The Privacy Survival Guide

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

COVID-19 Emergency Exception Under the TCPA

AI in Interviews: What Illinois' Artificial Intelligence Video Interview Act Means for Employers

HIPAA Update: Lessons Learned from Recent Enforcement Actions

A U.S. National Consumer Privacy Law

Changes to States' Data Breach Notification Statutes

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**.

COVID-19 Emergency Exception Under the TCPA

Iliana L. Peters
JD, LLM, CISSP
Shareholder
Washington, D.C.

On March 20, 2020, the Federal Communications Commission (FCC) issued a **Declaratory Ruling** regarding the COVID-19 pandemic, noting that it may constitute an "emergency" under the Telephone Consumer Protection Act (TCPA) (47 U.S.C. § 227). For messages to meet this "COVID-19 Emergency Exception," two elements must be considered: the identity of the caller; and the content of the call or message:

First, the caller must be from a hospital, or be a health care provider, state or local health official, or other government official as well as a person under the express direction of such an organization and acting on its behalf.

Second, the content of the call must be solely informational, made necessary because of the COVID-19 outbreak, and directly related to the imminent health or safety risk arising out of the COVID-19 outbreak.

The FCC also gave important examples of communications and scenarios that would be or would not be permitted under the COVID-19 Emergency Exception:

Permitted by COVID-19 Emergency Exception

- A call made by a hospital providing vital and time-sensitive health and safety information that citizens welcome, expect, and rely upon to make decisions to slow the spread of the COVID-19 disease.
- An informational call designed to inform and update the public regarding measures to address the current pandemic made on behalf of, and at the express direction of, a health care provider would be made in a situation that "affect[s] the health and safety of consumers."

Not Permitted by COVID-19 Emergency Exception

- A call made by a county official informing citizens of shelter-in-place requirements, quarantines, medically administered testing information, or school closures necessitated by the national emergency would be made for an emergency purpose as such measures are designed to inhibit the spread of the disease.

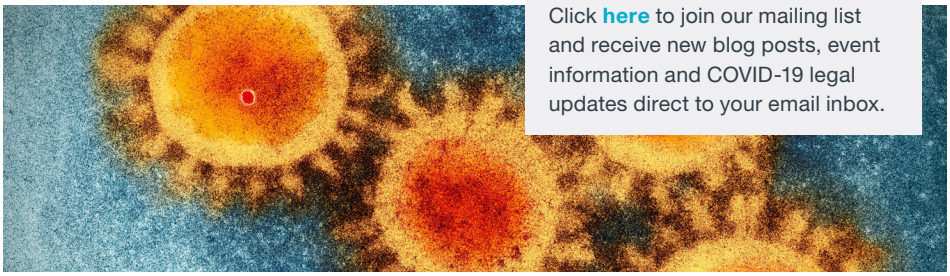
The FCC has arguably limited the emergency exception for communications to specific circumstances related to health care and public health in this Declaratory Ruling.

> **As a result, communications to individuals without express written consent under the TCPA should be limited to those related to their treatment by health care providers or COVID-19 issues identified by health care providers and for public health purposes.**

Read more about the TCPA and the COVID-19 Emergency Exception in the full article **here**.

COVID-19: What Your Business Needs To Know

Click **here** to join our mailing list and receive new blog posts, event information and COVID-19 legal updates direct to your email inbox.



AI in Interviews: What Illinois' Artificial Intelligence Video Interview Act Means for Employers

Adrienne A. Testa
Associate
Chicago

Scott M. Gilbert
Shareholder
Chicago

In the advent of automation and Artificial Intelligence (AI), U.S. companies are increasingly utilizing "smart" recruiting tools to streamline the hiring process. One trend that may redefine recruitment altogether is the use of AI in video interviews with potential job candidates. An applicant interviewed by an AI platform will respond to questions and generally present herself much the same way as she would an in-person interview. Meanwhile, as she speaks, the AI platform uses a series of algorithms to evaluate the applicant's choice of words, tone of voice, facial expressions, and body language. The resulting data – and that of all interviewed applicants – are then aggregated and analyzed, allowing employers to review interviewee performance in a fraction of the time it would have taken traditionally. In addition to yet-unequaled efficiency and flexibility, proponents of this technology also claim that AI video interviewing can eliminate the human bias element to hiring, yielding a fairer hiring landscape overall.

Illinois' Artificial Intelligence Video Interview Act: The First (but not the last) AI Law

Until recently, there were no U.S. laws regulating the use of AI to analyze video interviews with job applicants. That changed when Illinois enacted the Artificial Intelligence Video Interview Act (the "AIVI Act), **HB2557**, which passed by unanimous vote. Effective January 1, 2020, the AIVI Act imposes notification, transparency, consent, and data deletion requirements on employers using AI video interviews in their hiring processes. Although the Act specifies that it only applies to any applicant being interviewed for "positions based in Illinois," U.S. employers can reasonably anticipate a trend in similar legislation, now that other states can look to the AIVI Act as a first-of-its-kind model.

Key Employer Obligations Under the AIVI Act

Notify

Notify applicant before the interview that AI may be used to analyze his or her video interview and consider the applicant's fitness for the position.

Inform

Provide applicant with information before the interview explaining how the AI works and what general types of characteristics it uses to evaluate applicants.

Obtain Consent

- Obtain, before the interview, consent from applicant to be evaluated by the AI program.
- An employer may not use AI to evaluate applicants who have not consented to the use of AI analysis.

Limit Sharing

Do not share applicant's videos except with persons whose expertise or technology is necessary to evaluate applicant's fitness for a position.

Delete

- Upon request from applicant, delete applicant's interviews, including all electronically generated backup copies, within 30 days of receiving the request.
- Instruct any other persons in receipt of such videos to delete them.

Key Ambiguities of the AIVI Act

"Artificial Intelligence"

There is no definition of "Artificial Intelligence."

Enforcement?

The Act is silent on penalties, remedies, and enforcement of any kind.

Notice

- No indication of the extent to which an Employer must explain to candidates "how the AI works."
- Explaining an AI algorithm may prove extremely difficult depending both on the complexity of the software and the AI platform's willingness to divulge.

Withholding Consent

The Act is clear that consent is necessary before interviewing an applicant and using AI, but the Act is unclear whether an Employer may drop consideration of a candidate who does not consent.

Recordkeeping Laws

- Under the Act, Employers must delete interview videos within 30 days' of the applicant's request.
- It is unclear if and how this requirement interplays with Employers' other legal obligations to maintain personnel records for a defined period.

Key Takeaways

Companies will continue to lean on AI technology and, specifically, AI video interviewing to streamline and augment their human resources processes. However, AI's promise of ease and efficiency also brings employers the inextricable legal risks of a murky and underdeveloped regulatory landscape. Because the AIVI Act is the first law of

CONTINUED ON PAGE 4

CONTINUED FROM PAGE 3

its kind, Illinois employers can minimize risk of non-compliance by interpreting their obligations strictly until further clarification emerges. Employers using AI video interviewing should undertake the following to best insulate themselves in the interim:

- Determine a method for providing notice and obtaining consent from job applicants before conducting interviews.
- Alert the AI Platform provider of the employer's obligations under the AIVI Act to inform each applicant how the AI algorithm works and what characteristics the employer uses to evaluate applicants.
- Develop a process for receiving an applicant's request to delete interview videos, and for reconciling potentially competing record retention requirements.
- Maintain industry-standard security measures to prevent unauthorized access to confidential information.

Employers must always remain mindful of their other legal obligations during the hiring process. A company may still be liable for failing to accommodate

people with disabilities or discriminating against a protected class if its otherwise-compliant AI video interviews exhibit some other legal deficiency.

Finally, employers must remember that AI technology may inadvertently preserve human bias in the interview process. While AI video interviewing purports to eliminate human bias in interviewing through "neutral" algorithms, some speculate that algorithms emulate and build upon whatever human biases are present in their training datasets – often an employer's past hiring patterns. Given the lack of transparency into these proprietary algorithms, employers should be wary of this potential risk.

As always, employers are best-served consulting counsel before implementing any AI hiring platform.

HIPAA Update: Lessons Learned from Recent Enforcement Actions

Hale H. Melnick
Associate
Chicago

Abby E. Bonjean
Associate
Chicago

At the end of 2019, the Office for Civil Rights (OCR) announced a number of enforcement actions, including the imposition of two civil money penalties. A review of the recent enforcement actions reveals some common themes that covered entities and business associates can learn from to make any necessary updates to their HIPAA compliance programs. A few of the key takeaways are highlighted below.

Entities Continue to Struggle with the HIPAA Security Rule Risk Analysis Requirement

Almost all of the recent actions involving electronic protected health information (ePHI) highlighted the entity's failure to conduct an accurate and thorough risk analysis, as required by the HIPAA Security Rule. In November 2019, OCR announced that it imposed a $1.6 million civil money penalty (CMP) on the Texas Health and Human Services Commission (THHSC) after THHSC reported that the ePHI of 6,617 individuals was available on the internet. OCR's investigation found that, in addition to failing to conduct an accurate and thorough risk analysis, THHSC also failed to implement appropriate access and audit controls.

In October 2019, OCR imposed a $2.15 million CMP against Jackson Health System (JHS), a nonprofit academic medical center based in Miami. It operates six major hospitals, a network of urgent care centers, multiple primary and specialty care centers and several long-term care nursing facilities. JHS reported a number of incidents

CONTINUED ON PAGE 5

CONTINUED FROM PAGE 4

during the past few years, including an incident in 2016, which involved an employee inappropriately accessing the protected health information (PHI) of more than 24,000 patients during a five-year period and subsequently selling personal information. In addition to failing to provide timely notice to HHS regarding one of the incidents and failing to comply with the Information Access Management requirements, OCR determined that JHS failed to comply with the Security Management Process standard, which includes conducting an accurate and thorough risk analysis and implementing security measures to manage any identified risks.

Best practices for conducting an accurate and thorough risk analysis include:

Create an **inventory** of all of the ePHI in your organization and map how it flows throughout the organization

Identify a wide range of **threats** to the ePHI (e.g., hackers/thieves, internal users, natural disasters, etc.)

Identify existing **vulnerabilities** that a threat could exploit (e.g., a hacker is a threat that could exploit an unpatched software to gain access to an information system)

Evaluate existing **security measures**

Evaluate the **likelihood** that a threat will exploit a vulnerability and the impact it would have on the organization

Assign a **risk rating** by combining the likelihood and impact (e.g., high, medium or low)

Once the steps outlined above are completed, document a plan to address the identified risks. In addition to the risk analysis, OCR will request a copy of an organization's Risk Management Plan as part of any compliance review.

Encrypt, Encrypt, Encrypt

Despite advances in encryption technology and the fact that newer devices have it built-in, several of the recent enforcement actions stemmed from the loss or theft of unencrypted devices. At the end of October 2019, OCR announced a $3 million settlement with the University of Rochester Medical Center (URMC), one of the largest health systems in New York with more than 26,000 employees. URMC filed two breach reports in 2013 and 2017 regarding the loss of an unencrypted flash drive and the theft of an unencrypted laptop. OCR noted in its press release that, following a previous breach incident, URMC had identified unencrypted devices as a high risk, but failed to adequately address it.

While encryption is an addressable standard under the HIPAA Security Rule, it is not optional for entities to implement it. If an organization determines that it is not reasonable and appropriate to implement encryption based on an analysis of the factors outlined in 45 CFR 164.306, then the organization should document its rationale as to why it is not reasonable and appropriate and implement an equivalent security measure. If an organization has implemented encryption, it should maintain documentation of such, so it can prove a particular device is encrypted in the event it is lost or stolen.

Right of Access Initiative

Also toward the end of 2019, OCR announced the first settlements that are part of its Right of Access Initiative. The settlements followed an announcement OCR made earlier this year indicating that it planned to vigorously enforce the rights of patients to receive copies of their medical records promptly, without being overcharged, and in the readily producible format of their choice.

In September, Bayfront Health St. Petersburg (Bayfront), a Level II trauma and tertiary care center with 480 beds and 550 affiliated physicians, agreed to pay OCR $85,000 and adopt a corrective action plan after it failed to provide a mother timely access to records about her unborn child. In total, it took Bayfront more than nine months to adequately respond to the mother's initial written request, greatly exceeding the 30-day period required under HIPAA.

The corrective action plan requires Bayfront to, among other things:

- Develop, maintain, and revise its written access policies and procedures to comply with the Privacy Rule;
- Distribute the policies to its workforce members and business associates;
- Provide HHS the names of all of its business associates and all of its business associate agreements; and
- Develop and provide training to its workforce members and relevant business associates.

In December, Korunda Medical, LLC (Korunda), a health care company offering comprehensive primary care and interventional pain management, agreed to pay OCR $85,000 and adopt a corrective action plan after it repeatedly failed to timely forward a patient's medical record in electronic format to a third party and charged more than the reasonable cost-based fees allowed under HIPAA. Prior to entering into the settlement agreement and corrective action plan, and in response to the patient's initial complaint, OCR provided Korunda with technical assistance on how to resolve the issue. However, Korunda continued to fail to provide the requested record, and OCR intervened again, this time resulting in an official investigation.

Under the corrective action plan, Korunda is required to:

- Review and revise its policies and procedures related to patients' access to PHI;
- Provide annual training and training materials to all workforce members concerning an individual's right of access to PHI; and
- Submit a list of requests for access to PHI received by Korunda every 90 days during the term of the corrective action plan.

CONTINUED ON PAGE 6

CONTINUED FROM PAGE 5

Key Takeaways

- Review your organization's risk analysis process to confirm whether it addresses all of the elements described above.
- Ensure all devices are encrypted, especially if your organization has previously identified unencrypted devices as a high risk.
- Review your organization's access policies and procedures and ensure all relevant workforce members are trained on how to process access requests.

A U.S. National Consumer Privacy Law

Hale H. Melnick
Associate
Chicago

Joelle M. Wilson
Associate
Chicago

There is ongoing speculation surrounding whether the United States will implement a single, comprehensive federal law that regulates the collection and use of personal information. While the government currently regulates privacy and security, such regulations are segmented by sector and types of sensitive information (e.g., health and financial).

Over the years there have been several sweeping privacy regulations proposed or enacted in the US and Europe. In 2018, the European Union's General Data Protection Regulation (GDPR) went into effect, and California signed into law the California Consumer Privacy Act (CCPA).

In 2019, numerous national consumer privacy bills were proposed, (see Table 1), and several states proposed and/or passed legislation aimed at promoting transparency and protecting consumer privacy rights, (see Table 2). While we cannot predict if and when a national privacy law will be passed, proposed legislation and media insight provide a framework for what legislation could entail and how it could impact both consumers and businesses alike.

A national consumer privacy law would create a single unified law that could:

- Harmonize inconsistencies between existing federal and state laws and regulations;
- Apply across sectors, such as health and banking;
- Simplify business compliance;
- Provide individual with rights concerning transparency and control of their personal data;
- Provide consistent and coordinated enforcement of privacy violations; and
- Provide a mechanism for global interoperability.

CONTINUED ON PAGE 7

CONTINUED FROM PAGE 6

Table 1: Proposed National Privacy Bills

Proposed Privacy Act	Bill	Overview
Consumer Online Privacy Rights Act (COPRA)	S.2968	▪ Provides consumers with control over their personal data. ▪ Prohibits companies from using consumers' data to harm or deceive them. ▪ Establishes strict standards for the collection, use, sharing, and protection of consumer data. ▪ Penalizes companies that fail to meet data protection standards. ▪ Provides individuals with the right to pursue claims against entities that violate the law. ▪ Does not preempt state law.
Consumer Data Privacy Act of 2019 (CDAP)	Staff Discussion Draft Circulated	▪ Provides individuals with rights to access, delete, de-identify, and correct their data. ▪ Provides a right to data portability. ▪ Prohibits deceptive and harmful data practices. ▪ Creates a transparency requirement for organizations. ▪ Gives the Federal Trade Commission and state attorneys general enforcement authority. ▪ Preempts state laws related to data privacy and security. ▪ Does not provide individuals with a private right of action.
Online Privacy Act of 2019	H.R. 4978	▪ Provides individuals with rights to access, correct, and delete their data. ▪ Minimizes the amount of data companies collect, process, disclose, and maintain and bars companies from using data in discriminatory ways. ▪ Establishes an independent agency, the Digital Privacy Agency (DPA) to enforce privacy protections and investigate abuses. ▪ Empowers state attorneys general to enforce violations. ▪ Provides individuals with a private right of action.
Draft unnamed and unfinished Introduced by staffers on the House Energy and Commerce Committee, particularly Rep. Cathy McMorris-Rodgers (R-Wash.) and Rep. Jan Schakowsky (D-Ill).	Staff Discussion Draft Circulated	▪ Provides individuals with rights to access, delete, and correct covered information. ▪ Requires covered entities to publish transparent and accessible privacy policies and provide a mechanism for individuals to easily exercise their rights. ▪ Directs the Federal Trade Commission to establish a new Bureau of Privacy. ▪ Does not provide individuals with a private right of action. ▪ Does not state whether the bill would preempt state laws.
Social Media Privacy Protection and Consumer Rights Act of 2019	S.189	▪ Gives consumers the right to opt out and keep their information private by disabling data tracking and collection. ▪ Provides users greater access to and control over their data. ▪ Ensures users have the ability to see what information about them has already been collected and shared. ▪ Mandates that users be notified of a breach of their information within 72 hours. ▪ Offers remedies for users when a breach occurs. ▪ Requires that online platforms have a privacy program in place.

CONTINUED ON PAGE 8

CONTINUED FROM PAGE 7

While many agree on the need for a national privacy law, bipartisan support is necessary. The most divisive issues on the table include:

- **State Preemption:** Those in favor of state preemption believe that it ensures adequate protection for all consumers regardless of the state that they reside in, and would enable and ease compliance for small and large businesses alike. Those adverse to state preemption believe that federal law should not limit state laws that have taken measures to protect consumer privacy rights.
- **Private Right of Action:** Lawmakers in favor of private right of action argue that it would lead to increased corporate accountability. Those against it state that such a right would be detrimental to small businesses and cause frivolous litigation.

Will 2020 be the year of a U.S national consumer privacy law? Unlikely. But based on the proposed legislation pending in Congress and state legislatures, we are beginning to see what such a law would look like.

Table 2: Status of State Consumer Privacy Legislation*

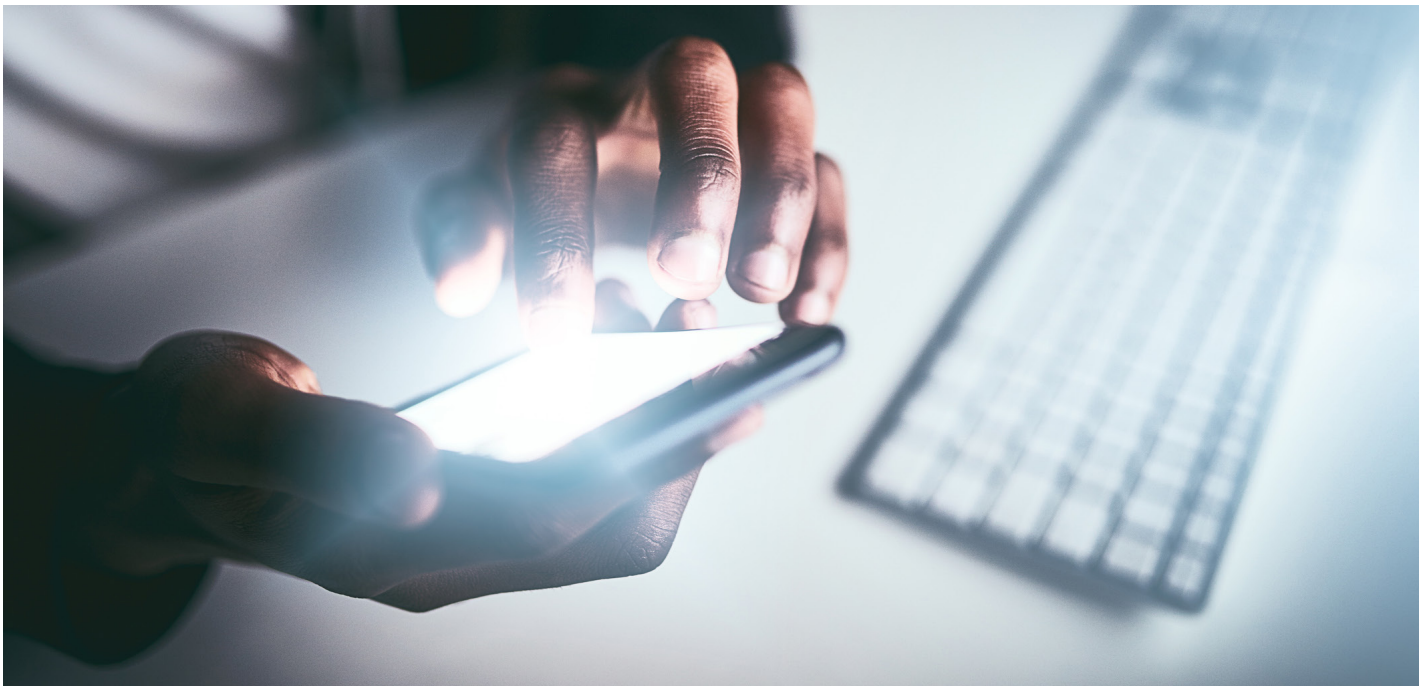
State	Statute/Bill	Status	Overview
Passed Legislation			
California	California Consumer Protection Act (CCPA) Ca. Civ. Code 1798.100-.199	Effective January 1, 2020	Gives California residents the right to know what data companies collect about them, and to opt out of having their data sold. Californians can sue businesses for certain types of data breaches.
Maine	Maine Act to Protect the Privacy of Online Consumer Information L.D. 946	Effective July 1, 2020	Prohibits a provider of broadband internet access service from using, disclosing, selling or permitting access to customers' personal information unless a customer expressly consents to that use, disclosure, sale or access. Requires providers to take reasonable measures to protect customers' personal information from unauthorized use, disclosure, sale or access.
Nevada	An Act Relating to Internet Privacy S.B. 220/Chapter 603A	Effective October 1, 2019	Prohibits an operator of a website or online service from selling certain information about consumers in the state.
Examples of Proposed Legislation			
Hawaii	Relating to Privacy S.B. 418	Pending	Requires a business to disclose the categories and specific pieces of identifying information collected about a consumer; the identity of third parties to which the business has sold or transferred identifying information; the categories of identifying information collected from consumers and the purposes for collection; and delete identifying information collected from a consumer upon request. Authorizes consumers to opt out of the sale of identifying information.
Illinois	Data Transparency and Privacy Act (DTPA) H.B. 3358	Pending	Provides that an entity that collects personal information about individual consumers, via the internet, must make disclosures to the individual regarding the collection of the information. Establishes that a consumer has a right to opt out of the sale of the consumer's information. Provides for enforcement by the attorney general.
Massachusetts	An Act Relative to Consumer Data Privacy S.D. 341/ S 120	Pending	Provides data subjects with the right to request a copy of their information or have it deleted. Requires organizations to inform individuals about the data they plan to collect and how it will be used. Provides individuals with a private right of action.
Minnesota	A Bill for an Act Relating to Data Privacy H.F. 2917/SF 2912	Pending	Requires controllers to provide, correct, or restrict processing of personal data upon a consumer's request. Requires controllers to provide a privacy notice and risk assessment. Provides for liability and civil penalties. Provides the attorney general with enforcement authority.

CONTINUED ON PAGE 9

CONTINUED FROM PAGE 8

State	Statute/Bill	Status	Overview
Passed Legislation			
New Jersey	An Act Concerning Commercial Internet Websites, Online Services, and Personally Identifiable Information S. 2834	Pending	Requires commercial websites and online services to notify customers of collection and disclosure of personally identifiable information. Provides individuals with the right to opt out.
New York	New York Privacy Act S. 5642	Pending	Requires companies to disclose their methods of de-identifying personal information, to place special safeguards around data sharing and to allow consumers to obtain the names of all entities with whom their information is shared. Creates a special account to fund a new office of privacy and data protection.
Pennsylvania	Consumer Data Privacy Act H.B. 1049	Pending	Provides privacy rights for consumers including the right to know and access personal information and the right to request deletion; provides individuals with the right to opt out; provides for a private right of action; provides the attorney general with enforcement oversight.
Rhode Island	Consumer Privacy Protection Act H. 5930/S. 0234	Pending	Requires businesses that collect, maintain or sell personal information to notify consumers; requires businesses to disclose information collected including the businesses' use of the information; provides consumers with the right to opt out and have personal information deleted; provides consumers with a private right of action.
Washington	Washington Privacy Act S.B 5376	Pending	Addresses the processing of personal data by controllers or processors; facial recognition for profiling; the state's citizens' right to privacy; transparency; exemptions; liability; and enforcement.

*The above table does not include proposed, passed or enacted legislation establishing a task force, advisory council, and/or legislative study of consumer data or consumer privacy.



Changes to States' Data Breach Notification Statutes

Jane P. Dennis
Associate
Seattle

Michael J. Waters
Shareholder
Chicago

Last year a handful of states amended their data breach notification statutes, many with a January 1, 2020, effective date. Specifically, six states amended their statutes to:

- Require notice to the state attorney general;
- Broaden existing definitions (e.g., expand the definition of "personal information");
- Add data security requirements;
- Regulate the insurance industry (through implementation of the National Association of Insurance Commissioner's 2017 Insurance Data Security Model Law);
- Require stricter notification timeframes;
- Allow the state attorney general to publish data breach information; and
- Add a specific risk of harm analysis.

A high-level overview of each state's data breach notification statute amendments are summarized in the chart below.

In light of these amendments, organizations should review their incident response plans to ensure compliance with the new data breach notification requirements.

Further to these amendments, recall amendments from the first and second quarters of 2019 in Michigan and Washington will soon take effect. Michigan's amendment states that impacting entities are regulated by the Insurance Code, and Washington's amendment broadens the definition of personal information and changes the timing of notification to both affected individuals and the attorney general from 45 to 30 days.

Additionally, keep in mind pending legislation in Iowa (S.F. 204), Maryland (H.B. 1127 and S.B. 786), Michigan (S.B. 653), Missouri (H.B. 1499), New Hampshire (H.B. 1482), New Jersey (A.B. 3245 and S.B. 2042), New York (A.B. 1387, 2540, 2868, 3001, 5635, and 7897, and S.B. 133, 5146, 5575, 5721, and 6701), North Carolina (H.B. 904), Oklahoma (S.B. 288), Pennsylvania (H.B. 245, 662, and 1181, and S.B. 308 and 487), Virginia (H.B. 1334), and Washington (S.B. 5064).

California

California amended its data breach notification statute (Cal. Civ. Code § 1798.82) to expand the definition of "personal information" to include biometric data and specific forms of identification.

Bill: A.B. 1130
Passed: October 11, 2019
Effective: January 1, 2020

Delaware

Delaware added a chapter to its Insurance Data Security Act (Del. Code tit. 18, §§ 8601-11) stating that a licensee has one year from July 31, 2019, to implement an information security program and two years from July 31, 2019, to implement oversight of third-party service provider arrangements.* The Act includes certain exceptions, including that a licensee with fewer than 15 employees is exempt from implementing an information security program. Notably, after the licensee determines that a cybersecurity event has occurred and certain criteria have been met, the licensee has three days to notify the Commissioner and 60 days to notify the impacted consumers.

Bill: H.B. 174
Passed: July 31, 2019
Effective: July 31, 2019*

State	AG Notice	Broader Definitions	Data Security Requirement	Insurance Regulation	Notice Time-Framing	Publication of Breach by AG	Specific Risk of Harm Analysis
California		■					
Delaware				■			
Illinois	■					■	
Maine		■			■		
New Hampshire				■			
New York		■	■				■

CONTINUED ON PAGE 11

CONTINUED FROM PAGE 10

New Hampshire

New Hampshire added a chapter to its Insurance Data Security Law (N.H. Rev. Stat. Ann. § 420-P:1, et seq.) stating that a licensee has one year from January 1, 2020, to implement an information security program and two years from January 1, 2020, to implement oversight of third-party service provider arrangements.* The Act includes certain exceptions, including that a licensee with fewer than 20 employees is exempt from implementing an information security program. Notably, after the licensee determines that a cybersecurity event has occurred and certain criteria have been met, the licensee has three business days to notify the Commissioner.

Bill: S.B. 194
Passed: August 2, 2019
Effective: January 1, 2020*

Maine

Maine amended its data breach notification statute (Me. Rev. Stat. tit. 10, § 1346, et seq.) to specifically include "municipalities" and "school administrative units" to the definition of a "person" required to provide notice of breaches in personal data security. Additionally, the statute now includes a notification time frame of 30 days if there is no delay due to a law enforcement investigation.

Bill: L.D. 696
Passed: June 28, 2019
Effective: September 18, 2019

New York

New York amended both its data breach notification statutes (N.Y. Gen. Bus. Law § 899-aa (non-governmental entities, and N.Y. State Tech. § 208 (governmental entities)) to broaden the definition of "personal information" to include account number alone if used to access an individual's financial account without additional information, biometric information, and user name or email address in combination with a password. The amendments expand the definition of a breach to include an unauthorized "access to" private information, and no longer require an entity to do business in New York in order to be subject to the statutes. Additionally, the amendments require covered entities that are obligated to notify the U.S. Department of Health and Human Services Office for Civil Rights of a data breach to provide such notification to the attorney general within five days of notifying the OCR.

Further, New York added data security protections (N.Y. Gen. Bus. Law § 899-bb) requiring businesses that own or license New York residents' private information in computerized form to "develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information including, but not limited to, disposal of data."

Bill: S. 5575-B
Passed: July 25, 2019
Effective:
October 23, 2019 (N.Y. Gen. Bus. Law § 899-aa & N.Y. State Tech. § 208)
March 21, 2020 (N.Y. Gen. Bus. Law § 899-bb)

Illinois

Illinois amended its data breach notification statute (815 Ill. Comp. Stat. 530/1, et seq.) to require notification to the state attorney general, if more than 500 individuals are affected, "in the most expedient time possible and without unreasonable delay[,] but in no event later than when the data collector provides notice to consumers[.]" The attorney general may also "publish the name of the data collector that suffered the breach, the types of personal information compromised in the breach, and the data range of the breach." This does not apply to covered entities or business associates in compliance with the Personal Information Protection Act (815 Ill. Comp. Stat. 530/50).

Bill: S.B. 1624
Passed: August 9, 2019
Effective: January 1, 2020

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

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

JUNE 2020 | VOL. 2