose significant privacy and security risks for health care organizations and safety risks to patients. Because of these risks, all stakeholders in the production and use of connected medical devices (manufacturers, health care providers, patients, and government regulators) must work together to ensure that these risks are properly assessed and managed. This article explores these issues and offers suggestions for what attorneys representing health care organizations can do to help manage this risk and improve patient care.

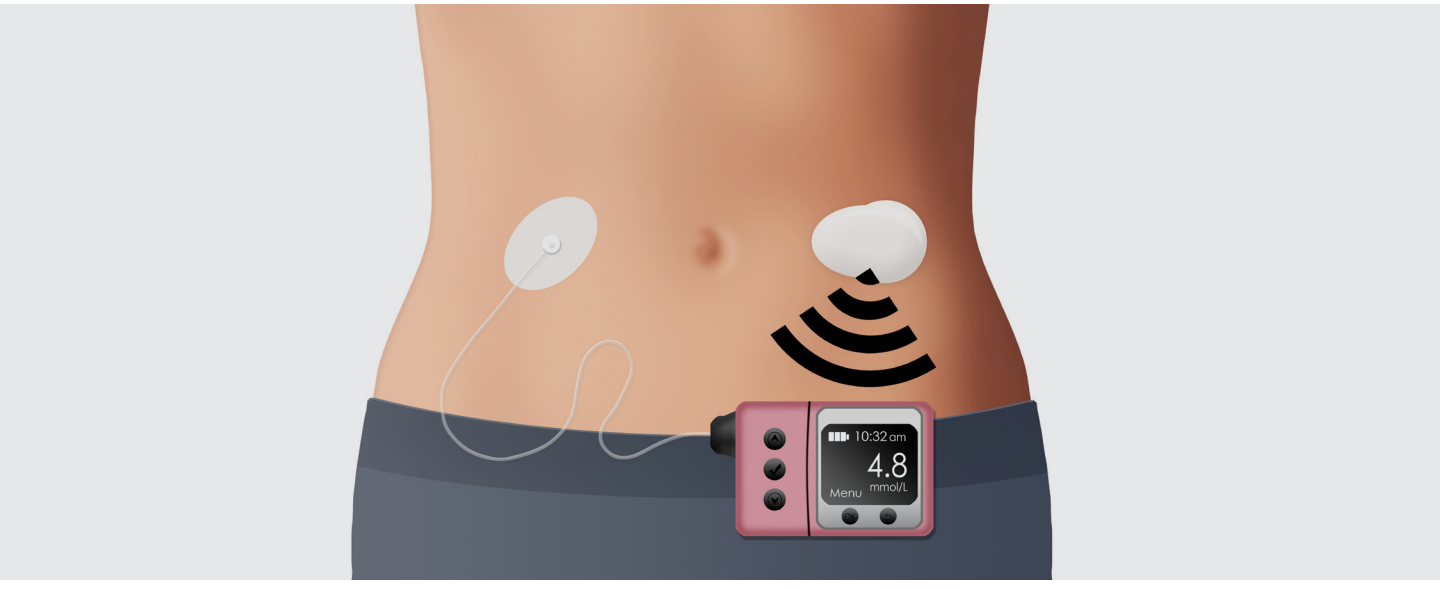
What Benefits Do Connected Medical Devices Provide?

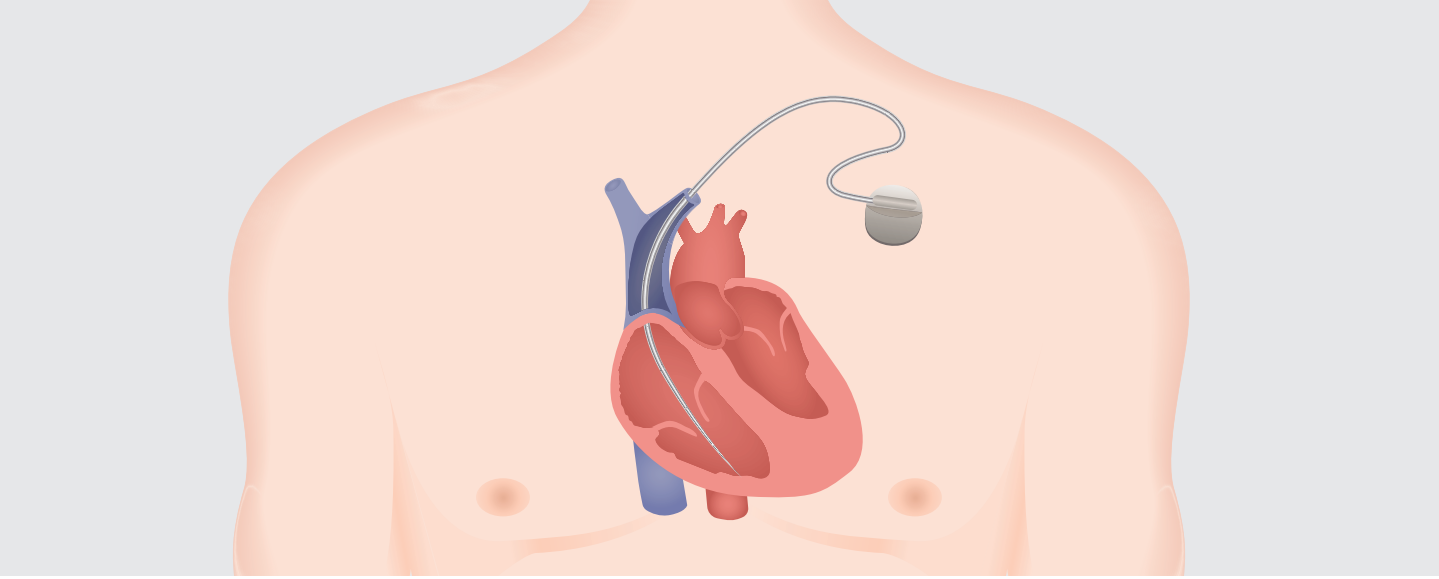
The Food and Drug Administration (FDA) currently regulates over 190,000 different medical devices, including basic medical supplies (bandages and hospital gowns), diagnostic tools (imaging machines), and implantable prostheses (heart valves and artificial pancreas).[1] With expanding technologies and design innovation, an ever-increasing number of medical devices are being connected to health care organizations' computer networks and integrated into patient care. Patients are also connecting personal devices that receive and transmit data through the Internet at home and elsewhere. Examples include implantable devices (cardiac pacemaker, cochlear implants), wireless insulin pumps and glucose monitors, other wearable devices that transmit data, scanning and imaging equipment (MRI, CAT scan), nurse call systems and other patient monitoring equipment, and mobile medical apps. New connected technologies are being designed every day.

Connected medical devices provide many benefits to both providers and patients. These devices can better personalize the delivery of health care to patients through the use of implantable and wearable devices that inject medication, provide reminders, and increase communication between patient and provider. Such devices increase the amount of data that allows providers to be more informed about their patients' health and adherence to treatment and allow for more interoperability as they can communicate with other devices and transmit data to the patient's electronic health record. Connected devices can also support better inpatient monitoring and the ability to respond more quickly in emergency situations. In sum, connected medical devices have the potential to lead to significantly safer and more effective patient care.

What Risks and Challenges Do Connected Medical Devices Pose?

The flipside of this increased connectivity is that, similar to computers and larger networks, these devices are vulnerable to cybersecurity breaches and can expose health care organizations and their patients to greater risks of stolen protected health information (PHI), impeded care and treatment to patients, and even physical harm to a patient.[2] In its June 2017 report, the Health Care Industry Cybersecurity Task Force noted: "The risk of potential cybersecurity threats increase as more medical devices use software and are connected to the Internet, hospital networks, and other medical devices."[3] Hackers increasingly view unsecured medical devices as a gateway into a health care organization's larger computer network.[4] Similar to other cybersecurity threats in the health care industry, vulnerabilities in connected devices can threaten the confidentiality, integrity, and availability of patient PHI and other data.[5] More importantly, however, these threats and vulnerabilities have the potential to cause patient injury or even death caused by the device itself failing to properly function





because it is compromised or the organization's health care operations in general are disrupted due to a larger network compromise.[6]

The Task Force's June 2017 report and a recent February 2018 draft report issued by the National Institute of Standards and Technology (NIST) on cybersecurity standardization for internet of things (IoT) technology provide a helpful summary of cybersecurity risks associated with connected medical devices. Some of the risks identified include:

- Failure of device manufacturers to provide timely security software updates and patches to medical devices and networks and to address related vulnerabilities in legacy devices.
- Malware that alters data on a diagnostic device.
- Denial of service attacks making a device unavailable for use.
- Exfiltration of PHI from the organization's computer network.
- Unauthorized access to the health care network, allowing access to devices and other segments of the network.
- Password problems leading to unrestricted access to the connected device.[7]

The Task Force also issued a series of recommendations for increasing the security and resiliency of medical devices and health IT in general. These recommendations included securing legacy device systems, improving transparency between device manufacturers and users to better understand vulnerabilities and how to implement security updates and patches, and the adoption of a full device lifecycle approach to combatting cyber threats.[8]

Both device manufacturers and health care organizations acknowledge that connected device security and the threat of a cyberattack are real problems. In a May 2017 survey conducted by the Ponemon Institute LLC, 56% of surveyed health care delivery organizations (HDOs) stated they believed an attack on a connected medical device they use was likely in the following 12 months.[9] Eighty percent of surveyed HDOs also said that medical devices are very difficult to secure.[10] Despite these results, only 15% of surveyed HDOs said their organizations were taking significant steps to prevent attacks against their connected devices.[11]

What Is the Legal and Regulatory Framework that Governs Connected Medical Devices?

Attorneys should familiarize themselves with several frameworks and guidance documents directed at increasing the safe and secure manufacturing and use of connected medical devices. In particular, the FDA's regulatory activity in this area and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and regulations are most relevant.

FDA Regulation and Guidance

The FDA is the primary federal agency responsible for regulating the safety and efficacy of medical devices. In the last five years, the FDA has issued final guidance documents that are designed to provide device manufacturers with recommendations for protecting connected devices from cybersecurity threats throughout the lifecycle of the device (design, development, and post-market risk management).[12] The FDA's guidance documents recognize that cybersecurity risk management must be a responsibility shared by device manufacturers, HDOs and providers, patients, and government agencies. They also stress that manufacturers must build in security controls when they design and develop devices, but then must also continuously monitor and address security risks once the device is on the market and is being used by providers and patients.[13]

Earlier this year, the FDA also released its initial *Medical Device Safety Action Plan*, a key focus of which is addressing cybersecurity of medical devices and the ever emerging threats and vulnerabilities.[14] As part of this plan, the FDA is considering requiring manufacturers to (a) build the capability to update and patch security into a device's design and demonstrate that as part of the

premarket process, and (b) develop a "software bill of materials" and provide it to the FDA and the device's customer and users, so the latter will be better equipped to manage the connected devices in their inventory and to be aware of the vulnerabilities related to those devices. The FDA's plan calls for updating its guidance documents to better protect against ransomware attacks and other moderate risks, as well as major risks that exploit a vulnerability in a device that could lead to a "multi-patient, catastrophic attack." The FDA also proposes the creation of a CyberMed Safety (Expert) Analysis Board, which would be a public-private partnership of members comprising a broad range of expertise with a focus on assessing vulnerabilities and risks and serving as a resource for device manufacturers, the FDA, and device users.[15]

HIPAA

Connected medical devices potentially implicate HIPAA to the extent they create, maintain, transmit, or receive patient electronic PHI (ePHI). Covered entities and business associates will need to incorporate connected devices into the organization's HIPAA compliance program. This includes conducting a risk analysis requiring "an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of [ePHI] held by" the organization and then implementing a risk management plan that reduces those "risks and vulnerabilities to a reasonable and appropriate level."[16]

What Should An Attorney Do to Help Manage a Client's Risks Associated with Connected Medical Devices?

Managing cybersecurity risks associated with connected medical devices is a complicated task and should be conducted as part of the organization's overall security program. As part of this program, attorneys should work with their client health care organizations and providers to focus on several areas of cybersecurity risk:

- Ensure that a thorough inventory is conducted of all connected medical devices that are used within the organization. This inventory should document information about the vendor and purchasing history, connectivity, the software a device runs, the data it collects and transmits, and how these devices are accessed. This is the first step in managing device risks.
- Have a plan in place to manage legacy medical devices, including how vulnerabilities will be monitored and a system for installing security updates and patches. A similar plan should also be adopted for newer connected devices. If a legacy device is no longer being serviced by the manufacturer, assess the need for the device's continued use and determine how ongoing security risks can be managed. Make sure that a procedure is in place for destroying PHI and other sensitive data stored on a device when it is removed from use and disposed of by the client.
- Work with device manufacturers and other vendors to be aware of the latest threats and vulnerabilities to the devices in use and to assist in securing the devices throughout their lifecycle. Relatedly, advise clients that when they are purchasing new connected devices to work with vendors upfront to identify the security needed and to obtain sufficient security information about the devices to manage any vulnerabilities after they are put to use.
- Include a discussion of connected devices in any cybersecurity training of the client's staff. In particular, staff should be trained on proper password usage to ensure that only staff with proper authorization has access to connected devices.

Conclusion

Connected medical devices present many benefits to health care organizations and will continue to be used with increasing frequency to support patient care. With that increasing use comes corresponding increased privacy and security risks. All of the stakeholders discussed in this article play an important role in managing these risks and improving patient care. Attorneys representing health care organizations can serve a vital role in this area by being aware of the applicable legal and regulatory frameworks and by working with their clients to adopt organizational risk management practices that address the use of connected devices.

---

1 U.S. Food & Drug Administration, *Medical Device Safety Action Plan: Protecting Patients, Promoting Public Health* (2018), at 1 (FDA Action Plan).

2 Interagency International Cybersecurity Standardization Working Group, Draft NISTIR 8200, *Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)*, National Institute of Standards and Technology (Feb. 2018), at 41-42 (NIST Draft Report).

3 Health Care Industry Cybersecurity Task Force, *Report on Improving Cybersecurity in the Health Care Industry* (June 2017), at 18 (Task Force Report).

4 Fred Donovan, *Medical Device Security Should Be Focus for Healthcare Providers* (Apr. 23, 2018), *available at* https://healthitsecurity.com/news/medical-device-security-should-be-focus-for-healthcare-providers (last accessed July 25, 2018).

5 Task Force Report, at 18-19; NIST Draft Report, at 41-42.

6 Task Force Report, at 18.

7 Task Force Report, at 18-19; NIST Draft Report, at 41-42.

8 Task Force Report, at 28-33.

9 Ponemon Institute LLC, *Medical Device Security: An Industry Under Attack and Unprepared to Defend* (May 2017), at 1.

10 *Id.* at 2, 7.

11 *Id.* at 1.

12 U.S. Food & Drug Administration, *Content of Premarket Submissions for the Management of Cybersecurity in Medical Devices*, Guidance for Industry and Food and Drug Administration Staff (Oct. 2014); U.S. Food & Drug Administration, *Postmarket Management of Cybersecurity in Medical Devices*, Guidance for Industry and Food and Drug Administration Staff (December 2016). The FDA has published additional information about medical device cybersecurity on its website. *See* https://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm (last accessed July 25, 2018).

13 Suzanne Schwartz, M.D., *Managing Medical Device Cybersecurity in the Postmarket: At the Crossroads of Cyber-safety and Advancing Technology* (Dec. 27, 2016), *available at* https://blogs.fda.gov/fdavoice/index.php/2016/12/managing-medical-device-cybersecurity-in-the-postmarket-at-the-crossroads-of-cyber-safety-and-advancing-technology/.

14 FDA Action Plan, at 8, 13-14.

15 *Id.* at 13.

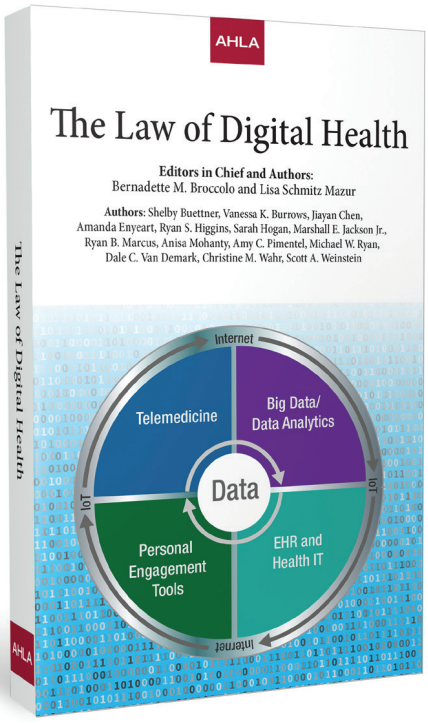
16 45 C.F.R. § 164.308(a)(1)(ii)(A)-(B).

The Law of Digital Health

Editors in Chief and Authors: Bernadette M. Broccolo and Lisa Schmitz Mazur
Additional Authors: Shelby Buettner, Vanessa K. Burrows, Jiayan Chen, Amanda Enyeart, Ryan S. Higgins, Sarah Hogan, Marshall E. Jackson Jr., Ryan B. Marcus, Anisa Mohanty, Amy C. Pimentel, Michael W. Ryan, Dale C. Van Demark, Christine M. Wahr, Scott A. Weinstein

Comprehensive Coverage of:

- Electronic health records and other health information technology
- Big data and data analytics
- Telemedicine
- Mobile personal engagement



Recognize the Implications

The Law of Digital Health offers a solid understanding of how new technologies are affecting:

- Provider-patient relationships
- Medical research
- Privacy and security concerns
- Relationships with health plans, and more

Harness the Potential

A forward thinking and comprehensive legal and regulatory compliance strategy will be a key to harnessing the potential of Digital Health. This book provides the fundamental understanding and tactical foresight you need.

Order today!

www.lexisnexis.com/ahla

Resource Corner

Are You a Member of these Affinity Groups?

Digital Health
Tech Licensing and Intellectual Property
Privacy and Cybersecurity Risk, Compliance and Enforcement

To join any or all of these Affinity Groups, please contact AHLA's Member Satisfaction Center at msc@healthlawyers.org or (202) 833-1100, #2.

Membership in these Affinity Groups is free to all members of the Health Information and Technology Practice Group as well as government, academic, and student members, and those that have paid for all-PGs access (PG 15). Please note that you must be a member of one of these groups to join.

Catch This On-Demand Webinar

Blockchain: Disruption and Enhancement in Health Care

During this on-demand webinar, a panel of legal and industry experts discuss blockchain's inevitable collision with health care focusing on: (i) the foundations of blockchain technology, (ii) health care specific blockchain use cases, and (iii) anticipated developments in the health care legal framework.

Access this on-demand webinar at https://distancelearning.healthlawyers.org/allrecordedwebinars.

HEALTH INFORMATION AND TECHNOLOGY PRACTICE GROUP LEADERSHIP

Alisa Lieberman Chestler, Chair—
Baker Donelson Bearman Caldwell & Berkowitz PC
Nashville, TN
(615) 726-5589
achestler@bakerdonelson.com

Amanda L. Enyeart, Vice Chair—Membership
McDermott Will & Emery LLP
Chicago, IL
(312) 984-5488
aenyeart@mwe.com

Kathleen Dillon Kenney, Vice Chair—Educational Programs
Polsinelli PC
Chicago, IL
(312) 463-6380
kdkenney@polsinelli.com

Gerard M. Nussbaum, Vice Chair—Publications
Zarach Associates LLC
Chicago, IL
(312) 620-9506
gerard@zarachassociates.com

Lisa Pierce Reisz, Vice Chair—Strategic Planning and Special Projects
Vorys Sater Seymour & Pease LLP
Columbus, OH
(614) 464-8353
lpreisz@vorys.com

Sean T. Sullivan, Social Media Coordinator
Alston & Bird LLP
Atlanta, GA
(404) 881-4254
sean.sullivan@alston.com

Leonardo Tamburello, Vice Chair—Research & Website
Willis Towers Watson
New York, NY
(212) 915-8248
leonardo.tamburello@willistowerswatson.com

PUBLISHING STAFF

Cynthia Conner
Vice President of Publishing
(202) 833-0755
cconner@healthlawyers.org

Bianca Bishop
Senior Managing Editor
(202) 833-0757
bbishop@healthlawyers.org

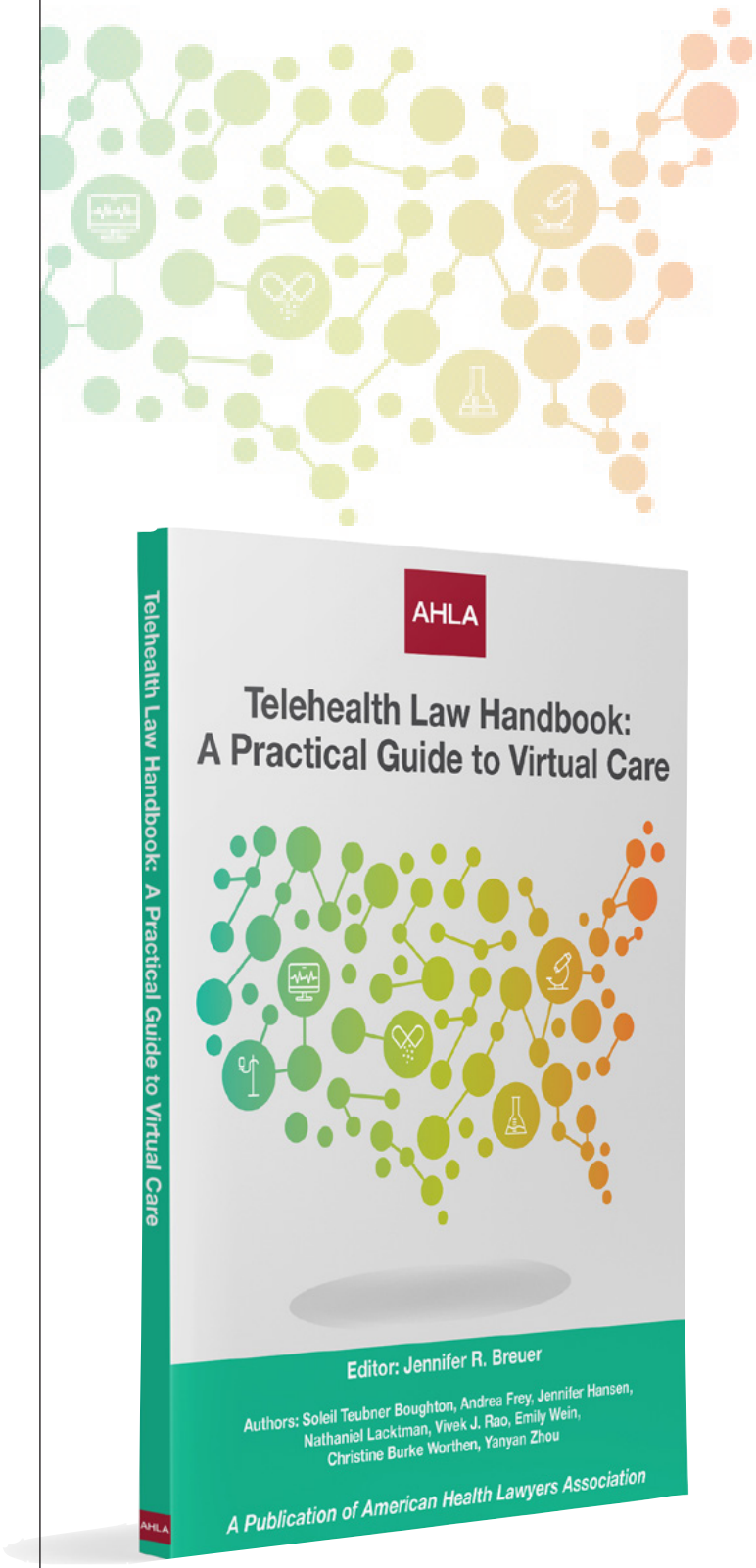
Lisa Salerno
Senior Legal Editor
(703) 489-8426
lsalerno@healthlawyers.org

Matt Ausloos
Manager of Publishing
(202) 833-6952
mausloos@healthlawyers.org

DESIGN STAFF

Mary Boutsikaris
Creative Director
(202) 833-0764
mboutsik@healthlawyers.org

Jen Smith
Graphic Designer/Administrator
(202) 833-0781
jsmith@healthlawyers.org



Telehealth Law Handbook: A Practical Guide to Virtual Care, Second Edition

Jennifer R. Breuer, Editor

Soleil Teubner Boughton, Andrea Frey, Jennifer Hansen, Nathaniel Lacktman, Vivek J. Rao, Emily Wein, Christine Burke Worthen, Yanyan Zhou, Authors

This new publication is an invaluable guide for attorneys, compliance officers, and providers looking to represent clients, manage risk, and address emerging issues in this area. Telehealth is becoming an integral part of the business plans of health care organizations across the country. While opportunities continue to grow, so do the attendant legal and regulatory issues.

THE LEGAL LANDSCAPE ACROSS JURISDICTIONS

In a highly state-dependent area of practice, you must be prepared to understand requirements in all 50 states. This new book will prove indispensable for this purpose.

COMPREHENSIVE AND IN-DEPTH COVERAGE

From licensure and regulatory requirements, to payment and ethical considerations, you'll find in-depth coverage from experts in this area. Look to the *Telehealth Law Handbook* for:

- Telemedicine licensure requirements in all 50 states including types of state licensure, exceptions, and how licensure laws apply in various practice situations
- The application of state regulations on the physician-patient relationship, validation of identity, informed consent, vulnerable populations, non-physician providers, remote prescribing, and continuity of care
- Payment and reimbursement rules under Medicare and Medicaid, telehealth commercial insurance, and a 50-state survey of state telehealth commercial insurance coverage laws
- Emerging legal and ethical issues, including medical staff credentialing, fraud and abuse compliance, corporate practice of medicine prohibitions, privacy and security, and mobile health technology

For more information go to:
www.healthlawyers.org/bookstore

HIT News

AHLA

American Health Lawyers Association
1620 Eye Street, NW, 6th Floor • Washington, DC 20006-4010
(202) 833-1100 • Fax (202) 833-1105 • www.healthlawyers.org