The Privacy Survival Guide

NEWSLETTER FROM POLSINELLI'S HEALTH INFORMATION PRIVACY AND SECURITY PRACTICE GROUP

Virginia's Consumer Data Protection Act

HHS Office for Civil Rights Enforcement Update

21st Century Cures Act Information Blocking Rule: Innovative and In Effect

Past, Present and Future: What's Happening With Illinois' and Other Biometric Privacy Laws

Data Localization and Data Transfer Restrictions

COVID-19 Privacy Response

Polsinelli's cross-disciplinary COVID-19 attorney response team provides guidance and counsel on the full array of legal concerns impacting clients' operations across all legal service areas and industries.

To access our Privacy and Cybersecurity Resource Center click **here**, or subscribe to our COVID-19 blog **here**.

Virginia's Consumer Data Protection Act

Virginia recently adopted a GDPR-inspired comprehensive data protection law for Virginia residents.

What Are the Main Points Covered by Virginia's Consumer Data Protection Act (CDPA)?

Like Europe's GDPR and California's CCPA, the CDPA **expands consumer rights** to access, correct, delete, and obtain a copy of personal data provided to or collected by a company, and to opt out of processing of the personal data for purposes of targeted advertising, sale, or profiling of the personal data.

The CDPA also **expands Virginia's definition of personal data, to include "sensitive data,"** which includes, among other categories, race, religion, sexual orientation, mental or physical health diagnosis, biometric data, personal data collected from a known child, and precise geolocation.

The CDPA also defines expectations and **requirements for controllers**, to limit the use of the personal data to the purpose for which it was collected, implement reasonable data protection safeguards, process data only with consent of the consumer, establish a clear privacy policy, disclose sale of personal data for advertising purposes to consumers and provide a simple mechanism to opt out of the sale, and provide a secure and reliable way for consumers to exercise these rights. As with GDPR, controllers will also be required to conduct and document **data protection assessments** of processing activities created or generated after the CDPA goes into effect, and the documentation could be requested by the Virginia Attorney General. Further, the CDPA defines **requirements that govern the controller-processor relationship**, including, that the processor must adhere to instructions of the controller, and controllers and processors must have a data processing agreement in place.

Who Does the CDPA Apply To?

The CPDA applies to businesses that conduct business in Virginia, or produce products or services that target Virginia residents, and that (1) during a calendar year, control or process personal data of at least 100,000 "consumers" or (2) control or process personal data of at least 25,000 "consumers" and derive over 50% of gross revenue from the sale of personal data. "Consumer" is defined as a natural person who is a resident of Virginia, acting only in an individual or household context. It does not include an individual acting in a commercial or employment context.

As with CCPA, there are broad exemptions for financial institutions subject to the Gramm-Leach-Bliley Act (GLBA) and covered entities and business associates governed by HIPAA or HITECH. Other exemptions include nonprofit organizations and higher education institutions.

What Is the Current Status of CDPA and When Will It Take Effect?

The CDPA was passed in March 2021. The CDPA will take effect in January 2023, at the same time as California's new California Privacy Rights Act (CPRA).

What Happens If Companies Don't Comply With the CDPA?

Unlike the CPRA, there is no private right of action for consumers. Instead, the Virginia Attorney General will have exclusive authority to enforce violations. Violators will have a 30-day period to cure infractions, after which the Attorney General can seek damages of up to $7,500 per violation.

> Click here to view the update published in February 2021.

HHS Office for Civil Rights Enforcement Update

Abby E. Bonjean
Associate
Chicago

Right of Access Initiative

The HHS Office for Civil Rights (OCR) continues to vigorously enforce an individual's right to access their medical records. OCR recently announced the 19th settlement as part of their Right of Access Initiative.

In 2019, OCR announced that it planned to focus its enforcement efforts on ensuring that patients receive their medical records in a timely manner consistent with the format and fee requirements set forth under the HIPAA Privacy Rule. Since that time, OCR has entered into 19 settlements ranging from $5,000 to $200,000, including several settlements involving solo providers, to address entities' failure to provide patients access to their medical records. OCR has announced five of those settlements since January, despite the change in administration, which typically results in a pause in settlement cases for at least a few months until the new leadership is brought up to speed.

As part of the most recent settlement, the Diabetes, Endocrinology & Lipidology Center, Inc. (DELC), a West Virginia-based practice providing treatment for endocrine disorders, agreed to take corrective actions and pay $5,000 after failing to provide a mother access to her minor child's medical records. According to OCR, the mother requested the records in July 2019, but DELC did not provide them until May 2021, almost two years after the mother made the initial request and well beyond the 30-day period required under HIPAA. Similar to other settlements under the Right of Access Initiative, DELC also agreed to a Corrective Action Plan (CAP) with a two-year monitoring period that requires it to take the following actions:

- Review and revise its policies and procedures related to an individual's access to PHI;
- Provide annual training and training materials to all workforce members concerning an individual's access to PHI; and
- Submit a list of requests for access to PHI received by DELC every ninety days during the term of the CAP.

Based on OCR's continued focus on enforcement of an individual's right of access, entities should prioritize responding to access requests in a compliant manner and address any access-related issues that are brought to their attention immediately.

Recent Security Rule Settlements

In addition to the Right of Access Initiative settlements, OCR has entered into two additional settlements to resolve potential violations of the HIPAA Security Rule during the past several months. In May, OCR announced that Peachstate Health Management, LLC, dba AEON Clinical Laboratories (Peachstate), a Georgia lab certified under the Clinical Laboratory Improvement Amendments of 1988 (CLIA), agreed to pay $25,000 to OCR. OCR initiated a review of Peachstate's HIPAA compliance in December 2017 as a result of OCR's review of Peachstate's parent company, related to a breach experienced by the parent company. OCR's investigation of Peachstate found systemic noncompliance with the HIPAA Security Rule, including failures to conduct an enterprise-wide risk analysis, implement risk management and audit controls, and document HIPAA Security Rule policies and procedures. In addition to paying $25,000 to settle the case, Peachstate agreed to a relatively robust CAP, which included engaging an independent monitor and a three-year monitoring period.

In January, Excellus Health Plan, Inc. (Excellus), a health plan based in New York, agreed to pay $5.1 million related to a breach affecting over 9.3 million people. Excellus reported that cyber-attackers gained access to its information systems on or before December 23, 2013, until May 11, 2015. OCR's investigation determined that Excellus failed to conduct an enterprise-wide risk analysis, and implement risk management, information system activity review and access controls.

In addition to the HIPAA Security Rule's risk analysis and risk management implementation specifications, entities continue to struggle with information system activity review. We recommend ensuring that your organization regularly reviews records of information system activity, such as audit logs and access reports, for any unusual activity that may identify security incidents.

Recognized Security Practices

At the beginning of January 2021, the previous administration signed into law H.R. 7898, which amends the Health Information Technology for Economic and Clinical Health (HITECH) Act to require HHS to consider covered entities' and business associates' implementation of "recognized security practices," when imposing fines or penalties under the HIPAA Security Rule.

Although HHS has not undertaken a formal rulemaking process, and the statute has not yet been implemented, OCR has begun requesting the following evidence of entities' implementation of "recognized security practices" as part of ongoing investigations:

- Policies and procedures related to the implementation of "recognized security practices;"
- Completed project plans or similar documentation showing the dates of implementation of "recognized security practices;"

CONTINUED ON PAGE 4

CONTINUED FROM PAGE 3

- Documentation explaining how "recognized security practices" are implemented (e.g., the scope of implementation throughout the entity);
- Names of any individuals responsible for ensuring "recognized security practices" are implemented by the entity's workforce members;
- Training materials provided to workforce members regarding "recognized security practices" and the dates of such training; and
- Documentation showing whether the "recognized security practices" were developed under:
  - Section 2(c)(15) of the National Institute of Standards and Technology (NIST) Act;
  - Section 405(d) of the Cybersecurity Act of 2015; and/or
  - Other programs and processes addressing cybersecurity that are developed, recognized, or promulgated through regulations under other statutory authorities.

While it is still unclear what HHS considers "recognized security practices," it seems likely that implementation of any of the following security standards would arguably satisfy the Act's documentation requirements: NIST Special Publications Guidance, Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients Guidance, and any additional programs that address specific legal requirements.

Please contact us if you would like additional information regarding the statute and what may constitute "recognized security practices." You can also find additional information regarding the statute **here**.

21st Century Cures Act Information Blocking Rule: Innovative and In Effect

Iliana L. Peters
Shareholder
Washington, D.C.

Adrienne A. Testa
Associate
Chicago

In May of 2020, the Office of the National Coordinator for Health Information Technology (ONC) released the **21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program** (the Information Blocking Final Rule). The Information Blocking Final Rule implemented far-reaching health IT provisions enacted in the 21st Century Cures Act, with the goals of achieving widespread interoperability among health IT systems and improving a patient's ability to access their medical information.

The Information Blocking Final Rule applies to three categories of "actors:"

- Health Care Providers
- Health Information Network or Health Information Exchange
- Health IT Developer of Certified HealthIT

All Actors were subject to the Information Blocking Final Rule's provisions beginning on April 5, 2021.

Information Blocking

The Information Blocking Final Rule prohibits Actors from undertaking any practice likely to interfere with, prevent, or materially discourage access to, exchange of, or use of Electronic Health Information (EHI).

Currently, EHI constitutes the data elements represented in the first version of the **United States Core Data for Interoperability** (USCDIv1) such as health data classes (e.g., patient demographics, clinical notes, and vital signs) and data elements (e.g., patient name, laboratory reports, and heart rate); essentially EHI constitutes information contained in a certified electronic health record (EHR). The definition of EHI will expand on October 6, 2022 to include all electronic PHI included in a patient's designated record set, excluding psychotherapy notes; and information compiled in anticipation of litigation or administrative action.

As set forth in 45 C.F.R. Part 171, what constitutes a prohibited practice further varies based on Actor-type.

Health Care Providers
Information blocking is a practice the provider knows is unreasonable and is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information.
HIN/HIE or Health IT Developers
Information blocking is a practice that such developer, network or exchange knows, or should know, is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information.

CONTINUED ON PAGE 5

CONTINUED FROM PAGE 4

Examples of information blocking include:

A health system requires staff to obtain patient written consent before sharing patient's EHI with unaffiliated providers.

A hospital customizes its EHR to include barriers to sending referrals and EHI to unaffiliated providers.

An EHR Vendor prevents (e.g., through high fees) third-party clinical decision support application from writing EHI into the EHR.

A Health IT Vendor discourages customer from getting data integration capabilities from a third party, claiming that it will have that same functionality soon while such functionalities are in early stages of development.

Information Blocking Exceptions

The Information Blocking Final Rule defines eight **information blocking exceptions** divided into two categories:

1. Exceptions that involve not fulfilling requests to access, exchange, or use EHI, and
2. Exceptions that involve procedures for fulfilling requests to access, exchange, or use EHI.

These exceptions are summarized below. Note: Any Actor preparing to invoke an exception must meet all sub-exceptions enumerated in the regulations.

Information Blocking Exceptions	
When not fulfilling requests for EHI (42 C.F.R. §§ 171.200 -171.205)	
▪ **Preventing Harm Exception:** Practices that are reasonable and necessary to prevent harm to a patient or another person, provided certain conditions are met. ▪ **Privacy Exception:** Practices implemented to protect the privacy of EHI, based in privacy laws tailored to specific privacy risks (e.g., HIPAA).	▪ **Security Exception:** Practices implemented to protect the security of EHI, as long as the measures are specifically tailored to the security risk and implemented in a consistent and nondiscriminatory manner. ▪ **Infeasibility Exception:** Denying requests for EHI if fulfilling the request is objectively and verifiably infeasible. ▪ **Health IT Performance:** Making technology temporarily unavailable for maintenance or updates.
When fulfilling requests for EHI (42 C.F.R. §§ 171.300-171.303)	
▪ **Content and Manner Exception:** Limiting the content of its responses to requests for access, exchange, or use of EHI or the manner in which it fulfills such a request. ▪ **Fees Exception:** Charging for costs it reasonably incurs when fulfilling requests for access, exchange, or use of EHI.	▪ **Licensing Exception:** When fulfilling requests, an organization may claim intellectual property rights, but it must respond to requests to license interoperability elements.

Penalties

Once the information blocking provisions go into effect, HIN/HIE and Health IT Developers face up to a $1 million penalty per violation of the information blocking prohibition. The requirements will be enforced by the HHS Office of the Inspector General, which has yet to promulgate enforcement rules. Furthermore, Health IT Developers face a Certification Ban for Certified EHR Technology. Healthcare Providers are subject to yet-to-be-defined "appropriate disincentives" for information blocking violations. These "appropriate disincentives" have not yet been published, but will be determined in future rulemaking.

Key Takeaways

Now that the compliance deadline has passed, Actors should take inventory of their current procedures for receiving, making, and responding to requests to access, exchange, or use EHI. Health care providers, specifically, should consider adopting "reasonable" policies, procedures, and practices, as the information blocking definition for healthcare providers requires providers to know that such a practice is "unreasonable." Furthermore, all Actors should take inventory of current practices for denying or fulfilling requests and determine which do (or do not) fit within an enumerated exception to information blocking.

If you have questions or would like assistance in understanding your risk or evaluating steps for complying with the Information Blocking Final Rule, please contact Polsinelli for more information.

Past, Present and Future: What's Happening With Illinois' and Other Biometric Privacy Laws

Dmitry Shifrin
Shareholder
Chicago

Mary Buckley Tobin
Associate
Chicago

Lindsay R. Dailey
Shareholder
Chicago

Introduction

Biometric information and biometric identifiers are becoming more highly regulated in today's data privacy and cybersecurity conscious landscape. Like other types of personal data, biometrics have the potential to identify individuals, and state legislatures are responding by changing their privacy laws to include biometrics within their grasp.

The most stringent of these laws is Illinois' Illinois Biometric Information Privacy Act (BIPA) which is seeing heavy class action activity in recent years, despite BIPA's existence since 2008. Also trending in biometric litigation is increasing settlement figures — for example, in February 2021, a federal court approved the $650 million proposed settlement of a BIPA class action against Facebook.

BIPA Requirements

BIPA requires private entities that obtain biometric information or identifiers to first inform the subject in writing that their information is being collected and stored, inform the subject of the specific purpose and term for collection and storage, and secure a written release from the subject. BIPA also prohibits the disclosure of the biometric information without the subject's consent, unless an exception is met. Private entities also cannot sell, lease, trade, or profit from a person's biometric information. Further, BIPA requires a private entity in possession of biometric identifiers and information to develop a publicly available written policy establishing a retention schedule and providing guidelines for the permanent destruction of the information.

Any person aggrieved by a BIPA violation may file suit to recover statutory damages of $1,000 for each negligent violation or $5,000 for each intentional or reckless violation, plus reasonable attorneys' fees and costs. To establish standing, actual harm is not required and mere procedural violations are sufficient.

Status of Current BIPA Cases in Illinois

Despite the increase in litigation, there is limited controlling precedent in state court to rely upon, with federal court litigation bringing its own unique considerations for parties. For example, BIPA does not provide for a statute of limitations, which is an important issue litigated across lower courts without prevailing input from appellate courts (yet). As of this writing, there also are two pending appellate court cases that will address key issues for businesses and employers facing BIPA lawsuits.

The Illinois Supreme Court is set to decide whether the exclusive remedies under the Illinois Workers' Compensation Act bar claims for statutory damages under BIPA where an employee alleges that an employer violated the employee's statutory privacy rights under BIPA. In *McDonald v. Symphony Bronzeville Park, LLC*, No. 1-19-2398 — a highly anticipated case because the decision will impact hundreds of BIPA cases — the Defendant-former employer seeks to bar the Plaintiff-employee's claims for injuries incurred when scanning her fingerprints to clock into and out of work. As of April 30, 2021, Defendant-Appellant filed its opening brief, and Plaintiff's response is forthcoming. A ruling in favor of Defendant will have resounding effects on current and future BIPA cases in the employment setting, which typically involve the alleged collection of biometric information for timekeeping purposes and access to computer systems.

Pending before the Seventh Circuit is a challenge to the Northern District of Illinois' decision that two independent and actionable BIPA violations **occurred and accrued** each time the Plaintiff used Defendant's finger-scan system without appropriate notice and consent (i.e., to access both work computers **as well as** weekly paystubs). In *Cothron v. White Castle System, Inc.*, No. 20-3202, the Defendant and Amicus Curiae argue that potentially crippling damages may ensue if each employee is entitled to one or more awards of statutory damages each time an employee uses biometric technology. If the lower court's reasoning stands, conservative estimates of damages for the plaintiff alone are estimated to exceed $3 million and the class to easily exceed $1 billion.

In response to the torrent of BIPA litigation, the Illinois House of Representatives is considering House Bill 559 which is intended to stem the impact of BIPA claims on businesses of all sizes in the state. Illinois House Bill 559 seeks to make several changes to BIPA: (1) narrowing the definition of biometric information by exempting "information derived from biometric information that cannot be used to recreate the original biometric identifier [e.g., a numerical identifier converted from a finger scan]"; (2) employees must provide employers with written

CONTINUED ON PAGE 7

CONTINUED FROM PAGE 6

notice and an opportunity to cure a BIPA violation 30 days before being able to file a lawsuit; (3) a one year statute of limitations to file a BIPA suit; (4) eliminating statutory penalties of $1,000 or $5,000 "for each violation" and limiting recovery to actual damages and attorneys' fees; (5) excluding suits filed by employees subject to a collective bargaining agreement; and (6) permitting electronic consent instead of requiring a "written release."

Current and Proposed Biometric Privacy Laws in Other States

Several states have followed Illinois in passing legislation regulating the use and disclosure of biometric information; however, Illinois currently is the only state whose statute includes a private right of action. Laws governing biometric information range from **comprehensive laws** governing biometric information that are similar to BIPA, to **data privacy laws** which include biometric information within the definition of "personal data," to **breach response laws** including biometric information under "covered personal information."

Currently, only two other states have a **comprehensive** law governing biometric information: Texas and Washington. Tex. Bus. & Com. Code §503.001 provides that a person may not capture a biometric identifier without prior consent, may not sell biometric data without consent or unless allowed by law, must use reasonable care in storing it, and shall destroy the biometric identifier within a reasonable time. Similarly, Wash. Rev. Code Ann. §19.375.020, prohibits any company or individual from entering biometric data "in a database for a commercial purpose, without first providing notice, obtaining consent, or providing a mechanism to prevent the subsequent use of a biometric identifier for a commercial purpose." While both laws have similar requirements to BIPA, neither include a private right of action and both authorize their respective state attorney general to enforce the laws.

Other states have introduced proposed **comprehensive** legislation that has failed to pass, with Maryland and New York as the latest to consider implementing a **comprehensive** biometric information privacy law. New York Assembly Bill 27 would require written consent for collecting biometric information, and prohibit the sale of that information. Maryland House Bill 218 would impose similar restrictions. Both laws would feature a private right of action, distinguishing them from the Washington and Texas statutes.

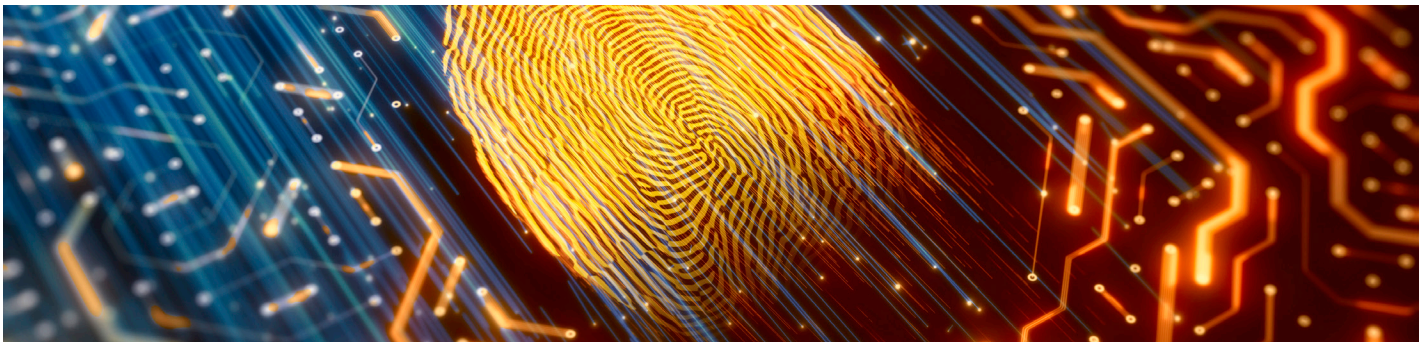
The California Consumer Privacy Act includes biometric data within the definition of **personal data**. The law intends to provide consumers rights related to the control of their personal information, which extends to biometric data defined as "physiological, biological or behavioral characteristics, including … DNA[,] that can be used … to establish individual identity," including "imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information." Cal. Civ. Code §1798.140(b).

New York and Arkansas both have **breach response** statutes covering biometrics. Specifically, in New York the 2019 Stop Hacks and Improve Electronic Data Security (SHIELD) Act includes "biometric information" within the definition of "private information." The law requires notification to individuals upon discovery of unauthorized access of their private information. And Arkansas' breach response law, Arkansas Code §4-110-103(7), now includes "fingerprints; faceprint; a retinal or iris scan; hand geometry; voiceprint analysis; deoxyribonucleic acid (DNA); or any other unique biological characteristics" as biometric data within the definition of covered personal information. Arkansas' law also requires notice to individuals upon discovery of a breach of personal information.

Congressional Interest in Biometric Privacy Laws

Federal lawmakers have also shown an interest in legislating biometric information. The National Biometric Information Privacy Act of 2020 was introduced in August 2020 and would require covered entities to obtain consent prior to capturing biometrics, and also impose retention, disclosures, and destruction requirements. The proposed federal law, which is currently still under review in the U.S. Senate, would also include a private right of action.

While the future of a federal law governing biometric information remains to be seen, it is clear that the regulatory landscape governing biometrics is constantly evolving and entities handling biometric information must be vigilant as to their obligations under current and future laws, particularly as enforcement increases and private litigation shows no sign of abating where permitted.



Data Localization and Data Transfer Restrictions

In the modern global economy, data is the most valuable resource. Businesses use data to create value for customers and increase profit for its stakeholders. Although these businesses can only maximize their use of the data when it can flow freely across borders, many countries have been enacting measures that would make transferring data more complicated, expensive, time consuming, and at times, illegal.

Data Localization vs. Data Transfer

Data localization laws govern the location where personal data is stored, whereas data transfer laws govern the ability to disclose copies of personal data outside the borders of a country or region, but do not require local storage. Often, data localization laws incorporate aspects of data transfer laws.

Globally, these rules are not uniform and many countries have adopted their own requirements which can vary based on the types of personal data covered and the scope of their respective requirements. The following are the most commonly seen categories of data localization and data transfer laws:

1. **Broad Localization Laws:** Cover all categories of personal data and a copy of the data must be stored in country. Cross border transfers are permitted under certain exceptions.
2. **Specific Localization Laws:** Cover specific categories of personal data and/or certain types of organizations which must comply, and a copy of the data must be stored locally. Cross border transfers are permitted under certain exceptions.
3. **Combined Localization/Transfer Laws:** Cover specific categories of personal data, and the data must be stored locally unless an exception applies. These types of laws typically do not require storing a copy of the data locally, and cross border transfers are permitted under certain exceptions.
4. **Pure Data Transfer Laws:** Pure data transfer laws do not require local storage but only permit cross border transfers under certain exceptions.

European Laws

The European Union's ("EU") General Data Protection Regulation, together with (a) the United Kingdom's Data Protection Act 2018 and associated post Brexit implementation laws, and (b) implementing laws of EU member states (collectively, "GDPR"), permit transfers of personal data to locations outside of the European Economic Area ("EEA"), which have not been designated as having 'adequate' protections for personal data, only in certain circumstances. Below is an overview of the main mechanisms pursuant to which personal data may be lawfully transferred.

1. **Adequate Safeguards:** In the absence of a transfer to a country deemed to have adequate protections for personal data, a controller or processor may transfer personal data outside of the EEA if adequate safeguards are in place and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. The GDPR lists a number of appropriate safeguards, the most commonly used being:
   a. Binding corporate rules – available only for purposes of intercompany transfers;
   b. Standard contractual clauses – currently available for controller to controller, and controller to processor, transfers. Draft updated standard contractual clauses are also under review and would also cover processor to controller, and processor to processor, transfers.
   c. Approved certification mechanism (such as the recently invalidated EU / US Privacy Shield framework).

The recent Schrems II decision from the European Court of Justice[1] invalidated the Privacy Shield framework, meaning that personal data could no longer be transferred from the EU to the US under that mechanism. In the same judgment, the European Court of Justice confirmed that Standard Contractual Clauses could still be utilized as a method of transfer, but that in certain circumstances additional safeguards over and above those contained within the clauses would be required. This is particularly applicable to transfers of personal data to the United States, where US government surveillance laws such as FISA 702 mean (at least in the consideration of the European Court of Justice) that enforceable rights and effective legal remedies are not available to data subjects. Recent guidance from the European Data Protection Board has provided further clarity as to the type

[1] https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf

CONTINUED ON PAGE 9

CONTINUED FROM PAGE 8

of additional safeguards that may be required, including data minimization, and encryption of personal data in transit and at rest.

2. **Derogations for Specific Situations:** In the absence of an adequacy decision, or appropriate safeguards, a transfer of personal data can still take place pursuant to one of a number of derogations, including:
   - **a.** The data subject has explicitly consented to the proposed transfer, after having been informed of the risks of such transfers. It should be noted, however, that there are significant limitations on what is considered valid consent under GDPR, and therefore use of consent for international transfers should be carefully considered in advance.
   - **b.** The transfer is necessary for performance of a contract between the data subject and the controller, or a contract between the controller and a third party where the contract is for the benefit of the data subject.
   - **c.** The transfer is necessary for important reasons of public interest recognized under EU or member state law (note, this is usually only applicable in the case of international data exchanges between government authorities and will rarely apply in the context of transfers for business purposes).
   - **d.** The transfer is necessary for the establishment, exercise, or defense of legal claims.
   - **e.** The transfer is necessary to protect the vital interests of the data subject or other persons, where the data subject is incapable of giving consent.

It should be noted that transfers undertaken on the basis of derogations should concern a limited number of data subjects only, and may not be repetitive. As a result, reliance on derogations as a mechanism for transfer is appropriate only for occasional transfers and is therefore not a reliable transfer mechanism for most business related transfers (for example, reliance on derogations would not be appropriate for transfers of data to a US based cloud hosting provider, payment processor, or for HR administration purposes).

Laws Outside of the European Union

Below are examples of how various countries outside of the EU have approached data localization and data transfer requirements, and how they fit into the categories of localization/ transfer laws described above.

1. **Broad Localization Laws:**
   - Russia requires a copy of the data to be stored on local servers, and cross border transfers are permitted under certain exceptions, such as data subject consent.
2. **Specific Localization Laws:**
   - Japan requires medical care records to be stored within the country.
   - China requires certain types of information to be located within mainland China including financial and health or medical information. China's cybersecurity law also requires certain types of organizations to conduct security assessments prior to transferring personal data outside of China.
   - Australia requires certain health information to remain inside of the country.
   - India requires licensed banks and payment system providers to retain their information locally, and may also be stored additionally outside of India if certain criteria are met.
3. **Combined Localization/ Transfer Laws:**
   - British Columbia and Nova Scotia in Canada both require personal information maintained by "public bodies" (e.g., hospitals) to be stored locally unless the explicit consent to transfer such data outside of Canada and be accessed by non-Canadians is obtained from the data subject.
4. **Pure Data Transfer Laws:**
   - Brazil restricts the disclosure of personal data outside of the country unless prior consent is obtained, or another exception applies.
   - For private entities, Mexico restricts disclosing personal data outside of the country unless notice is given and consent is obtained, or another exception applies. Note that Mexico also has national security provisions applicable to governmental entities that require local storage of national security and public information within the facilities of the relevant public entities.

Conclusion

With the growth of international enterprises, and the ever increasing digital economy, organizations should carefully consider the application of data localization and data transfer laws to their operations and those of their customers. Consideration of these issues as part of product or service development can save time and money and avoid unanticipated legal risk.

Contacts for More Information

Lisa J. Acevedo
Shareholder
Chicago

312.463.6322
lacevedo@polsinelli.com

Mary Clare Bonaccorsi
Office Managing Partner
Department Chair
Chicago

312.463.6310
mbonaccorsi@polsinelli.com

Lindsay R. Dailey
Associate
Chicago

312.873.2984
ldailey@polsinelli.com

Colleen M. Faddick
Shareholder
Practice Chair
Denver

303.583.8201
cfaddick@polsinelli.com

Kathleen D. Kenney
Shareholder
Chicago

312.463.6380
kdkenney@polsinelli.com

Abby E. Bonjean
Associate
Chicago

312.463.6230
abonjean@polsinelli.com

The explosion of digital data, along with the proliferation of technology, devices and other health care innovation has created a multi-layered range of privacy and data security issues in the health care industry. Polsinelli's multi-disciplinary Health Information Privacy and Security Team brings together attorneys across the firm specializing in the areas of privacy, security, technology and litigation, who understand the value of your health-related data and are adept at assisting clients in maximizing the benefits of that data while minimizing and responding to ever-changing threats and risks.

Our team has deep experience in the full breadth of privacy/security-related laws and regulations impacting the health care industry, including HIPAA, FERPA, federal laws and regulations governing the confidentiality of alcohol and drug abuse treatment records, state privacy/security laws related to the confidentiality of health information (including mental health, HIV/AIDS and genetic information), and international privacy laws impacting data use and transfers.

POLSINELLI

AUGUST 2021 | VOL. 3