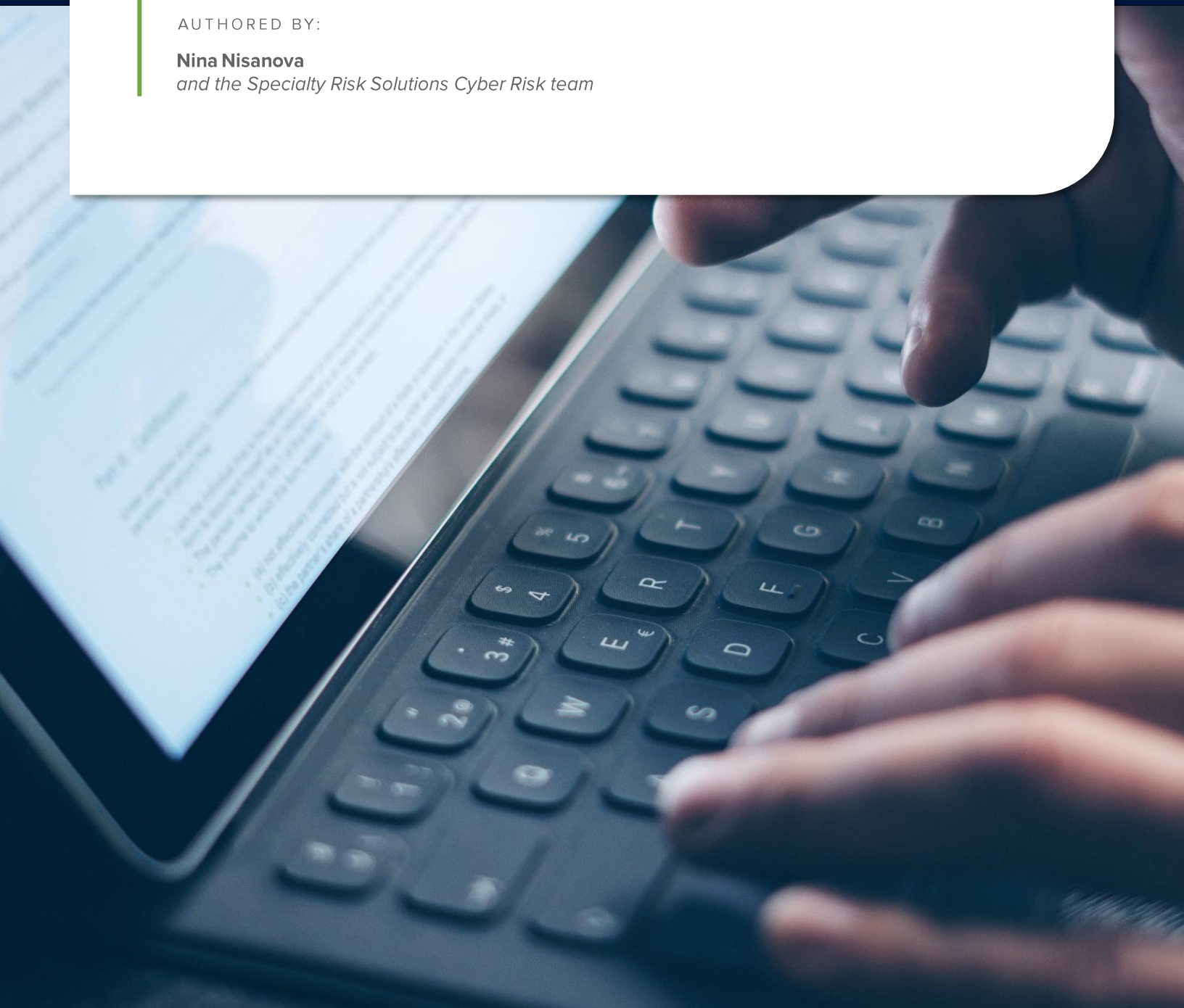
Brown & Brown

WHITE PAPER

Annual Data Privacy Regulatory Updates

AUTHORED BY:

Nina Nisanova
and the Specialty Risk Solutions Cyber Risk team



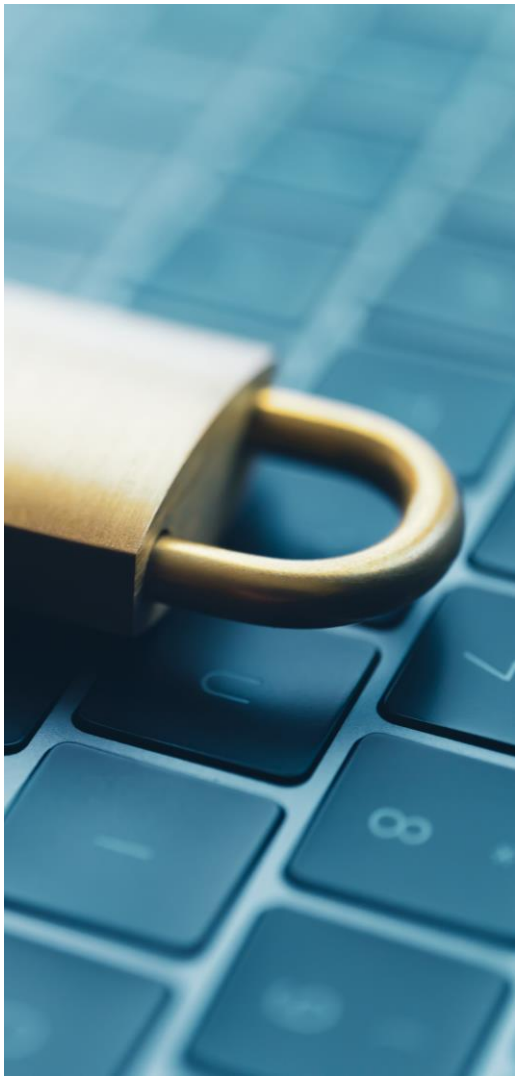
Introduction

While various ransomware attacks have been monopolizing recent headlines, it is critical to remember that data breaches are the baseline to cyber losses. As of Sept. 30, 2021, the number of publicly reported data breaches, year-to-date, had already exceeded the total number of breaches reported for the entirety of 2020. From both a regulatory and consumer-obligation perspective, organizations and their management teams should remain informed about developments to both novice and existing data privacy rules and regulations. This piece intends to provide customers with an update on data privacy regulations from an international and domestic standpoint.

Data Privacy Regulation Update

European Union (EU) – General Data Protection Regulation

Since the spring of 2018, the General Data Protection Regulation (GDPR) has served as the primary legislative mechanism regulating how companies protect citizens' personal data of the European Union (EU). The introduction of the GDPR bolstered the EU's commitment to addressing "privacy" as a fundamental human right; the EU now possesses some of the strictest data privacy and protection laws worldwide.



During the summer of 2021, the European Commission published novice Standard Contractual Clauses (SCCs) regarding the transfer of personal data from the EU to third-party countries outside of EU jurisdiction, such as the United States. However, there was one jurisdictional exception: post-Brexit, the SCCs do not apply to transfers of personal data from the United Kingdom.

While the previous SCCs only stipulated specific requirements for controller-to-controller and controller-to-processor transfers, the SCCs introduced in June 2021 stipulate requirements for those as well as transfers between processor-to-sub-processors and processors-to-controllers. The new guidelines contain novice requirements for data importers or controllers and processors located beyond the borders of the EU. They are required for all new transfer agreements entered on or after Sept. 27, 2021. Agreements already in effect must be replaced with the new SCCs by Dec. 22, 2022.

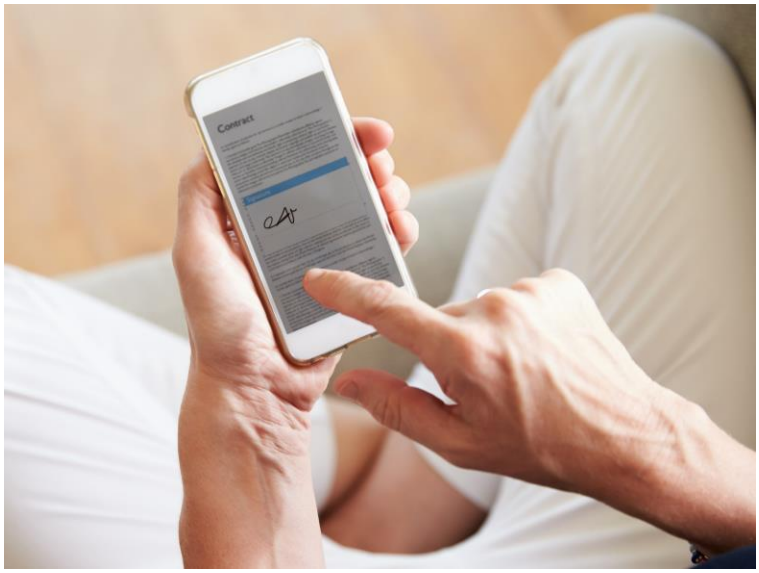
The new SCCs require data importers to confirm they will only disclose personal data to third parties outside of EU jurisdiction if such a party has agreed to be bound by the terms of the clauses ***or*** that a specific legal exemption applies. Since previous guidance explained that exemptions are not permitted for systemic transfers of personal data, a data importer must now ensure that any party involved in processing the data, this includes any potential sub-processor, has also signed and agreed to the updated SCCs.

With the novel SCCs, it is no longer necessary for organizations to enter into separate data processing agreements to comply with Article 28 of the GDPR. Article 28 requires data controllers to ensure they only appoint data processors capable of providing "sufficient guarantees" of their intent and abilities to implement the terms set forth by the GDPR. The Article also requires data processing to be conducted pursuant to a contract, making it a violation of the regulation for controllers and processors to fail to enter a written data-processing contract. Modules Two and Three of the new clauses contain the requirements articulated within Article 28; therefore, for controller-to-processor and processor-to-processor data transfers, supplementary data processing agreements are no longer imperative.

The new clauses also contain a "docking clause". While the previously utilized SCCs were devised for two-party contracts, the new provisions allow for execution by multiple parties. The "docking clause" permits and highlights the process of adding additional parties to the SCCs during a contract's lifetime.

China – Personal Information Protection Law

On Aug. 20, 2021, the Standing Committee of China's National People's Congress passed the Personal Information Protection Law (PIPL or "the Law"). Taking effect Nov. 1, 2021, PIPL is China's first exhaustive legislation addressing personal data protection to help protect the public's rights and interests by regulating personal data processing. The new law is meant to enhance existing data privacy laws within China's legal system's framework. PIPL should be read and analyzed in conjunction with all other national and provincial laws that dictate data protection rules and regulations.



Updates to China's data privacy framework are substantial, including the PIPL requiring consumers to provide expressed and informed consent for the processing of all personal information. The PIPL also requires separate, explicit consent for certain, specified activities, including the following:

- Processing of sensitive information
- Overseas transfers
- Public disclosure of personal information

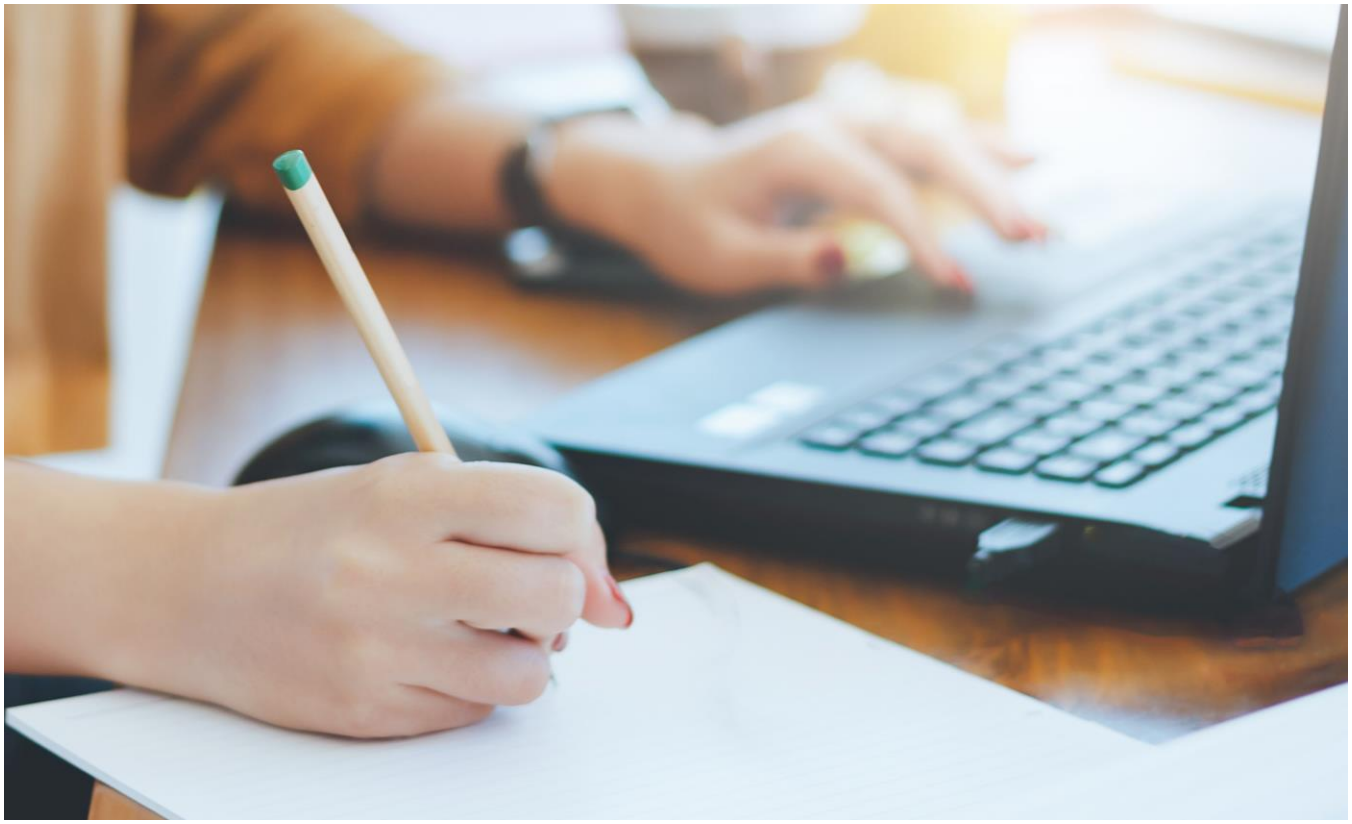
Both consent requirements are new regulations and did not appear in China's data privacy scheme prior to the Law.

The PIPL establishes measures for internet platform providers, data controllers processing large amounts of data and complex businesses. Any organization described by those classifications must set up personal data protection compliance mechanisms and external independent data protection agencies to supervise them. Organizations must also establish and publish data processing obligations and rules that regulate their products openly and fairly. Internet platform providers, large volume data controllers and complex businesses are required to publish social responsibility reports referencing their personal data processing schemes.

PIPL regulations related to overseas transfers and data localization are new additions to the framework. As of the Law's passing, data controllers may only transfer or access personal data outside of China's mainland if the organizations involved in the transfer have adopted the necessary protective measures for personal data processing, obtained separate, explicit consent from consumers or cleared various hurdles set forth by the Cyberspace Administration of China (CAC).

The PIPL also introduced rules surrounding the disclosure of personal data to government entities. Data controllers are not permitted to provide personal data stored within China's borders to overseas authorities without securing approval from the designated Chinese authority. Chinese authorities are then permitted to provide requested data if and to the extent that international treaties or similar regulations that promote fairness are in place.

The Law has enhanced the rights of data subjects or consumers. In addition to consumers' existing rights, which include the rights to access, copy, transfer and correct or supplement data, close relatives of deceased consumers now retain the rights to access, copy, correct or delete personal data of the consumer if the family member possesses a legitimate and proper interest in doing so. Consumers may now bring civil actions against data controllers who do not uphold data subjects' rights.



EU and China – Guidance for U.S. Organizations

U.S. organizations subject to the authority of the GDPR because of an establishment or the effective, real and stable exercise of activity in the EU may rely on the new SCCs to transfer personal data from the EU to a data importer within the U.S. The same reliance on the clauses would be activated for U.S. organizations that are not established in the EU and offer goods and services to EU consumers because such activity subjects organizations to the regulation. Even in instances involving U.S. organizations not subject to the GDPR, the reliance on the SCCs would apply if the organizations receive or access personal data stored in or from the EU.

While historically, China's data privacy regulations have only applied to related activities occurring inside the country, the PIPL expands its application to the processing of personal data outside of the PRC's jurisdictional boundaries. When an outside organization, such as a U.S.-headquartered operation, acts with the purpose of providing goods or services to consumers within China, the PIPL applies.

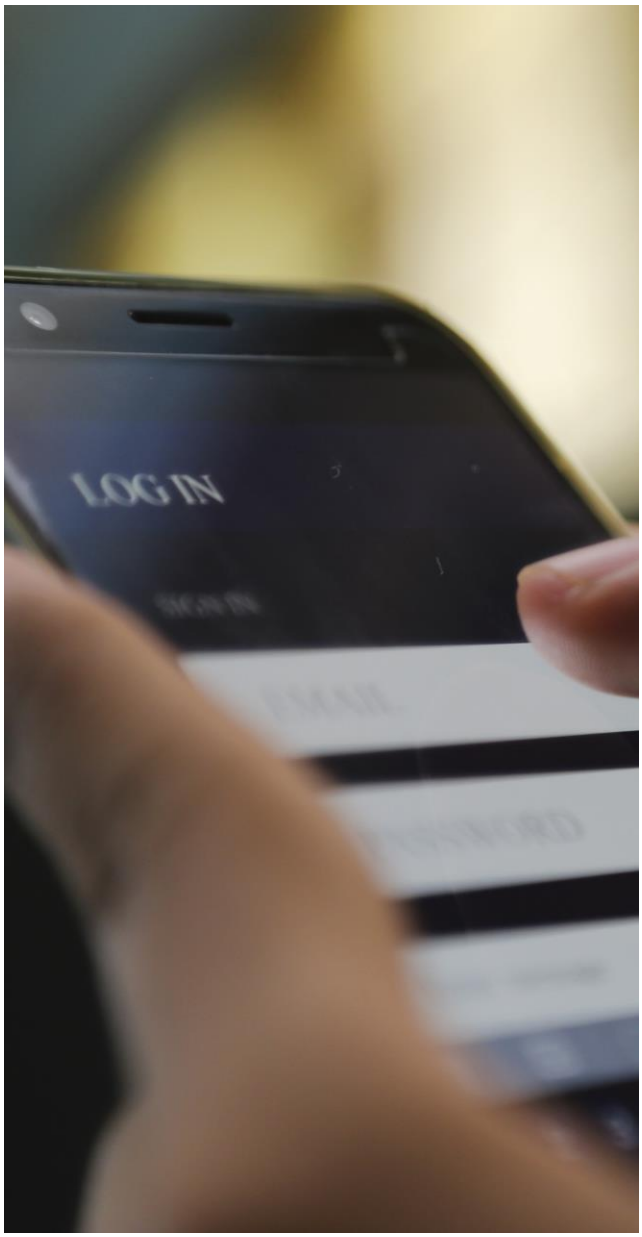
The same conclusion is reached when an outside organization analyzes or assesses activities within China. Penalties for non-compliance can be as detrimental to the infringing organization as being fined 5% of the violator's annual revenue, or up to 50 million RMB (approximately $7.7 million).

U.S. organizations engaging in transferring, receiving or accessing personal data from the EU or China should take several steps to help ensure compliance with the new SCCs and the PIPL. Organizations must identify ongoing transfers that will require updating, develop internal processes and policies for handling data transfers from the EU and/or China to help ensure compliance and train employees to identify transfers that contain customer, consumer and human resources data.

Data Privacy with the United States: Updates

At present, the United States does not possess a uniform, comprehensive federal legislation tasked with regulating the collection or utilization of individuals' personal data. Within the U.S., the existing system of federal and state laws and regulations that address data privacy have led to both overlap and contradiction. This mix of authority includes the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA), among others. While HIPAA protects communications and medical data between a covered entity and an individual, the GLBA requires consumer financial products, like loan services, to disclose how they utilize personal data collected. Both Acts demonstrate efforts to regulate data privacy violations but remain constrained by their respective objectives. Since 2019, several strides have been made toward adopting more stringent regulations.

U.S. – The FTC and GLBA Standards for Safeguarding Customer Information



On Oct. 27, 2021, the Federal Trade Commission (FTC) released a final rule amending the Standards for Safeguarding Customer Information (Safeguards Rule) propagated by the GLBA. Under the Safeguards Rule, financial institutions under the jurisdiction of the FTC are required to develop, implement and maintain reasonably comprehensive information security programs. Security programs must possess appropriate administrative, technical and physical safeguards to protect sensitive customer information. The recently publicized rule expands upon the utilized definition of "financial institution" by including any entity engaged in ventures the Federal Reserve Board considers incidental to financial activities. While previous FTC guidelines required financial institutions to engage in a risk assessment and address any risks subsequently identified, the final Safeguards Rule requires the risk assessment to be written and for the safeguards developed to target identified risks to address the following:

- Access controls
- Data inventory and classification
- Encryption
- Incident response

The final Safeguards Rule also requires financial institutions to designate a single individual, a "Qualified Individual", to be responsible for implementing and overseeing the institution's information security program. Qualified Individuals are required to provide boards of directors or other governing bodies with periodic reports, helping to ensure senior management of the covered financial institutions are aware of the security programs' development and progression.

U.S. – HIPAA and OCR Guidance for Returning-to-Work

On Sept. 30, 2021, the U.S. Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) issued guidance to better assist anyone concerned with how and when HIPAA applies to requests and disclosures of personal information related to the COVID-19 vaccine. The provided guidance reminds all affected that HIPAA only applies to covered entities, such as health plans, health care clearinghouses and health care providers engaged in electronic transfers of patients' personal data. The OCR confirming that HIPAA does not prohibit any person or business from asking customers and employees for their COVID-19 vaccination status was timely, arriving when many organizations were attempting to construct comprehensive return-to-work plans.

While an individual's medical vaccination status is considered protected health information (PHI), organizations and providers not covered under the HIPAA definition of "covered entity" do not have to be concerned with violating the Act when asking their staff or clientele for their status. When the entity is "covered," they may still avoid liability if the disclosure of an individual's vaccination status is being requested by the vaccine manufacturer and/or the FDA for activities related to the safety and efficacy of the vaccine or when required by law.

U.S. – California and the CCPA/CPRA

Effective Jan. 1, 2020, the California Consumer Privacy Act (CCPA) bolstered California residents' privacy and consumer protection rights. Its passage and adoption remain significant due to the abundance of technology companies within the state's borders. To protect consumers' personal data, the CCPA provides residents the right to access, delete and transfer their personal data, as well as the right to request businesses not to sell any personal information. It also provides a right of action, or the right of consumers to bring a civil action if their personal data is subject to theft, disclosure without their consent or has been accessed without authorization.

In November 2020, California once again asserted its position as a frontier state related to data privacy legislation by passing a bill for adopting the California Privacy Rights Act (CPRA), an expansion of the CCPA. Intended as an addendum to the CCPA, the CPRA will become fully effective on Jan. 1, 2023, and will aim to tighten business regulations addressing the use of consumers' personal data by establishing the California Privacy Protection Agency (CPPA), a governmental agency tasked with enforcing data privacy protection state-wide. Among the amendments encompassed within the CPRA, the Act creates a category of personal data titled "sensitive personal information," including previously excluded biometric data. The addendum states that organizations that use or disclose personal data must notify consumers, and maintain a clear and visible opt-out link on their business internet homepage. Organizations will no longer be allowed to retain an individual's personal data for an indefinite period of time, as the CPRA constrains the timeframe for storing data only to that which is reasonably necessary.

Data Specific Updates: Biometrics

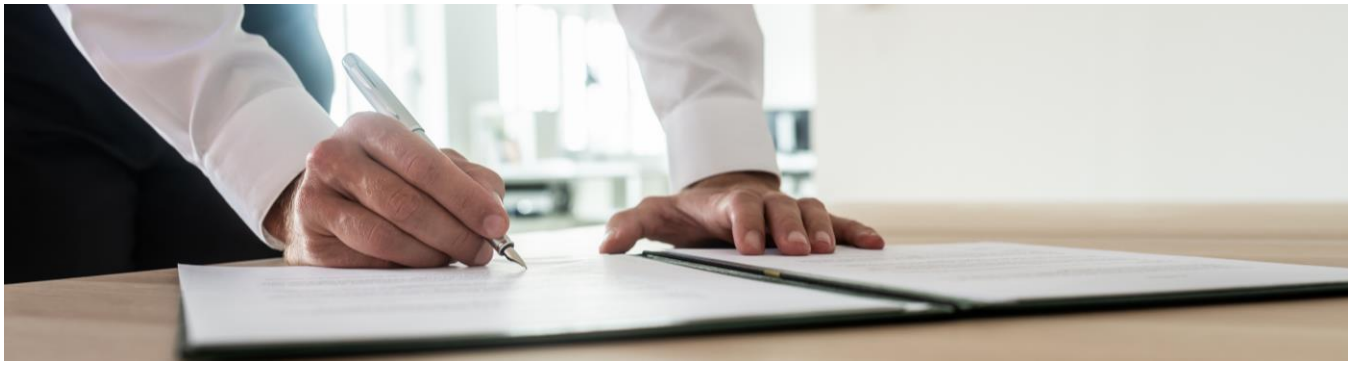
Despite the remarkable and individualized nature of such information, there has been a notable lack of legal provisions specifically targeting the protection of biometric data, which often includes the following:

- Retina or iris scans
- Hand scans
- Facial geometric scans
- DNA
- Voiceprints
- Fingerprints
- Other identifying, biological information

To remedy this, several states have either recently adopted or amended legislation addressing the data privacy concerns surrounding biometric data.

U.S. – California and Biometric Data Under the CCPA

Effective January 2020, the CCPA's definition of biometric data is broader than the definition utilized by the GDPR, as it considers an individual's physiological and behavioral characteristics and DNA. The November 2020 passing of the CPRA established that as of Jan.1, 2023, biometric data will be protected "sensitive personal information." "While the CPRA does permit the utilization of publicly available data, including information made available by the consumer, biometric data collected by a company without the consumer's knowledge cannot be regarded as "publicly available." Organizations will be required to provide consumers with notice prior to using or disclosing their biometric data, and consumers will be able to opt-out of having their personal data disclosed.



U.S. – Illinois, the Biometric Privacy Act and Rosenbach v. Six Flags

In 2008, the Illinois legislature passed the Biometric Information Privacy Act (BIPA), often regarded as the most robust biometric data privacy law in the U.S. The Act provides consumers with various protections by prohibiting businesses from collecting their biometric data without informing the consumer of the following:

- The data being collected
- The specific purpose for collection
- The length of time for which the data will be collected, stored and utilized

The consumer's written consent is also required for collection. BIPA prohibits businesses from selling or profiting from the biometric data collected from consumers, remaining the sole legal statute in the U.S. that addresses biometric data privacy and provides consumers with a private right of action to enable them to take businesses violating their data privacy rights to court.

While BIPA is consistently referenced as being one of the most consumer-friendly biometric data privacy statutes in the country, Illinois recently expanded consumers' rights even further. In January 2019, the Illinois Supreme Court decided *Rosenbach v. Six Flags*, ruling that a consumer-plaintiff alleging a breach of their right to privacy regarding their biometric data does not need to demonstrate additional harm besides a loss of the statutory biometric privacy right itself. The court held that a business defendant who has violated BIPA could be sanctioned with penalties even without a supplementary showing of injury.

U.S. – New York City and the Biometric Privacy Act

In July 2021, New York City enacted a novice biometric ordinance intended to regulate how businesses process and maintain consumers' biometric data. Requirements are imposed upon commercial establishments, including retail stores, restaurants, entertainment centers and others that use biometric data to identify consumers. Commercial establishments must post clear and visible signs near all consumer entrances to notify data subjects of the collection and purpose of collection of their biometric data. The ordinance also serves to make it unsuitable for businesses to sell, lease or profit from the biometric data collected and creates a private right of action for consumers to sue if they suffer violations of their right to privacy.

Violations are punishable by fines: Consumers' whose biometric data privacy rights have been infringed upon can recover $500 in damages per violation for a commercial establishment's failure to post adequate notice and $500 for each time an establishment negligently sells or shares consumers' data. If the establishment intentionally or recklessly sells or shares biometric data, consumers can recover $5,000 in fines per occurrence.

Conclusion

As more statutes and laws come into effect, the possibility of a company being impacted by regulatory investigations and penalties is growing. The risk depends on the willingness of administrative branches of government to impose fines and the size of those fines. With some statutes incorporating private rights of action, the risk is also being influenced by plaintiffs' counsel willing to take advantage of these new statutes.

Headlines have been dominated by hefty penalties imposed on large technology and social media companies that collect and monetize large amounts of personal information. However, these are not the only common claims. Statutes such as the BIPA are being used against many different companies on an increasing basis but with fewer headline-grabbing fines and judgments. As this is a dynamic area of cyber risk, there will be surprises in the way new privacy statutes are used before the risk becomes more predictable.

To date, cyber insurance policies have covered privacy fines and penalties along with the cost to defend investigations and court actions enforcing them. As fines are imposed on controls within a company's ability to put into place, insurance buyers should be proactive in communicating to cyber insurance underwriters that they have done their utmost to comply with these laws. The Brown & Brown Specialty Risk Solutions Cyber Risk team is available to assist companies in understanding cyber privacy laws and other developing cyber exposures.

About the Author

Nina Nisanova, *Executive Liability Intern*

Nina Nisanova is an intern in Brown & Brown's Executive Liability Practice in New York. She is currently a rising second-year student at Brooklyn Law School, aiming to complete her certificate in Business Law. Nina has a Bachelor of Arts from CUNY Hunter College in Political Science, with a concentration in International Relations.

Brown & Brown

Find Your Solution at BBrown.com