Distributed by Genesee Regional Bank with permission

New York SHIELD Act Compliance Checklist

CHANGES TO N.Y. GEN. BUS. LAW § 899-AA (NEW YORK'S DATA BREACH NOTIFICATION STATUTE) – EFFECTIVE OCTOBER 23, 2019

New information types added to definition of "private information" that can give rise to a reportable breach:

- Biometric information*
- Account number (such as a credit card or other financial account number) if the number can be used without additional identifying information (such as over the phone or other card-not-present transactions)*
- User name or e-mail address and password

*in combination with some type of identifier, such as name, number, or personal mark

Compliance needs

Has your organization:

- ☐ Identified and secured repositories of these types of information?
- ☐ Incorporated these types of information as triggers for potentially material security incidents in your Incident Response Plan?
- ☐ Reviewed vendor contracts to ensure proper protection of these types of information, as well as appropriate reporting to and indemnification of your organization in the case of a third-party breach?
- ☐ Properly disposed of these types of information after they are no longer needed for business purposes by erasing electronic media so that the information cannot be read or reconstructed?

Includes unauthorized "access" to private information as a trigger for a reportable breach.

Compliance needs

Has your organization:

- ☐ Educated internal stakeholders that unauthorized access, on its own, can lead to a reportable breach?
- ☐ Established logging procedures, and a log management system, to determine whether unauthorized access to private information has occurred?
- ☐ Added an unauthorized access trigger to your Incident Response Plan, when determining whether a potentially material incident has occurred?
- ☐ Reviewed vendor contracts to ensure that these entities inform you of unauthorized access?

Extends the reach of §§ 899-aa and 899-bb to any person or business that owns or licenses private information of a New York resident, regardless of geography.

Compliance needs

Has your organization:

- ☐ Analyzed its operations and affiliates to ensure proper data protection of New York private information regardless of location?

Requires HIPAA-regulated entities covered by the law to report all HIPAA-reportable breaches to the New York Attorney General's Office.

Compliance needs

Has your organization:

- ☐ Educated internal stakeholders that a HIPAA reportable breach is now reportable to the New York authorities?
- ☐ Adjusted your Incident Response Plan to ensure prompt notification to state authorities, as appropriate?

Increases monetary penalties, as well as the time within which the attorney general may commence an action following a violation of the law.

Compliance needs

Has your organization:

- ☐ Created a policy of keeping written documentation of all decisions surrounding potential incidents for at least seven years (one year longer than the statute of repose)?

NEW REQUIREMENTS UNDER § 899-BB (DATA SECURITY PROTECTIONS) – EFFECTIVE MARCH 21, 2020

Any person or business that owns or licenses computerized private information of a New York resident must develop, implement, and maintain reasonable safeguards to protect the security, confidentiality, and integrity of that private information including, but not limited to, disposal of data.

Compliance needs

Has your organization:

- ☐ Reviewed your security program in light of the changes noted above in the definition of "private information" under § 899-aa (*e.g.*, biometric information, user name and password)?
- ☐ Reviewed your disposal practices to ensure they safeguard the security, confidentiality and integrity of the data disposed of?

* Note: "disposal" is mentioned three separate times in § 899-bb. It is a key element to SHIELD Act compliance and one often overlooked by organizations standing up SHIELD-Act compliant security programs.

A "compliant regulated entity" meets the requirement above if it is governed by and compliant with any of the following regulatory regimes in relation to information security: HIPAA; GLBA, 23 N.Y.C.R.R. Part 500, or any other applicable state or federal information security law or regulation.

Compliance needs

Has your organization:

- ☐ Determined whether, and to what extent, your organization is a "compliant regulated entity?"

* Note: an organization is only a "compliant regulated entity" to the extent it is compliant with, and subject to, one of the regulatory regimes noted above. A reportable breach is usually a sign of potential non-compliance.

Any other person or business can show compliance with the SHIELD Act, by implementing a data security program that includes the following:

Administrative Safeguards, including:

- designating one or more employees to coordinate the security program;
- identifying reasonably foreseeable internal and external risks;
- assessing the sufficiency of safeguards in place to control the identified risks;
- training and managing employees in the security program practices and procedures;
- selecting service providers capable of maintaining appropriate safeguards, and requiring those safeguards by contract; and
- adjusting the security program in light of business changes or new circumstances; and

Technical Safeguards, including:

- assessing risks in network and software design;
- assessing risks in information processing, transmission and storage;
- detecting, preventing and responding to attacks or system failures; and
- regularly testing and monitoring the effectiveness of key controls, systems and procedures; and

Physical Safeguards, including:

- assessing risks of information storage and disposal;
- detecting, preventing and responding to intrusions;
- protecting against unauthorized access to or use of private information during or after the collection, transportation and destruction or disposal of the information; and
- disposing of private information within a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so that the information cannot be read or reconstructed.

Compliance needs

Has your organization:

- ☐ Reviewed your information security program in light of these requirements?
- ☐ Conducted a formal Risk Assessment, with the aid of counsel? (Risk Assessment is mentioned twice in § 899-bb and a key element of establishing any information security program.)
- ☐ Tested your ability, in a table-top exercise, to detect, prevent, and respond to attacks (mentioned twice in § 899-bb)?
- ☐ Assessed and adjusted disposal practices, in light of the new requirements?

For More Information:

Contact a Harter Secrest & Emery Privacy and Data Security team member or subscribe to our Privacy and Data Security Blog at hselaw.com/blog/privacy-and-data-security.

F. Paul Greene, CIPP/US
Partner and Chair
fgreene@hselaw.com
585.231.1435

Daniel J. Altieri
Senior Associate
daltieri@hselaw.com
716.844.3741

Laura K. Schwalbe, CIPP/US
Senior Associate
lschwalbe@hselaw.com
716.844.3752