**NY SHIELD ACT CHEAT SHEET Jan 2020**

|  |  |
| --- | --- |
| **Data Governance**  | **PI (Personal Information)**consisting of any information in combination with any one or more of the following data elements:Where the PI plus the data element are not encrypted, or the encryption key has also been accessed or acquired:* social security number;
* driver's license number or non-driver identification card number;
* account number, credit or debit card number:
	+ in combination with any required security code, access code, password permitting access to a financial account.
* biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as:
	+ fingerprints;
	+ voice prints;
	+ retina or iris image; or
	+ other unique physical representation or digital representation of biometric data used to authenticate or ascertain the individual's identity.
 |
| **a user name or e-mail address in combination with a password or security question and answer that would permit access to an online account; or** |
| **any unsecured protected health information held by a "covered entity" as defined by HIPAA.** |
| **Security** (Administrative and Technical Safeguards)  | **Deemed Compliant if it:*** is a compliant regulated entity as defined in this Act; or
* implements a data security program that includes administrative and technical safeguards, in which the person or business:
	+ is a compliant regulated entity as defined in this Act; or
	+ implements a data security program that includes administrative and technical safeguards, in which the person or business:
	+ *designates one or more employees to coordinate the security program;*
	+ *identifies reasonably foreseeable internal and external risks;*
	+ *assesses the sufficiency of safeguards in place to control the identified risks;*
	+ *trains and manages employees in the security program practices and procedures;*
	+ *selects service providers capable of maintaining appropriate safeguards, and requires those safeguards by contract;*
	+ *adjusts the security program in light of business changes or new circumstances;*
	+ *assesses risks in: network and software design; and information processing, transmission, storage and disposal.*
	+ *detects, prevents and responds to intrusions, attacks or system failures;*
	+ *regularly tests and monitors the effectiveness of key controls, systems and procedures;*
	+ *protects against unauthorized access to or use of PI during or after the collection, transportation and destruction or disposal of PI*

A small business is deemed compliant if its security program contains reasonable safeguards appropriate to the business': size and complexity; nature and scope of its activities; and sensitivity of PI it collects from or about consumers. |
| **Data Management**(Data Destruction)  | **Deemed Compliant if it:*** If the business disposes PI 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.
 |
| **Breach Notification**  | **Definition of “ breach of security of the systems”*** unauthorized access to or acquisition of, or access to or acquisition without valid authorization, of computerized data *that compromises the security, confidentiality, or integrity of PI maintained by a business.*
* good faith access to, or acquisition of PI by an employee or agent of the business for the purposes of the business is not a breach: provided the PI is not used or subject to unauthorized disclosure.
* in determining whether information has been accessed, by an unauthorized person:

*the business may consider indications that the information was viewed, communicated with, used or altered by an unauthorized person* |
| **Breach Notification** 1. **Notification is not required if the exposure of PI was inadvertent:**
* by persons authorized to access PI; and
* the person or business reasonably determines such exposure will not likely result in:
	+ *misuse of the information; or*
	+ *financial or emotional harm to the affected persons.*

**such a determination must be documented in writing and maintained for at least 5 years;****the person or business must provide a copy to the state attorney general ("AG") within 10 days after the determination.**1. **Notification is not required where notification is made in accordance with the following laws, no further action is required:**
* regulations promulgated pursuant to the: GLBA & HIPAA.
* part 500 of Title 23 of the official compilation of codes, rules and regulations of the state of the New York; or
* any other data security rules and regulations administered by an official agency or department in the state of New York
1. **Form of notice:**

**email notification is permitted,** except if the breached information includes an email address in combination with a password or security question and answer permitting access to an online account.where email cannot be used for this purpose, clear and conspicuous notice must be delivered online to the consumer:when the consumer is connected to the online account from an IP address or online location that the consumer is known to customarily use.1. **Content of notice:**
* Regardless of the method, notice shall include:
	+ contact information for the person or business making the notification; and
	+ the telephone numbers and websites of the relevant state and federal agencies that provide relevant information.
* Where New York residents are involved, notification is required to the AG, department of state and the office of information technology services:
* as to the: timing, content and distribution of the notices; and

approximate number of affected persons. * including a copy of the template of the notice sent to affected persons.
 |
| **Enforcement Action** | **Enforcement:*** Violation of the breach notification provisions is only punishable if action is commenced within 3 years of the AG becoming aware of the violation; and
* Nothing in the security provisions shall create a private right of action: however, failure to comply is subject to enforcement by the AG.
 |