SPECIAL REPORT

2018 DIGITAL HEALTH YEAR IN REVIEW: FOCUS ON DATA

JANUARY 28, 2019

McDermott Will & Emery

McDermott Will & Emery

SPECIAL REPORT

TABLE OF CONTENTS

3 Introduction

4 Data Security and Privacy

- 4 GDPR
- 5 UK Update
- 6 California Consumer Privacy Act
- 7 Protection of Biometric Data
- 8 State Breach Notification Laws
- 9 OCR Updates
- 11 Other Federal Privacy and Security Developments
- 13 Other Notable US Health Care Privacy and Security Enforcement

14 Information Blocking and Interoperability

- 14 Information Blocking Proposed Rule
- 14 Interoperability and Patient Access
- 14 Promoting Interoperability Program Update

LEARN MORE

For more information, please contact your regular McDermott lawyer, or:

JAMES A. CANNATTI III
PARTNER
jcannatti@mwe.com
Tel +1 202 756 8866

JIAYAN CHEN
PARTNER
jychen@mwe.com
Tel +1 202 756 8722

AMANDA ENYEART
PARTNER
aenyeart@mwe.com
Tel +1 312 984 5488

DANIEL F. GOTTLIEB
PARTNER
dgottlieb@mwe.com
Tel +1 312 984 6471

SHARON LAMB
PARTNER
slamb@mwe.com
Tel +44 20 7577 6943

For more information about McDermott Will & Emery visit mwe.com

INTRODUCTION

The past year was an active one for data privacy and security legislation and enforcement. Protection for certain personal data was enhanced internationally by the EU General Data Protection Regulation (GDPR) and in the United States at the state level. Notable new state legislation includes the California Consumer Privacy Act of 2018 (CCPA) and developments in a number of state data breach notification laws that may affect organizations that handle health information. At the same time, the US federal government sought ways to reduce the regulatory burden on health care industry participants and increase the flow of data to promote interoperability.

This report highlights the notable actions and guidance that will shape the data privacy and security landscape for health care providers, digital health companies and other health care industry stakeholders in the coming year.

DATA PRIVACY AND SECURITY

GDPR

On May 25, 2018, the highly anticipated GDPR took effect and became enforceable against certain entities that process the personal data of individuals in the European Union and other European Economic Area countries. Replacing the EU Data Protection Directive, the GDPR harmonizes data privacy laws across the European Union; grants individuals rights over their personal data; regulates how personal data may be collected, used, disclosed and otherwise processed by "data controllers" and "data processors"; and creates strict data breach reporting requirements. An organization's failure to comply with the GDPR may trigger administrative fines of up to EUR 20 million or 4 percent of its annual global revenue—whichever is greater.

The GDPR expanded the territorial scope of European data privacy law. Not only does the GDPR apply to organizations with a location or other establishment in the European Union, it also regulates organizations established outside of the European Union that meet specific criteria. First, the GDPR applies to organizations that offer goods and services to individuals in the European Union. For example, the GDPR may apply to a US-based telehealth provider that deliberately offers health care services to patients who are located in the European Union. Second, the GDPR applies to organizations that monitor the behavior of individuals in the European Union. In this case, the GDPR may apply to a digital health vendor in the United States whose mobile app or wearable device tracks the behavior of users while they are in the European Union, such as by collecting geolocation data, monitoring the physical wellness of users, or serving online behavioral-based advertisements.

In light of the GDPR's broad, extra-territorial reach, US-based digital health providers and vendors should remain mindful of the GDPR's potential applicability to their operations. Moreover, organizations operating in the digital health space should take heed of any GDPR obligations with which they have agreed to comply through contractual arrangements with their customers or other third parties. Please visit McDermott's GDPR Rundown site for additional analysis, webinar presentations and information on how to access our GDPR Toolkit, which includes user-friendly template compliance policies and forms that may be tailored to your organization's operations. You may also access *The Race to the GDPR: A Study of Companies in the United States in Europe*, a comprehensive survey sponsored by McDermott and independently conducted by the Ponemon Institute that includes statistical analysis to provide industry benchmarks for peer organizations throughout Europe and the United States at different stages of GDPR readiness.

UK UPDATE

While implementation of the GDPR has been a key focus of digital health and data specialists in the United Kingdom this year, it is worth remembering that, in addition to the GDPR, the UK law on health data is complex. There is a multiplicity of legislation and guidance governing the use and processing of health data—in practice, this can mean navigating a sometimes contradictory and confusing maze.

This complex legal position was neatly highlighted in 2018 by the decision of the Information Commissioner's Office (ICO) in relation to its investigation of the Royal Free NHS Foundation Trust and its provision of patient data to Google Deepmind for clinical safety testing of the Streams application.

The ICO looked at whether patients were adequately informed about the processing of their data for this testing phase. In its assessment, the ICO did not focus on the data protection law. Instead, the ICO looked at whether the transfer breached the common law duty of confidentiality. The ICO found that because the transfers had been in breach of that duty, the data had not been lawfully processed under data protection law.

The implication of this ruling is that breaches of other data laws may constitute a breach of the GDPR, significantly widening both the scope of the GDPR and the complexity of implementing health data projects.

This is particularly important as the United Kingdom grapples with the challenge and opportunities of using NHS data for secondary purposes—for example, risk stratification, personalized medicine, research, and monitoring drug and treatment efficacy.

> 2018 has seen a significant escalation in public and political concerns about the use of health data, in particular whether commercial organizations are using health data fairly and whether NHS bodies are receiving adequate value for their participation in digital health schemes.

The GDPR and common law duty of confidentiality generally permit the use of health data for primary purposes only (direct care). However, there is a

statutory scheme for the NHS (known as the section 251 exception) that allows for certain of these rights to be overridden in certain circumstances and where protective steps are taken to keep data secure and ensure that anonymization standards set out under the scheme are achieved.

In 2018, NHS bodies rolled out a new scheme allowing patients to "opt out" of their confidential information being used for research and planning purposes. This "opt out" approach replaces previous schemes and means that patient data may be used under the section 251 exception unless patients expressly opt out.

Despite the extensive protection of health data, 2018 has also seen a significant escalation in public and political concerns about the use of health data, in particular whether commercial organizations are using health data fairly and whether NHS bodies are receiving adequate value for their participation in digital health schemes. These concerns contributed to the publication of a 2018 draft code of conduct for the use of health data in the United Kingdom. As discussed in our article "UK Code of Conduct for Data-Driven Health Technology: Key Takeaways for Stakeholders," this code set out initial proposals on principles for both government and commercial organizations on acceptable standards for the use of data. The final code has not yet been published and is now expected early 2019.

CALIFORNIA CONSUMER PRIVACY ACT

As is often the case, California paved the way for enhanced data protection when the California legislature unanimously adopted a new consumer privacy bill: the CCPA, which, as of January 1, 2020, will be the most progressive and comprehensive personal information privacy law in the United States. At a high level, the bill reaches far beyond California's borders to give California consumers more visibility into, and control over their personal information. The CCPA is expected to be further scrutinized and amended before it goes into effect, as stakeholders review the implications of the bill and the Attorney General solicits public participation. Shortly after its passage, we issued an in-depth review of the legislation and a webinar on the impact of the CCPA on corporate compliance programs and business.

The CCPA will regulate the collection, use and disclosure of personal information pertaining to California residents by for-profit businesses that conduct business in California (including out of state businesses) and meet one or more of the enumerated revenue or volume thresholds. Given the requirement that the entity be organized/operated for-profit, nonprofit corporations are likely not covered. Thus, if an organization in the health care sector does not operate a for-profit business, it would not be subject to the CCPA as it is currently drafted. Furthermore, the law will not apply to privileged information or to information governed by HIPAA and other enumerated federal laws. Health care organizations will need to assess whether their business operations in California are limited to HIPAA-regulated functions, as non-HIPAA-regulated functions may be subject to the CCPA.

> The CCPA will affect the clinical and other scientific research activities of academic medical centers and other research organizations in the United States if the research involves personal information about California consumers.

The CCPA will provide a set of enhanced rights to California residents with respect to their personal information, which is defined broadly but also excludes from its application the processing of:

- Aggregated and de-identified data
- Medical information protected under California's Confidentiality of Medical Information Act
- Protected health information (PHI) that is collected by a covered entity or its business associates under HIPAA
- Information collected as part of a clinical trial subject to the Federal Policy for the Protection of Human Subjects (Common Rule)

While the CCPA exempts PHI collected by covered entities and business associates, it also exempts data maintained by a covered entity "in the same manner" as PHI under HIPAA. Business associates are not expressly listed in this exemption, however. The scope of this exemption is not clear, and we expect to see additional guidance on these health-care-related exemptions.

The CCPA will affect the clinical and other scientific research activities of academic medical centers and other research organizations in the United States if the research involves personal information about California consumers. The CCPA defines research broadly to encompass scientific, systematic study and observation, including "basic research or applied research that is in the public interest and that adheres to all other applicable ethics and privacy laws or studies conducted in the public interest in the area of public health." The CCPA imposes specific requirements on a research initiative involving personal information that may have been collected from a consumer in the course of the consumer's interactions with the business's service or device.

Businesses that do not comply with the requirements of the CCPA may be subject to civil suits, including the potential for private rights of action relating to data security breaches, as well as enforcement action from the California Attorney General.

Thus, businesses must maintain policies and procedures that address not only their overall data privacy and security measures, but also how they will ensure that the consumer requests they receive are legitimate and that disclosures are provided to the appropriate consumer. The CCPA permits the imposition of penalties for intentional violations of any provision of the CCPA of up to $7,500 per violation, or $2,500 for unintentional violations if a business fails to cure any unintentional violation within 30 days of receiving notice of the alleged noncompliance.

PROTECTION OF BIOMETRIC DATA

The privacy and protection of biometric data has become increasingly important over the last few years. Three states (Illinois, Texas and Washington) now have laws regulating the collection, use and disclosure of biometric information, and additional states are considering similar legislation. The processing of biometric data is also regulated by the GDPR, and will be regulated by the CCPA.

Illinois's Biometric Information Privacy Act (BIPA), the strongest of the three states' biometric privacy laws, allows injured parties to bring private rights of action for injuries caused by violations of BIPA. BIPA requires regulated companies to provide notice to and obtain written consent from individuals whose biometric data the companies collect. Over the last few years, we have seen a surge of biometric privacy lawsuits in Illinois—Illinois circuit courts have presided over at least 100 BIPA cases in the last two years. Many of these lawsuits are brought against employers and

businesses on the basis of violations of BIPA's notice and consent provisions.

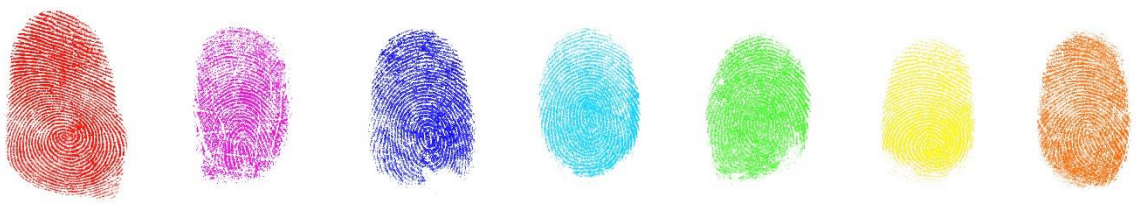
In November 2018, the Illinois Supreme Court heard oral arguments on *Rosenbach v. Six Flags*, which focuses on whether an individual whose biometric data has been collected in violation of BIPA has standing to sue under the act's private right of action without needing to allege actual harm. In this case, the mother of a 14-year-old boy sued Six Flags Entertainment Corporation, alleging that Six Flags scanned her son's fingerprint without obtaining prior written consent and without disclosing Six Flags' practices regarding the collection, use and retention of fingerprint data.

Six Flags moved to dismiss the case on the basis that the mother was not "aggrieved" because she did not allege an actual injury. The Circuit Court of Lake County denied Six Flags' motion. After Six Flags successfully moved for reconsideration, the Circuit Court certified for appellate review two questions regarding whether an individual is "aggrieved" under BIPA if the individual only alleges a technical violation without any concrete harm. The Appellate Court of Illinois, Second District answered both questions in the negative, finding that an individual who raises technical violations of BIPA without alleging any concrete injury or adverse effect is not aggrieved.

The mother appealed the Illinois Appellate Court's ruling, and the Supreme Court of Illinois held oral arguments on November 20, 2018. In a unanimous decision on January 25, 2019, the high court reversed the Appellate Court's ruling, concluding that she can be an "aggrieved" person under BIPA based merely on a statutory violation, without needing to allege concrete harm. In its opinion, the Supreme Court stated, "Contrary to the appellate court's view, an individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act, in order to qualify as an 'aggrieved' person and be entitled to seek liquidated damages and injunctive relief pursuant to the Act." This decision will have significant implications, not just for the numerous similar pending cases in Illinois and on companies implementing biometric technologies in Illinois, but also as a study in contrasts from other federal and state laws that have faced similar challenges regarding the need to allege concrete injury. Moving further into 2019, we will likely see additional legislation, regulator enforcement and class actions relating to biometric data. We will continue to monitor these developments.

STATE BREACH NOTIFICATION LAWS

In March 2018, Alabama and South Dakota became the final US states to adopt a data breach notification statute, joining the other 48 states, the District of Columbia, Puerto Rico, Guam and the US Virgin Islands. Alabama's Data Breach Notification Act became effective on May 1, 2018, and the South Dakota law became effective on July 1, 2018. In addition, on May 22, 2018, Vermont became the first state to enact a breach notification law specifically directed to "data brokers"—*i.e.*,



companies that knowingly collect, sell or license to third parties the personal information of consumers with whom they do not have a direct relationship. The reporting requirements under the Vermont's Data Broker Regulation law went into effect on January 1, 2019.

Notably, a data security incident that involves health or medical information in combination with an individual's first name (or first initial) and last name may trigger the applicability of the Alabama and South Dakota laws. Digital health providers and vendors that experience privacy or security incidents should be mindful of potential notification requirements under state laws, many of which include health-related information in their definitions of "personal information."

Although breach notification measures are now in place in each US state and territory, we do not expect them to remain stagnant. According to the National Conference of State Legislatures, at least 31 states, the District of Columbia and Puerto Rico considered measures in 2018 that would amend their respective existing state breach notification laws. Several of those attempts are likely to continue in 2019.

OCR UPDATES

The US Department of Health and Human Services (HHS) Office for Civil Rights (OCR) continues to aggressively enforce the HIPAA Privacy, Security and Breach Notification Rules against covered entities and business associates. OCR also sought input for future HIPAA rulemaking and issued guidance about HIPAA compliance topics. Following is an overview of notable enforcement actions, requests for input from stakeholders, and guidance issued by OCR in 2018.

Key Lessons from OCR Enforcement Actions

OCR announced 10 enforcement actions and collected approximately $25.68 million in settlements and civil money penalties (CMPs) from HIPAA-regulated entities in 2018. Notably, an HHS administrative law judge upheld the fourth CMP that OCR has assessed against a HIPAA-regulated entity. OCR also entered into a $16 million settlement—the largest monetary settlement in the history of the agency's HIPAA enforcement program. OCR continued to emphasize to HIPAA-regulated entities the importance of implementing a security risk management process, appropriately identifying and handling relationships with business associates, and safeguarding PHI against unauthorized disclosures.

OCR announced **10 enforcement actions** and collected approximately **$25.68 million** in settlements and civil money penalties from HIPAA-regulated entities in 2018.

Below are key lessons that covered entities and business associates alike can glean from select OCR enforcement actions in 2018:

- OCR will often scrutinize not only a breached entity's incident response and mitigation efforts, but also all aspects of the entity's pre-breach HIPAA compliance program. Digital health vendors that are HIPAA business associates should be mindful that OCR continues to exercise the regulatory authority it received in 2013 to hold business associates directly liable for noncompliance with the HIPAA Rules.
- A HIPAA-regulated entity's security risk management process does not end with

performing a Security Rule risk analysis. OCR also expects the entity to create and implement an ongoing plan to reduce identified risks to reasonable and appropriate levels.

- HIPAA-regulated entities should incorporate a review of the potential need to enter into a business associate agreement—which contractually requires a business associate to protect any PHI it receives in accordance with HIPAA standards—into their vendor management practices to avoid violations of HIPAA's business associate agreement requirement.
- HIPAA-regulated entities must implement administrative and technical safeguards to ensure that terminated or departed workforce members no longer have privileges to access electronic PHI (ePHI) after they have left their positions.

OCR Rulemaking

In May 2018, OCR released two advanced notices of proposed rulemaking (ANPRM) regarding amendments to the HIPAA Rules required by the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009. First, OCR issued an ANPRM soliciting public comment on how to implement the HITECH Act's requirement that OCR begin sharing a percentage of the HIPAA settlement and CMP monies it collects with consumers who are harmed by a HIPAA violation.

Second, OCR issued an ANPRM requesting comments on how to address the HITECH Act's modification to the HIPAA Privacy Rule's accounting of disclosures provision, which expands the types of disclosures that a covered entity must track in an accounting. OCR concurrently withdrew its 2011 proposed rulemaking regarding accountings of disclosures, which garnered largely negative feedback from the health care industry. In the 2011 proposed rulemaking, OCR had sought to require covered entities that use electronic health record (EHR) systems to provide "access reports" describing each access of ePHI maintained in a designated record set during a three-year period, regardless of whether the access resulted in a "use" or "disclosure" of the ePHI.

In December 2018, OCR issued a Request for Information to solicit comments and feedback from stakeholders on whether the HIPAA Rules need to be modified to better facilitate the health care industry's transformation to value-based health care and the coordination of care between patients and covered entities, and non-HIPAA regulated health care providers. For more information, please see our analysis of the Request for Information.

OCR Guidance Materials

In 2018, OCR published the following guidance materials and tools that organizations operating in the digital health space may find helpful as they navigate HIPAA compliance challenges.

- **OCR Cyber-Security Newsletter: Risk Analyses vs. Gap Analyses—What Is the Difference?** In the April 2018 edition of its monthly cybersecurity newsletter, OCR discussed one of the common deficiencies it encounters in the HIPAA Security Rule risk analyses performed by covered entities and business associates. In particular, OCR explains why a "gap analysis"—which generally evaluates security controls in place against an information security framework—is insufficient to meet the agency's expectations for a Security Rule risk analysis of potential threats and vulnerabilities to ePHI. For more information, please see our analysis of the continuing disconnect regarding HIPAA's risk analysis requirements.
- **OCR and ONC's Security Risk Assessment Tool**. In September 2018, OCR and the HHS Office of the National Coordinator for Health

Information Technology jointly released an updated version of their HIPAA Security Risk analysis tool. This tool is designed to help small to medium-sized health care providers and business associates comply with the Security Rule's risk analysis requirement.

- **Uses and Disclosures of PHI for Research**. In June 2018, OCR issued guidance pursuant to the 21st Century Cures Act of 2016 on obtaining HIPAA-compliant authorizations from research subjects to use or share their PHI for future research purposes. This guidance explains the criteria for sufficient HIPAA authorizations for future research and recommends methods for research subjects to revoke their authorizations.

OTHER FEDERAL PRIVACY AND SECURITY DEVELOPMENTS

Federal protection of the privacy and security of health information is not limited to HIPAA. Both the Federal Trade Commission (FTC) and the Federal Communications Commission (FCC) have exercised authority to regulate the use and disclosure of data related to certain populations or communicated via specific channels.

Children's Privacy

In 2018, the FTC was active in enforcement of the Children's Online Privacy Protection Act (COPPA). COPPA settlements and fines in 2018 ranged from $235,000 to $4.95 million—the largest COPPA penalty to date. As organizations continue to develop mobile apps and online services, consumer-facing organizations in the health care industry should be aware of COPPA compliance obligations and recent FTC enforcement.

At a high level, COPPA imposes requirements on operators of websites or online services directed to children under 13 years of age, and operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age. COPPA requires that regulated companies clearly disclose to parents the information collected and details on how the information will be used, and seek verifiable parental consent. Regulated companies must take reasonable measures to protect the confidentiality, security and integrity of the information collected about children. COPPA also requires online service providers to retain personal information of a child "for only as long as is reasonably necessary to fulfill the purposes for which the information was collected." The operator must then delete the information using reasonable measures to ensure secure deletion.

In several instances, the FTC settled with companies that allegedly violated COPPA by collecting personal information from children under the age of 13 without providing the COPPA-required notice and obtaining their parents' consent. Several companies also allegedly failed to take reasonable steps to secure the personal information collected from children, as required by COPPA. In other cases, the FTC sent letters to companies that market electronic devices and apps that collect geolocation data from children, warning such companies that they may be violating COPPA. Foreign companies are also required to comply with COPPA if their services are directed to children in the United States or they knowingly collect information from US-based children.

The FTC is authorized to issue rules under COPPA, and, along with state attorneys general, enforces potential COPPA violations. In December 2018,

AOL's successor, Oath Inc., agreed to pay a record $4.95 million in penalties and implement a comprehensive COPPA compliance program. The penalty resulted from the New York Attorney General's finding that AOL "flagrantly" violated COPPA by knowingly collecting and disclosing personal information from children under the age of 13 through one of the operator's advertising exchanges, which runs an auction network allowing third-party advertisers to track and serve targeted ads to covered children. This auction activity occurred despite AOL's policies against violating COPPA. In addition to paying the record penalty, AOL agreed to destroy the covered personal information. The New York Attorney General's office has actively enforced COPPA violations, and we expect state attorneys general offices to become more active in enforcement in the coming year.

Companies in the health care industry should review their data policies and procedures to ensure compliance with COPPA.

Data Privacy and Security

The FTC continued to make data security a high priority in 2018, settling more than 60 alleged data security violations and investigating several additional allegations. In at least one instance, the FTC settled with a technology company over charges that the company misled consumers about its privacy and security practices.

As part of the FTC's ongoing series of public hearings on competition and consumer protection, the FTC held hearings on data security in December 2018. The hearings included panel discussions on research focused on data breaches and data security threats, and the US framework as it relates to data security. Over the course of the two-day hearings, panelists from academia, law firms, security companies and other organizations weighed in on the current data security landscape, incentives to invest in security, the effectiveness of the FTC's existing enforcement tools and whether different tools are needed.

Although the panelists generally agreed that multiple incentives exist for companies to invest in data security (for example, customer trust and demand, public reputation, compliance obligations and associated liability risk, competitive advantage), the panelists offered varying opinions on these incentives' impact and effectiveness. Additionally, although there was a diverse range of backgrounds amongst the panelists, there was broad consensus around the preferred approach to regulating and enforcing data security:

- Reasonable data security requires a risk- or process-based approach, not a checklist of requirements.
- A uniform, comprehensive approach to data security is preferable to the current US system and its patchwork of various federal and state laws imposing various data security rules.
- The FTC's standard of reasonable security, not strict liability, is the correct approach.

The FTC has a hearing on consumer privacy scheduled at the beginning of 2019. We will continue to monitor FTC guidance and developments, and will provide commentary on key takeaways.

In light of the FTC's recent enforcement actions, companies should ensure that their privacy practices accurately and comprehensively reflect their information practices. Companies should implement a comprehensive security program that addresses security risks associated with how the company collects, uses and shares personal information, including via mobile devices, apps and connected

devices. Companies also should perform appropriate due diligence of service providers that perform services involving an individual's personal information.

Telephone Consumer Protection Act

The Telephone Consumer Protection Act (TCPA) regulates telemarketing calls, text messages, prerecorded or auto-dialed calls, and unsolicited faxes. Companies in the health care industry should pay particular attention to the TCPA, in part because of its interplay with HIPAA.

On March 16, 2018, the US Court of Appeals for the DC Circuit issued a long-awaited decision on an omnibus challenge to the FCC's interpretation of the TCPA. The court struck down two key portions of the FCC's 2015 Declaratory Ruling and Order as arbitrary and capricious, while rejecting challenges to other portions of the 2015 Order.

The decision, discussed in-depth in our article "Appeals Court Strikes Down Key Portions of FCC's Onerous TCPA Rulemaking," provided some relief for operators facing the prospect of TCPA liability. The ruling still leaves open many questions, however. TCPA compliance should remain a priority for all organizations with large-scale calling or texting operations. We expect further guidance from the FCC on these issues, and we will continue to monitor these developments.

OTHER NOTABLE US HEALTH CARE PRIVACY AND SECURITY ENFORCEMENT

Cybersecurity remains a priority in the health care industry. The past year saw several notable data security incidents in the United States. A recurring vulnerability that often leads to data security incidents is poor vendor management. As health care organizations become more dependent on third-party vendors, the risk of a data security incident increases. Just in 2018, a number of enforcement actions focused on vendor management.

- The New Jersey Office of the Attorney General fined a covered entity more than $418,000 for its business associate's failure to keep its online database of patient data private by removing password protection during a data upload that left the data vulnerable to unauthorized access without proper authentication and available for indexing by search engines. The attorney general found that the covered entity failed to thoroughly analyze the risk to the confidentiality of PHI sent to its business associate, and that the covered entity failed to implement adequate security measures that would have reduced such risk. Compounding the issue, the business associate failed to notify the covered entity of the breach. This penalty highlights the need for health care providers to thoroughly evaluate third-party vendors that use or disclose PHI.
- Data security incidents have also extended into unauthorized disclosures of PHI on paper records. The New Jersey Office of the Attorney General fined a health insurer's vendor $100,000 for its 2016 data breach affecting more than 6,000 residents. The breach was caused when the insurer's vendor mailed letters to customers with their Medicare Part D Prescription Drug Plan's Evidence of Coverage—and also included beneficiary

identification numbers that were composed of the patients' Social Security numbers. The attorney general concluded that the vendor violated New Jersey's Identity Theft Prevention Act, HIPAA and the New Jersey Consumer Fraud Act. In addition to paying its fine, the vendor must reform its compliance functions to improve security of sensitive policyholder data, including prohibiting the use of Social Security numbers as ID numbers.

These representative examples illustrate how regulators, including state attorneys general, have made privacy and data security a priority.

INFORMATION BLOCKING AND INTEROPERABILITY

The focus on interoperability and the flow of information in the health care ecosystem continued in 2018.

INFORMATION BLOCKING PROPOSED RULE

The Office of the National Coordinator for Health Information Technology (ONC) took another step toward issuing its long-awaited proposed rule to implement various provisions of the 21st Century Cures Act, including proposed regulations distinguishing between (1) prohibited health information blocking by health information technology developers, exchanges, networks and health care providers, and (2) permissible restrictions on access to health information. ONC submitted its proposed rule to the Office of Management and Budget (OMB) for review on September 17, 2018. OMB review is one of the final steps in the process before a proposed rule is published in the Federal Register. As of the date of this publication, OMB has yet to release the proposed rule. Once ONC releases the proposed rule, the industry will have an opportunity to provide public comment on ONC's proposal before it becomes final and enforcement begins. Engaging in prohibited information blocking can carry stiff penalties, including CMPs of up to $1 million per violation, adjusted annually. For additional information, please see our discussions concerning the proposed rule and what the industry can do pending its release.

INTEROPERABILITY AND PATIENT ACCESS

Not to be outdone, the Centers for Medicare & Medicaid Services (CMS) is also working on rules to facilitate the flow of information. On September 21, 2018—just a few days after ONC's submission of the information blocking rule to OMB—CMS submitted a proposed rule entitled Interoperability and Patient Access to OMB for review. Like the ONC proposed rule, it has yet to be released, but we understand that it will involve policy changes intended to effectuate a health care ecosystem that is more accessible and interoperable than the one we have today. While little is known about the details of CMS's proposed rule, many wonder whether it will include proposals connecting information sharing to CMS conditions of participation, a concept that was previously the subject of a CMS request for information. The public should also have an opportunity to comment on CMS's proposed rule once it is published.

PROMOTING INTEROPERABILITY PROGRAM UPDATE

In 2018, CMS marked its increased focus on interoperability and patient access by changing the name of the Medicare and Medicaid EHR Incentive Programs to the Promoting Interoperability (PI) Programs. CMS also finalized changes to the PI Programs in the Fiscal Year 2019 Inpatient Prospective Payment System and Long-Term Care

Hospital Prospective Payment System final rule, to reduce burden and emphasize interoperability.

Notable among the changes, CMS finalized a 90-day reporting period for calendar years 2019 and 2020; established a new scoring methodology with fewer objectives; finalized two new e-Prescribing measures designed to help address the opioid crisis by improving controlled substance prescribing practices; removed measures that did not emphasize interoperability and information exchange; and reiterated that, beginning in CY 2019, the PI Programs require use of certified EHR technology (CEHRT) that has been certified to the 2015 Edition criteria. This reflects the end of a long transition from the 2014 Edition to the 2015 Edition, which has a greater focus on interoperability. Entities that had not previously upgraded to technology certified to the 2015 Edition will have to do so in order to be successful under the PI Programs in 2019.

CMS's focus on interoperability carried over into the EHR-related portion of the Merit-Based Incentive Payment System (MIPS) under the Quality Payment Program. CMS renamed the Advancing Care Information performance category as the Promoting Interoperability performance category and sought to align requirements for eligible clinicians with those for eligible hospitals and Critical Access Hospitals under the PI Programs. Like participants in the PI Programs, MIPS eligible clinicians will be required to use CEHRT certified to the 2015 Edition criteria starting in 2019.

CONTRIBUTORS

JAMES A. CANNATTI III
PARTNER
jcannatti@mwe.com
Tel +1 202 756 8866

JIAYAN CHEN
PARTNER
jychen@mwe.com
Tel +1 202 756 8722

AMANDA ENYEART
PARTNER
aenyeart@mwe.com
Tel +1 312 984 5488

DANIEL F. GOTTLIEB
PARTNER
dgottlieb@mwe.com
Tel +1 312 984 6471

SHARON LAMB
PARTNER
slamb@mwe.com
Tel +44 20 7577 6943

MATTHEW R. CIN
ASSOCIATE
mcin@mwe.com
Tel +1 312 984 2099

DEEPALI DODDI
ASSOCIATE
ddoddi@mwe.com
Tel +1 312 984 3265

BOSTON
28 State Street
Boston, MA 02109-1775
USA
Tel: +1 617 535 4000
Fax: +1 617 535 3800

BRUSSELS
Avenue des Nerviens 9 - 31
1040 Brussels
Belgium
Tel: +32 2 230 50 59
Fax: +32 2 230 57 13

CHICAGO
444 West Lake Street
Chicago, IL 60606-0029
USA
Tel: +1 312 372 2000
Fax: +1 312 984 7700

DALLAS
2501 North Harwood Street
Suite 1900
Dallas, TX 75201-1664
USA
Tel: +1 214 295 8000
Fax: +1 972 232 3098

DÜSSELDORF
Stadttor 1
40219 Düsseldorf
Germany
Tel: +49 211 30211 0
Fax: +49 211 30211 555

FRANKFURT
Feldbergstraße 35
60323 Frankfurt a. M.
Germany
Tel: +49 69 951145 0
Fax: +49 69 271599 633

HOUSTON
Two Allen Center
1200 Smith Street
Suite 1600
Houston, TX 77002-4403
USA
Tel: +1 713 653 1700
Fax: +1 972 232 3098

LONDON
110 Bishopsgate
London
EC2N 4AY
Tel: +44 20 7577 6900
Fax: +44 20 7577 6950

LOS ANGELES
2049 Century Park East
38th Floor
Los Angeles, CA 90067-3218
USA
Tel: +1 310 277 4110
Fax: +1 310 277 4730

MIAMI
333 SE 2nd Avenue
Suite 4500
Miami, FL 33131-2184
USA
Tel: +1 305 358 3500
Fax: +1 305 347 6500

MILAN
Via Dante 15
20123 Milan
Italy
Tel: +39 02 36575701
Fax: +39 02 36575757

MUNICH
Nymphenburger Str. 3
80335 Munich
Germany
Tel: +49 89 12712 0
Fax: +49 89 12712 111

NEW YORK
340 Madison Avenue
New York, NY 10173-1922
USA
Tel: +1 212 547 5400
Fax: +1 212 547 5444

ORANGE COUNTY
18565 Jamboree Road
Suite 250
Irvine, CA 92612-2532
USA
Tel: +1 949 851 0633
Fax: +1 949 851 9348

PARIS
23 rue de l'Université
75007 Paris
France
Tel: +33 1 81 69 15 00
Fax: +33 1 81 69 15 15

SAN FRANCISCO
415 Mission Street
Suite 5600
San Francisco, CA 94105-2533
USA
Tel: +1 628 218 3800
Fax: +1 628 218 3900

SEOUL
18F West Tower
Mirae Asset Center1
26, Eulji-ro 5-gil, Jung-gu
Seoul 04539
Korea
Tel: +82 2 6030 3600
Fax: +82 2 6322 9886

SHANGHAI
MWE China Law Offices
Strategic alliance with
McDermott Will & Emery
28th Floor Jin Mao Building
88 Century Boulevard
Shanghai Pudong New Area
P.R.China 200121
Tel: +86 21 6105 0500
Fax: +86 21 6105 0501

SILICON VALLEY
275 Middlefield Road
Suite 100
Menlo Park, CA 94025-4004
USA
Tel: +1 650 815 7400
Fax: +1 650 815 7401

WASHINGTON, DC
The McDermott Building
500 North Capitol Street, NW
Washington, DC 20001-1531
USA
Tel: +1 202 756 8000
Fax: +1 202 756 808

McDermott
Will & Emery

mwe.com |