GORDON REES
SCULLY MANSUKHANI LLP

Legal Education Conference 2015

Cyber/Data Breach Reference Guide: Best Practices, State Surveys, HIPAA Enforcement

DATA BREACH: BEST PRACTICES

ASSESS

- ✓ What type of sensitive data do you have? Financial? Health?
  Engage legal counsel to determine framework for security per applicable laws
- ✓ How is your IT and cybersecurity infrastructure?
- ✓ Who has access to your network and databases? How is the access managed?
- ✓ Engage IT personnel with expertise in cybersecurity and data management.
  Does your company have an intrusion detection or prevention system? Is it current?
  How is the system managed? How are intrusion alerts triaged and managed?
- ✓ Implement up to date anti-malware software

PREVENT

- ✓ Microchip cards (e.g.”Europay MasterCard Visa”) technology
- ✓ Advise customers/clients and vendors to protect themselves
  (e.g., don’t recycle passwords and have some level of uniqueness for passwords)
- ✓ Shredding
- ✓ Secure with lock and key or pass code; restrict access to keys and pass codes
- ✓ Encryption
- ✓ Train employees on cybersecurity
- ✓ Data Governance Committee
  - Report to BOD audit committee
    - Comprised of chief information officer, the chief risk officer, the chief operating officer, the chief marketing officer and the general counsel—everybody that has a role in how the organization uses, retains and secures data; create director position for cybersecurity/data
    - Role: monitor data compliance processes within the company, and propose policy fixes and revisions for the company’s handling of data; examine alleged violations of data governance policies and escalate issues up the corporate chain of command; review contracts with third party IT vendors to ensure all data is secure and accounted for; perform annual evaluations of data governance and security; understand how data works across all departments.

CONTACTS

Andrew D. Castricone
275 Battery Street, Suite 2000
San Francisco, CA 94111
(415) 875-3183
acastricone@gordonrees.com

Craig J. Mariam
633 West Fifth Street, 52nd Floor
Los Angeles, CA 90071
(213) 270-7856
cmariam@gordonrees.com

DATA BREACH STATUTES: A STATE BY STATE SURVEY

As referenced below, Personal Information ("PI") is defined as: An individual's first name or first initial and last name plus one or more of the following data elements: (i) Social Security number, (ii) driver's license number or state- issued ID card number, (iii) account number, credit card number or debit card number combined with any security code, access code, PIN or password needed to access an account and generally applies to computerized data that includes personal information. Personal Information shall not include publicly available information that is lawfully made available to the general public from federal, state or local government records, or widely distributed media. In addition, Personal Information shall not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

DATA BREACH NOTIFICATION STATUTES

State	Statute(s)	Summary	Notes
AK	Alaska Stat. § 45.48.010 *et seq.*	PI of Alaska residents, as well as passwords, personal identification numbers, or other access codes for financial accounts; Notice is not required if, after an investigation and written notice to the Attorney General, the entity determines that there is not a reasonable likelihood that harm to the consumers has or will result. The determination must be documented in writing and maintained for five years. Safe Harbor: The statute only applies to unencrypted information or encrypted information when the encryption key has also been disclosed.	Alaska permits a private right of action against a non-governmental agency under the Unfair or Deceptive Act or Practices, AS 45.50.471; 45.50.561. Not limited to electronic records.
AZ	Ariz. Rev. Stat. § 44-7501	PI of Arizona residents. Notice not required if the breach does not materially compromise the security of the personal information maintained or if the entity or a law enforcement agency, after a reasonable investigation, determines that a breach of the security of the system has not occurred or is not reasonably likely to occur. Safe Harbor: Notification requirement only applies where personal information was unencrypted.	The Act is to be repealed one year after the effective date of the federal personal data privacy and security act.
AR	Ark. Code Ann. § 4-110-101 *et seq.*	PI of Arkansas residents., as well as medical information. Notification not required if, after a reasonable investigation, the person or business determines that there is no reasonable likelihood of harm to customers. Safe Harbor: Statute only applies to unencrypted data elements.	
CA	Cal. Civ. Code §§ 1798.29, 1798.45 *et seq.*, 1798.80 *et seq.*	PI of California residents, as well as username or e-mail address in combination with password or security question and answer. Medical and health information. Required reporting to California Attorney General and California Department of Health Services no later than 15 days (effective Jan 1, 2015) after unauthorized access is detected. Safe Harbor: Notification under the general breach notification statute only applies where unencrypted personal information was acquired, or is believed to acquired, by an unauthorized person.	California permits a private right of action. Any customer injured by a violation of the general breach notification statute may institute a civil action to recover damages. Any business that violates, proposes to violate, or has violated this title may be enjoined.

DATA BREACH NOTIFICATION STATUTES

State	Statute(s)	Summary	Notes
CO	Colo. Rev. Stat. § 6-1-716	PI of Colorado residents. Notification is not required if after a good-faith, prompt and reasonable investigation, the entity determines that misuse of personal information about a Colorado resident has not occurred and is not likely to occur. Safe Harbor: Statute applies only to the disclosure of unencrypted computerized data.	
CT	Conn. Gen Stat. § 36a-701b	PI of Connecticut residents. "Breach of security" means unauthorized access to or unauthorized acquisition of electronic files, media, databases, or computerized data containing personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable. Notification is not required if, after a reasonable investigation and consultation with relevant law enforcement agencies, it is determined that there is no reasonable likelihood of harm to customers. Required reporting to Connecticut Attorney General.Safe Harbor: A breach of security only occurs when access to the personal information has not been secured by encryption or by any other method or technology that renders personal information unreadable or unusable.	
DE	Del. Code Ann. tit. 6, § 12B-101 *et seq.*	PI of Delaware residents. Notification only required if an investigation determines that the misuse of information about a Delaware resident has occurred or is reasonably likely to occur. Safe Harbor: The statute applies to unencrypted computerized data.	
FL	Fla. Stat. § 501.171	PI of Florida residents, as well as username or e-mail address in combination with password or security question and answer that would permit access to an online account, financial account with any required security code, medical history, and health insurance policy or subscriber information. Notice is not required if, after an appropriate investigation and consultation with relevant federal, state, or local law enforcement agencies, the covered entity reasonably determines that the breach has not and will not likely result in identity theft or any other financial harm to the individuals whose personal information has been accessed. Determination must be documented in writing and maintained for at least 5 years. Required reporting to Florida Department of Legal Affairs no later than 30 days after breach has occurred. Safe Harbor: The statute applies to unencrypted information.	

DATA BREACH NOTIFICATION STATUTES

State	Statute(s)	Summary	Notes
GA	Ga. Code Ann. §§ 10-1-910-912; § 46-5-214	PI of Georgia residents, as well as any of the following standing alone if the information compromised would be sufficient to steal identity: social security number; driver's license number or state identification card number; account number, credit card number, or debit card number; account passwords or personal identification numbers or other access codes. Safe Harbor: The statute applies to unencrypted personal information.	
HI	Haw. Rev. Stat. § 487N-1 *et seq.*	PI of Hawaii residents. Notification required where illegal use of PI has occurred or is reasonably likely to occur and creates a risk of harm to a person. Required reporting to Hawaii Office of Consumer Protection. Safe Harbor: The statute applies only to disclosure of unencrypted or unredacted information.	Not limited to electronic records.
ID	Idaho Code Ann. §§ 28-51-104 to -107	PI of Idaho residents. Notification required if an investigation determines that the misuse of information about an Idaho resident has occurred or is reasonably likely to occur. Required reporting to Idaho Attorney General within 24 hours of discovery of breach.	
IL	815 Ill. Comp. Stat. §§ 530/1 to 530/25	PI of Illinois residents. State agencies must report breaches to Illinois General Assembly within 5 days. Safe Harbor: The statute applies to unencrypted and unredacted personal information.	
IN	Ind. Code §§ 24-4.9 *et seq.*	PI of Indiana residents. Notification required if the database owner knows, should know, or should have known that the unauthorized acquisition constituting the breach has resulted in or could result in identity deception, identity theft, or fraud affecting the Indiana resident. Required reporting to Indiana Attorney General. Safe Harbor: The statute does not cover personal information if it is"encrypted, redacted, or otherwise altered in such a manner that the name or data elements are unreadable" unless the keys to unencrypt, unredact, or otherwise read the data have been obtained through a breach of security.	

DATA BREACH NOTIFICATION STATUTES

State	Statute(s)	Summary	Notes
IA	Iowa Code §§ 715C.1, 715C.2	PI of Iowa residents, including a unique electronic identifier or routing code, in combination with any required security code, access code, or password that would permit access to an individual's financial account; unique biometric data, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data. Notification is not required if, after an appropriate investigation or after consultation with the relevant federal, state, or local agencies responsible for law enforcement, the person determined that no reasonable likelihood of financial harm to the consumers whose personal information has been acquired has resulted or will result from the breach. Such a determination must be documented in writing and the documentation must be maintained for five years. "Breach of security" means unauthorized acquisition of personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of the personal information."Breach of security" also means unauthorized acquisition of personal information maintained by a person in any medium, including on paper, that was transferred by the person to that medium from computerized form and that compromises the security, confidentiality, or integrity of the personal information. Required reporting to Iowa Attorney General within 5 days.	Not limited to electronic records
KS	Kan. Stat. Ann. § 50-7a01 et seq.	PI of Kansas residents, as well as account number alone or in combination with any required security code or password to permit access to financial account. Notification required if, following reasonable and prompt investigation, it is determined that misuse of information has occurred or is reasonably likely to occur. Safe Harbor: The statute is triggered by disclosure of unencrypted or unredacted information.	
KY	Ky. Rev. Stat. Ann. § 365.732, KRS §§ 61.931 to 61.934	PI of Kentucky residents. Notification is required if the unauthorized acquisition of unencrypted and unredacted computerized data actually causes, or leads the information holder to reasonably believe has caused or will cause identity theft or fraud against any Kentucky resident.	
LA	La. Rev. Stat. Ann. § 51:3071 *et seq.*, L.A.C. tit. 16, § 701.	PI of Louisiana residents. Notification is not required if after reasonable investigation the person or business determines that there is no reasonable likelihood of harm to customers. Required reporting to Louisiana Attorney General within 10 days of breach. Safe Harbor: The statute is triggered by unauthorized acquisition of unencrypted and unredacted computerized data.	Louisiana provides a private right of action. A civil action may be instituted to recover actual damages resulting from the failure to disclose in a timely manner to a person that there has been a breach of the security system resulting in the disclosure of a person's personal information.

DATA BREACH NOTIFICATION STATUTES

State	Statute(s)	Summary	Notes
ME	Me. Rev. Stat. tit. 10 § 1347 *et seq.*	PI of Maine residents, as well as a password, if any of the other data elements alone would be sufficient to permit a person to fraudulently assume or attempt to assume the identity of the person whose information was compromised. Notification is not required if after conducting a good-faith, reasonable and prompt investigation, the entity determines that there is not a reasonable likelihood that the personal information has been or will be misused. Required reporting to Maine Attorney General or Department of Professional and Financial Regulation. Safe Harbor: The statute only applies to disclosure of information that is not encrypted.	
MD	Md. Code Ann., Com. Law §§ 14-3501 *et seq.,* Md. Code Ann., State Gov't §§ 10-1301 to 1308	PI of Maryland residents, as well as individual Taxpayer Identification Number. Notification is not required if after a good-faith, reasonable and prompt investigation the entity determines that the personal information of the individual was not and will not be misused as a result of the breach. If after the investigation is concluded, the entity determines that notification is not required, the entity shall maintain records that reflect its determination for three years after the determination is made. Required reporting to Maryland Attorney General. Safe Harbor: The statute only applies to disclosure of personal information that has not been encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable.	Maryland provides a private right of action. Consumers may bring actions under Title 13 of the Maryland Code, the Unfair and Deceptive Trade Practices Act.
MA	Mass. Gen. Laws § 93H-1 *et seq.*	PI of Massachusetts residents, as well as financial account information with or without password or security code information. Data is any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics. Notice to affected residents must include (1) consumer's right to obtain a police report; (2) how a consumer requests a security freeze; and (3) fees paid to any of the consumer reporting agencies. Required reporting to Massachusetts Attorney General. Safe Harbor: No notice is required as long as the data acquired or used is encrypted, and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information has not been acquired.	Massachusetts provides for a private right of action. Massachusetts consumers may seek damages under Chapter 93A, which allows for certain instances of treble damages. Not limited to electronic records.

DATA BREACH NOTIFICATION STATUTES

State	Statute(s)	Summary	Notes
MI	Mich. Comp. Laws §§ 445.63, 445.72	PI of Michigan residents. The person or agency does not have to provide notice if the person or agency determines that the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to, one or more residents of Michigan. In making this determination, a person or agency shall act with the care an ordinarily prudent person or agency in like position would exercise under similar circumstances. Required reporting to Michigan Attorney General. Safe Harbor: A person or agency does not have to give notice if the resident's data was encrypted or redacted, and the person gaining unauthorized access did not have the encryption key.	
MN	Minn. Stat. §§ 325E.61, 325E.64	PI of Minnesota residents. A person or business must give notice of a security breach if personal information is acquired. Personal information does not include encrypted data.	Private right of action.
MS	Miss. Code Ann. § 75-24-29	PI of Mississippi residents. Notification is not required if, after an appropriate investigation, the person reasonably determines that the breach will not likely result in harm to the affected individuals. Safe Harbor: Does not cover encrypted data unless obtained in encrypted form by a party with unauthorized access to encryption key.	
MO	Mo. Rev. Stat. § 407.1500	PI of Missouri residents, as well as unique electronic identifier or routing code in combination with required security code, access code, or password that would permit access to an individual's financial account; medical and health insurance information, including an individual's medical history, mental or physical condition, treatment or diagnosis, health insurance policy number and any other unique identifier used by a health insurer. Notification is not required if, after an appropriate investigation by the person or after consultation with the relevant federal, state, or local agencies responsible for law enforcement, the person determines that a risk of identity theft or other fraud to any consumer is not reasonably likely to occur as a result of the breach. Such a determination shall be documented in writing and the documentation shall be maintained for five years. Safe Harbor: Personal information does not include information that is encrypted.	

DATA BREACH NOTIFICATION STATUTES

State	Statute(s)	Summary	Notes
MT	Mont. Code Ann. § 2-6-504, 30-14-1701 *et seq.*	PI of Montana residents, including insurance policy number. Notification required if the unauthorized acquisition of computerized data materially compromises the security, confidentiality, or integrity of personal information and causes or is reasonably believed to cause loss or injury to a Montana resident. Safe Harbor: The statute applies only to disclosures of unencrypted information.	
NE	Neb. Rev. Stat. §§ 87-801 *et seq.*	PI of Nebraska residents, as well as a unique electronic identification number or routing code, in combination with any required security code, access code, or password; or unique biometric data, such as finger print, voice print, or retina or iris image, or other unique physical representation. If the investigation determines that the use of information about a Nebraska resident for an unauthorized purpose has occurred or is reasonably likely to occur, the individual or commercial entity shall give notice to the affected Nebraska resident. Safe Harbor: Notice is not required if data is encrypted or redacted.	
NV	Nev. Rev. Stat. §§ 603A.010 *et seq.*, 242.183	PI of Nevada residents. Notification is required if the unauthorized acquisition of computerized data materially compromises the security, confidentiality, or integrity of personal information maintained by the data collector. Safe Harbor: If the data is encrypted, notice is not required.	
NH	N.H. Rev. Stat. Ann. §§ 359-C:19, -C:20, -C:21	PI of New Hampshire residents, as well as medical information as defined under federal law. For Personal Information Breach Notification Statute: Notification is not required if it is determined that misuse of the information has not occurred and is not reasonably likely to occur. Required reporting to New Hampshire Attorney General. Safe Harbor: If the data elements are encrypted, notification is not required.	New Hampshire provides for a private right of action. Persons injured as a result of a violation may bring an action for damages and for such equitable relief as the court deems necessary and proper. A prevailing plaintiff shall be awarded the costs of the suit and reasonable attorney's fees. An aggrieved individual whose health records were wrongly disclosed may bring a civil action under RSA 332-I:4 or RSA 332-I:5 and, if successful, shall be awarded special or general damages of not less than $1,000 for each violation, and costs and reasonable legal fees.

DATA BREACH NOTIFICATION STATUTES

State	Statute(s)	Summary	Notes
NJ	N.J. Stat. Ann. § 56:8-163	PI of New Jersey Residents, as well as dissociated data that, if linked, would constitute personal information is personal information if the means to link the dissociated data were accessed in connection with access to the dissociated data. "Breach of security" means unauthorized access to electronic files, media or data containing personal information that compromises the security, confidentiality or integrity of personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable. Notification is not required if the business or public entity establishes that misuse of the information is not reasonably possible (must retain a record of this decision for five years). Required reporting to New Jersey Division of State Police before consumers are notified. Safe Harbor: Statute applies to personal information that has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable.	
NM	None		
NY	N.Y. Gen. Bus. Law § 899-aa, N.Y. State Tech. Law § 208	The law applies to"private information," which means personal information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person, in combination with any one or more of the following data elements: (1) Social Security number; (2) driver's license number or non-driver identification card number; or (3) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, such business may consider the following factors, among others: (1) indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or (2) indications that the information has been downloaded or copied; or (3) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported. Required reporting to New York Attorney General, Consumer Protection Board, and state office of Cyber Security and Critical Infrastructure. Safe Harbor: When the private information is encrypted and the encryption key has not been acquired.	Private information does not include publicly available information which is lawfully made available to the general public from federal, state, or local government records.

DATA BREACH NOTIFICATION STATUTES

State	Statute(s)	Summary	Notes
NC	N.C. Gen. Stat §§ 75-61, 75-65	The law applies to a person's first name or initial and last name, in combination with any one or more of the following: (1) Social Security number; (2) driver's license or State ID number; (3) account number, credit or debit card number, in combination with security or access codes or passwords to an individual's financial account; (4) biometric data; (5) finger prints; (6) other information that would permit access to a person's financial account or resources. Notification not required if a breach does not result in illegal use of personal information, is not reasonably likely to result in illegal use, or there is no material risk of harm to a consumer. Required reporting to North Carolina Attorney General. Safe Harbor: Notification requirement only applies where the personal information acquired is unencrypted and unredacted.	Provides a private right of action only if individual is injured as a result of the violation. Not limited to electronic records. Personal Information does not include electronic identification numbers, electronic mail names or addresses, Internet account numbers, Internet identification names, parents' legal surname prior to marriage, or a password unless this information would permit access to a person's financial account or resources.
ND	N.D. Cent. Code § 51-30-01 *et seq.*	"Personal information" means an individual's first name or first initial and last name in combination with any of the following data elements, when the name and the data elements are not encrypted: (1) the individual's social security number; (2) the operator's license number assigned to an individual by the department of transportation; (3) a nondriver color photo identification card number assigned to the individual by the department of transportation; (4) the individual's financial institution account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial accounts; (5) the individual's date of birth; (6) the maiden name of the individual's mother; (7) medical information; (8) health insurance information; (9) an identification number assigned to the individual by the individual's employer; or (10) the individual's digitized or other electronic signature. Safe Harbor: Notification is not required when data has been secured by encryption or by any other method or technology that renders the electronic files, media, or data bases unreadable or unusable.	

DATA BREACH NOTIFICATION STATUTES

State	Statute(s)	Summary	Notes
OH	Ohio Rev. Code Ann. §§ 1347.12, 1349.19, 1349.191, 1349.192	Personal Information of Ohio residents, excluding publicly available information that is lawfully available to the general public from federal, state, or local government records or any of the following media that are widely distributed: 1) any news or editorial advertising statement published in any bona fide newspaper, journal, or magazine, or broadcast over radio or television; 2) any gathering or furnishing of information or news by any bona fide reporter, correspondent, or news bureau to news media; 3) any publication designed for and distributed to members of any bona fide associations or charitable or fraternal nonprofit corporation; Notification required only if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to the resident. Where notification is required, must be accomplished no later than 45 days following discovery unless disclosure impedes law enforcement investigation. Safe Harbor: If the data is encrypted, redacted, or altered by any method or technology in such a manner that the data elements are unreadable, notification is not required.	
OK	Okla. Stat. §§ 74-3113.1, 24-161 to -166	Notification required if the breach causes, or the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of this state. Safe Harbor: Notification is not required for encrypted or redacted information unless the encrypted information is accessed and acquired in an unencrypted form or if the security breach involves a person with access to the encryption key and the individual or entity reasonably believes that such breach has caused or will cause identity theft or other fraud to any resident of this state.	

DATA BREACH NOTIFICATION STATUTES

State	Statute(s)	Summary	Notes
OR	Or. Rev. Stat. § 646A.600 to .628	A consumer's first name or first initial and last name in combination with any one or more of the following data elements when the data elements are not rendered unusable through encryption, redaction or other methods, or when the data elements are encrypted and the encryption key has also been acquired: (1) Social Security number; driver license number or state identification card number issued by the Department of Transportation; (2) passport number or other United States issued identification number; or (3) financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to a consumer's financial account. For a person that owns the data, notification is not required if, after an appropriate investigation or after consultation with relevant federal, state or local agencies responsible for law enforcement, the person determines that no reasonable likelihood of harm to the consumers whose personal information has been acquired has resulted or will result from the breach. Such a determination must be documented in writing and the documentation must be maintained for five years. Safe Harbor: If data is encrypted or redacted, notice is not required.	Oregon provides for a private right of action. Compensation can be ordered by the state upon a finding that enforcement of the rights of consumers by private civil action would be so burdensome or expensive as to be impractical.
PA	73 Pa. Cons. Stat. § 2301 *et seq.*	PI of Pennsylvania residents. Notification required only if the access and acquisition materially compromises the security or confidentiality of personal information. Safe Harbor: Notification is not required when encrypted or redacted information is accessed and acquired. Notice is required, however, if encrypted information is accessed and acquired in an unencrypted form, if the security breach is linked to a breach of the security of the encryption or if the security breach involves a person with access to the encryption key.	
RI	R.I. Gen. Laws § 11-49.2-1 *et seq.*	PI of Rhode Island residents. Notification required if the breach poses a significant risk of identity theft following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Notification of a breach is not required if, after an appropriate investigation or after consultation with relevant federal, state, or local law enforcement agencies, a determination is made that the breach has not and will not likely result in a significant risk of identity theft to the individuals whose personal information has been acquired. Safe Harbor: If the information is encrypted, notice is not required.	

DATA BREACH NOTIFICATION STATUTES

State	Statute(s)	Summary	Notes
SC	S.C. Code Ann. § 39-1-90, 2013 H.B. 3248	PI of South Carolina residents, as well as other numbers or information which may be used to access a person's financial accounts or numbers or information issued by a governmental or regulatory entity that uniquely will identify an individual. Notification required when personal identifying information that was not rendered unusable through encryption, redaction, or other methods was, or is reasonably believed to have been, acquired by an unauthorized person, and the illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to the resident. Required reporting to South Carolina Department of Consumer Affairs for notices involving more than 1000 persons at one time. Safe Harbor: If data is rendered unusable through encryption, redaction, or other methods, notice to consumers is not required.	South Carolina provides for a private right of action. A resident who is injured may: institute a civil action to recover damages in case of a willful and knowing violation; institute a civil action to recover only actual damages resulting from a violation in case of a negligent violation; seek an injunction to enforce compliance; and recover attorney's fees and court costs, if successful
SD	None		
TN	Tenn. Code Ann. §§ 47-18-2101 *et. seq.*	PI of Tennessee residents. Notification required for unauthorized acquisition of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the information holder. Safe Harbor: Notification requirement only applies where personal information was unencrypted.	Tennessee provides for a private right of action. A violation under the data breach notification statute may also be a violation of the Tennessee Consumer Protection Act, which could give rise to a private cause of action.
TX	Tex. Bus. & Com. Code Ann. §§ 521.002, 521.053, Tex. Educ. Code Ann. § 37.007(b)(5)	The statute applies to"Sensitive personal information", which includes Personal Information of Texas residents. In addition: information that identifies an individual and relates to: 1) the physical or mental health or condition of the individual; 2) the provision of health care to the individual; or 3) payment for the provision of health care to the individual. Notification required to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Safe Harbor:"Sensitive personal information" only applies to data items that are not encrypted unless the encryption key is also breached.	A violation under the data breach notification statute may also be a violation of the Texas Deceptive Trade Practices Act, which could give rise to a private cause of action.
UT	Utah Code Ann. §§ 13-44-101 *et seq.*	PI of Utah residents. Notification required if misuse of personal information for identity theft or fraud purposes has occurred, or is reasonably likely to occur Safe Harbor: If the personal information is encrypted or protected by another method that renders the data unreadable or unusable, notice is not required.	

DATA BREACH NOTIFICATION STATUTES

State	Statute(s)	Summary	Notes
VT	Vt. Stat. Ann. tit. 9, § 2430, 2435	"Personally identifiable information" of Vermont residents, which means an individual's first name or first initial and last name in combination with any one or more of the following data elements when either the name or the data elements are not encrypted, redacted, or otherwise protected: (i) Social Security number; (ii) motor vehicle operator's license number or non-driver identification card number; (iii) financial account number or credit or debit card number, if circumstances exist in which the number could be used without additional identifying information, access codes, or passwords; (iv) account passwords or personal identification numbers or other access codes for a financial account. Notice of a security breach is not required if the data collector establishes that misuse of personal information is not reasonably possible and the data collector provides notice of the determination and a detailed explanation for said determination to the Vermont attorney general or to the department of banking, insurance, securities, and health care administration. If the data collector later gathers facts to indicate that the misuse of personal information is reasonably possible, then notice is required. Notification of breach where required shall be accomplished no later than 45 days Required reporting to Vermont Attorney General. Safe Harbor: If personal information is encrypted, redacted, or protected by another method that renders them unreadable or unusable, notice is not reuiqred.	
VA	Va. Code Ann. § 18.2-186.6, § 32.1-127.1:05	PI of Virginia residents, as well as medical information, including treatment, policy number or claims information. Notification required if the entity reasonably believes that such a breach has caused or will cause identity theft or other fraud to any resident of Virginia. For medical information, notice required if the medical information was accessed and acquired by an unauthorized person or the entity reasonably believes the medical information was accessed and acquired by an unauthorized person. Required reporting to Virginia Attorney General and Virginia Commissioner of Health for medical information breaches. Safe Harbor: The unauthorized acquisition of encrypted or redacted data, without access to the encryption key, does not trigger the notice requirement under this statute.	Though generally enforced by the Attorney General, nothing in the data breach notification statute precludes recovery of economic damages.

DATA BREACH NOTIFICATION STATUTES

State	Statute(s)	Summary	Notes
WA	Wash. Rev. Code § 19.255.010, 42.56.590	PI of Washington residents. A person, business, or agency shall not be required to disclose a technical breach of the security system that does not seem reasonably likely to subject customers to a risk of criminal activity. Safe Harbor: If both an individual's first name or first initial and last name and accompanying data element (i.e. social security number) are encrypted, notice is not required.	Washington provides for a private right of action. Any customer injured by a violation may institute a civil action to recover damages.
WV	W. Va. Code §§ 46A-2A-101 *et seq.*	PI of West Virginia residents. Notification required only if the individual or entity reasonably believes the breach has caused or will cause identity theft or other fraud to any resident of this State. Safe Harbor: If encrypted or redacted information is accessed and acquired and the person does not have access to the encryption key, notice is not required.	
WI	Wis. Stat. § 134.98	An individual's last name and the individual's first name or first initial, in combination with and linked to any of the following elements, if the element is not publicly available information and is not encrypted, redacted, or altered in a manner that renders the element unreadable: (1) the individual's Social Security number; (2) the individual's driver's license number or state identification number; (3) the number of the individual's financial account number, including a credit or debit card account number, or any security code, access code, or password that would permit access to the individual's financial account; (4) DNA profile; (5) the individual's unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation. This statute does not define a"breach of security", and its definition of"personal information" is not restricted to computerized information alone. Notification is not required if the acquisition of personal information does not create a material risk of identity theft or fraud to the subject of the personal information. Where notification of breach is required, not later than 45 days after the discovery of the breach. Safe Harbor: If one of the data elements linked to an individual's name is encrypted, redacted, or altered in a manner that renders the element unreadable, it is not considered personal information, meaning no notice is required.	Not limited to electronic records.

State	Statute(s)	Summary	Notes
WY	Wyo. Stat. Ann. § 40-12-501 *et seq.*	"Personal identifying information", which includes the first name or first initial and last name of a person in combination with one or more of the following data elements when either the name or the data elements are not redacted: (A) Social Security number; (B) driver's license number or Wyoming identification card number; (C) account number, credit card number or debit card number in combination with any security code, access code or password that would allow access to a financial account of the person; (D) tribal identification card; or (E) federal or state government issued identification card. Notification is required when unauthorized acquisition of computerized data materially compromises the security, confidentiality or integrity of personal identifying information maintained by a person or business and causes or is reasonably believed to cause loss or injury to a resident of this state. Residents must be notified of a breach of the security of the system when, after a good faith, reasonable, and prompt investigation, the individual or commercial entity determines that the misuse of personal identifying information about the residents has occurred or is reasonably likely to occur. Safe Harbor: both an individual's first name or first initial and last name and combined data element (i.e. social security number) are redacted, the data is not considered personal identifying information, and notice is not required.	
D.C.	D.C. Code § 28- 3851 *et seq.*	A person's first name or first initial and last name, or phone number, or address, in combination with one of the following: (1) Social Security number; (2) driver's license number or District of Columbia Identification Card number (3) credit card number or debit card number; or any other number or code or combination of numbers or codes, such as account number, security code, access code, or password, that allows access to or use of an individual's financial or credit account. Safe Harbor: The acquisition of data that has been rendered secure, so as to be unusable by an unauthorized third party is not considered a breach of the security system.	District of Columbia provides for a private right of action. A resident, may recover actual damages, the costs of the action, and reasonable attorney's fees. Actual damages shall not include pain and suffering.

DATA BREACH NOTIFICATION STATUTES

State	Statute(s)	Summary	Notes
Puerto Rico	P.R. Laws Ann. tit. 10, §§ 4051 *et seq.*	At least the name or first initial and the surname of a person, together with any of the following data so that an association may be established between certain information with another and in which the information is legible enough so that in order to access it there is no need to use a special cryptographic code: (1) Social Security number; (2) driver's license number, voter's identification or other official identification; (3) bank or financial account numbers of any type with or without passwords or access code that may have been assigned; (4) names of users and passwords or access codes to public or private information systems; (5) medical information; (6) tax information; (7) and work-related evaluations. "Violation of the system's security" means any situation in which it is detected that access has been permitted to unauthorized persons or entities to the data files so that the security, confidentiality or integrity of the information in the data bank has been compromised; or when normally authorized persons or entities have had access and it is known or there is reasonable suspicion that they have violated the professional confidentiality or obtained authorization under false representation with the intention of making illegal use of the information. This includes both access to the data banks through the system and physical access to the recording media that contain the same and any removal or undue retrieval of said recordings. Required reporting to Puerto Rico Department of Consumer Affairs. Safe Harbor: This statute is triggered only when unencrypted information or information not protected by a cryptographic code is disclosed.	Consumers may bring actions apart from the statute.
V.I.	V.I. Code Ann. tit. 14, Ch. 110, Sub. Ch. I §§ 2208-2209	PI of Virgin Island residents that was, or is reasonably believed to have been, acquired by an unauthorized person PI defined as: an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social Security number. (2) Driver's license number. (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.Safe Harbor: Statute applies only where personal information was unencrypted.	Any customer injured by a violation may commence a civil action to recover damages.

DATA DESTRUCTION LAWS: A STATE BY STATE SURVEY

State	Statute(s)	Summary	Notes
AL	None		
AK	Alaska S at. § 45.48.500	"When disposing of records that contain personal information, a business and a governmental agency shall take all reasonable measures necessary to protect against unauthorized access to or use of the records."	Business and Government application.
AZ	Ariz. Rev. Stat. § 44-7601	"An entity shall not knowingly discard or dispose of records or documents without redacting the information or destroying the records or documents if the records or documents contain an individual's first and last name or first initial and last name in combination with" other personal information	Business and Government application.
AR	Ark. Code Ann. § 4-110-104	"A person or business shall take all reasonable steps to destroy or arrange for the destruction of a customer's records within its custody or control containing personal information that is no longer to be retained by the person or business by shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means."	Business and Government application.
CA	Cal. Civ. Code 1798.81	"A business shall take all reasonable steps to dispose, or arrange for the disposal, of customer records" that contain"personal information when the records are no longer to be retained by the business by (a) shredding, (b) erasing, or (c) otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means."	Business only application. Not to government.
CO	Colo. Rev. Stat. § 6-1-713	"Each public and private entity in the state that uses documents during the course of business that contain personal identifying information shall develop a policy for the destruction or proper disposal of paper documents containing personal identifying information."	Business and Government application.
CT	Conn. Gen. Stat. § 42-471	"Any person in possession of personal information of another person shall safeguard the data, computer files and documents containing the information from misuse by third parties, and shall destroy, erase or make unreadable such data, computer files and documents prior to disposal."	Business only application. Not to government.
DE	Del. Code Ann. tit. 6, § 5002C	"In the event that a commercial entity seeks permanently to dispose of records containing consumers' personal identifying information within its custody or control, such commercial entity shall take reasonable steps to destroy or arrange for the destruction of each such record by shredding, erasing, or otherwise destroying or modifying the personal identifying information in those records to make it unreadable or indecipherable."	Business only application. Not to government.

DATA DESTRUCTION LAWS

State	Statute(s)	Summary	Notes
FL	Fla. Stat. § 501.171	"Each covered entity or third-party agent shall take all reasonable measures to dispose, or arrange for the disposal, of customer records containing personal information within its custody or control when the records are no longer to be retained. Such disposal shall involve shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means."	Business and Government application.
GA	Ga. Code Ann. § 10-15-2	"A business may not discard a record containing personal information unless it: (1) Shreds the customer´s record before discarding the record; (2) Erases the personal information contained in the customer´s record before discarding the record; (3) Modifies the customer´s record to make the personal information unreadable before discarding the record; or (4) Takes actions that it reasonably believes will ensure that no unauthorized person will have access to the personal information contained in the customer´s record for the period between the record´s disposal and the record´s destruction."	Business only application. Not to government.
HI	Haw. Rev. Stat. § 487R-2	"(a) Any business or government agency that conducts business in Hawaii and any business or government agency that maintains or otherwise possesses personal information of a resident of Hawaii shall take reasonable measures to protect against unauthorized access to or use of the information in connection with or after its disposal. (b) The reasonable measures shall include: (1) Implementing and monitoring compliance with policies and procedures that require the burning, pulverizing, recycling, or shredding of papers containing personal information so that information cannot be practicably read or reconstructed; (2) Implementing and monitoring compliance with policies and procedures that require the destruction or erasure of electronic media and other nonpaper media containing personal information so that the information cannot practicably be read or reconstructed; and (3) Describing procedures relating to the adequate destruction or proper disposal of personal records as official policy in the writings of the business entity."	Business and Government application.
ID	None		

DATA DESTRUCTION LAWS

State	Statute(s)	Summary	Notes
IL	815 Ill. Comp. Stat. 530/30 815 Ill. Comp. Stat. 530/40	Sec. 30:"Safe disposal of information. Any State agency that collects personal data that is no longer needed or stored at the agency shall dispose of the personal data or written material it has collected in such a manner as to ensure the security and confidentiality of the material." "A person must dispose of the materials containing personal information in a manner that renders the personal information unreadable, unusable, and undecipherable. Proper disposal methods include, but are not limited to, the following: (1) Paper documents containing personal information may be either redacted, burned, pulverized, or shredded so that personal information cannot practicably be read or reconstructed. (2) Electronic media and other non-paper media containing personal information may be destroyed or erased so that personal information cannot practicably be read or reconstructed."	Business and Government application.
IN	Ind. Code § 24-4-14-8	"A person who disposes of the unencrypted, unredacted personal information of a customer without shredding, incinerating, mutilating, erasing, or otherwise rendering the information illegible or unusable commits a Class C infraction. However, the offense is a Class A infraction if: (1) the person violates this section by disposing of the unencrypted, unredacted personal information of more than one hundred (100) customers; or(2) the person has a prior unrelated judgment for a violation of this section."	Business only application. Not to government.
IA	None		
KS	Kan. Stat. Ann. § 50–7a03	"Unless otherwise required by federal law or regulation, a person or business shall take reasonable steps to destroy or arrange for the destruction of a customer's records within its custody or control containing personal information which is no longer to be retained by the person or business by shredding, erasing or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means."	Business and Government application.
KY	Ky. Rev. Stat. Ann. § 365.725	"When a business disposes of, other than by storage, any customer's records that are not required to be retained, the business shall take reasonable steps to destroy, or arrange for the destruction of, that portion of the records containing personally identifiable information by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or indecipherable through any means."	Business only application. Not to government.
LA	None		
ME	None		

DATA DESTRUCTION LAWS

State	Statute(s)	Summary	Notes
MD	Md. Code Ann., Com. Law § 14-3503, Md. Code Ann., State Gov't §§ 10-1301 to 1303	To protect personal information from unauthorized access, use, modification, or disclosure, a business that owns or licenses personal information of an individual residing in the State shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information owned or licensed and the nature and size of the business and its operations.	Business and Government application.
MA	Mass. Gen. Laws ch. —, § § 93I	Requires that paper records set for destruction be”either redacted, burned, pulverized or shredded.“ Electronic media”shall be destroyed or erased so that personal information cannot practicably be read or reconstructed.”	Business and Government application.
MI	Mich. Comp. Laws § 445.72a	“A person or agency that maintains a database that includes personal information regarding multiple individuals shall destroy any data that contain personal information concerning an individual when that data is removed from the database and the person or agency is not retaining the data elsewhere for another purpose not prohibited by state or federal law.” “A person or agency is considered to be in compliance with this section if the person or agency is subject to federal law concerning the disposal of records containing personal identifying information and the person or agency is in compliance with that federal law.”	Business and Government application.
MN	None		
MS	None		
MO	None.		Business only application. Not to government.
MT	Mont. Code Ann. § 30-14-1703	“A business shall take all reasonable steps to destroy or arrange for the destruction of a customer's records within its custody or control containing personal information that is no longer necessary to be retained by the business by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or undecipherable.”	Business only application. Not to government.
NE	None		

DATA DESTRUCTION LAWS

State	Statute(s)	Summary	Notes
NV	Nev. Rev. Stat. § 603A.200	"A business that maintains records which contain personal information concerning the customers of the business shall take reasonable measures to ensure the destruction of those records when the business decides that it will no longer maintain the records .... 'Reasonable measures to ensure the destruction' means any method that modifies the records containing the personal information in such a way as to render the personal information contained in the records unreadable or undecipherable, including, without limitation: (1) Shredding of the record containing the personal information; or (2) Erasing of the personal information from the records.	Business only application. Not to government.
NH	None		
NJ	N.J. Stat. Ann. § C.56:8-162	"A business or public entity shall destroy, or arrange for the destruction of, a customer's records within its custody or control containing personal information, which is no longer to be retained by the business or public entity, by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable, undecipherable or non-reconstructable through generally available means."	Business and Government application.
NM	None		
NY	N.Y. Gen Bus § 399-h	"Disposal of records containing personal identifying information. No person, business, firm, partnership, association, or corporation, not including the state or its political subdivisions, shall dispose of a record containing personal identifying information unless the person, business, firm, partnership, association, or corporation, or other person under contract with the business, firm, partnership, association, or corporation does any of the following: a. shreds the record before the disposal of the record; or b. destroys the personal identifying information contained in the record; or c. modifies the record to make the personal identifying information unreadable; or d. takes actions consistent with commonly accepted industry practices that it reasonably believes will ensure that no unauthorized person will have access to the personal identifying information contained in the record."	Business only application. Not to government.

DATA DESTRUCTION LAWS

State	Statute(s)	Summary	Notes
NC	N.C. Gen. Stat. § 75-64	"Any business that conducts business in North Carolina and any business that maintains or otherwise possesses personal information of a resident of North Carolina must take reasonable measures to protect against unauthorized access to or use of the information in connection with or after its disposal. (b) The reasonable measures must include: (1) Implementing and monitoring compliance with policies and procedures that require the burning, pulverizing, or shredding of papers containing personal information so that information cannot be practicably read or reconstructed. (2) Implementing and monitoring compliance with policies and procedures that require the destruction or erasure of electronic media and other nonpaper media containing personal information so that the information cannot practicably be read or reconstructed."	Business only application. Not to government.
ND	None		
OH	None		
OK	None		
OR	Or. Rev. Stat. § 646A.622	"Disposes of personal information after it is no longer needed for business purposes or as required by local, state or federal law by burning, pulverizing, shredding or modifying a physical record and by destroying or erasing electronic media so that the information cannot be read or reconstructed."	Business and Government application.
PA	None		
RI	R.I. Gen. Laws § 6-52-2	"A business shall take reasonable steps to destroy or arrange for the destruction of a customer's personal information within its custody and control that is no longer to be retained by the business by shredding, erasing, or otherwise destroying and/or modifying the personal information in those records to make it unreadable or indecipherable through any means for the purpose of: (1) Ensuring the security and confidentiality of customer personal information; (2) Protecting against any reasonably foreseeable threats or hazards to the security or integrity of customer personal information; and (3) Protecting against unauthorized access to or use of customer personal information that could result in substantial harm or inconvenience to any customer."	Business only application. Not to government.
SC	S.C. Code Ann. § 37-20-190; S.C. Code Ann. 30-2-310	"When a business [or public body] disposes of a business record that contains personal identifying information of a customer of a business, the business shall modify, by shredding, erasing, or other means, the personal identifying information to make it unreadable or undecipherable."	Business and Government application.

DATA DESTRUCTION LAWS

State	Statute(s)	Summary	Notes
SD	None		
TN	Tenn. Code Ann. § 39-14-150(g)	"If a private entity or business maintains a record that contains . . . personal identifying information . . . concerning one of its customers, and the entity, by law, practice or policy discards such records after a specified period of time, any record containing the personal identifying information shall not be discarded unless the business: (A) Shreds or burns the customer's record before discarding the record; (B) Erases the personal identifying information contained in the customer's record before discarding the record; (C) Modifies the customer's record to make the personal identifying information unreadable before discarding the record; or (D) Takes action to destroy the customer's personal identifying information in a manner that it reasonably believes will ensure that no unauthorized persons have access to the personal identifying information contained in the customer's record for the period of time between the record's disposal and the record's destruction."	Business only application. Not to government.
TX	Tex. Bus. & Com. Code Ann. § 72.004, § 521.052	"When a business disposes of a business record that contains personal identifying information of a customer of the business, the business shall modify, by shredding, erasing, or other means, the personal identifying information so as to make the information unreadable or undecipherable." "A business shall destroy or arrange for the destruction of customer records containing sensitive personal information within the business's custody or control that are not to be retained by the business by: (1) shredding; (2) erasing; or (3) otherwise modifying the sensitive personal information in the records to make the information unreadable or indecipherable through any means."	Business only application. Not to government.
UT	Utah Code Ann. § 13-44-201	"Any person who conducts business in the state and maintains personal information shall implement and maintain reasonable procedures to: (a) prevent unlawful use or disclosure of personal information collected or maintained in the regular course of business; and (b) destroy, or arrange for the destruction of, records containing personal information that are not to be retained by the person. (2) The destruction of records under Subsection (1)(b) shall be by: (a) shredding; (b) erasing; or (c) otherwise modifying the personal information to make the information indecipherable."	Business only application. Not to government.

DATA DESTRUCTION LAWS

State	Statute(s)	Summary	Notes
VT	Vt. Stat. Ann. tit. 9, § 2445	"A business shall take all reasonable steps to destroy or arrange for the destruction of a customer's records within its custody or control containing personal information which is no longer to be retained by the business by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or indecipherable through any means for the purpose of: (1) ensuring the security and confidentiality of customer personal information; (2) protecting against any anticipated threats or hazards to the security or integrity of customer personal information; and (3) protecting against unauthorized access to or use of customer personal information that could result in substantial harm or inconvenience to any customer."	Business only application. Not to government.
VA	None		
WA	Wash. Rev. Code § 19.215.020	"An entity must take all reasonable steps to destroy, or arrange for the destruction of, personal financial and health information and personal identification numbers issued by government entities in an individual's records within its custody or control when the entity is disposing of records that it will no longer retain."	Business and Government application.
WV	None		
WI	Wis. Stat. § 134.97	"A financial institution, medical business or tax preparation business may not dispose of a record containing personal information unless the financial institution, medical business, tax preparation business or other person under contract with the financial institution, medical business or tax preparation business does any of the following: (a) Shreds the record before the disposal of the record. (b) Erases the personal information contained in the record before the disposal of the record. (c) Modifies the record to make the personal information unreadable before the disposal of the record. (d) Takes actions that it reasonably believes will ensure that no unauthorized person will have access to the personal information contained in the record for the period between the record's disposal and the record's destruction."	Business only application. Not to government.
WY	None		

OFFICE FOR CIVIL RIGHTS (OCR) ENFORCEMENT ACTIVITY & AUDITS UNDER HIPAA/HITECH

Resolution Agreements and Civil Money Penalties

A resolution agreement is a contract signed by HHS and a covered entity in which the covered entity agrees to perform certain obligations (e.g., staff training) and make reports to HHS, generally for a period of three years. During the period, HHS monitors the covered entity's compliance with its obligations. A resolution agreement likely would include the payment of a resolution amount. These agreements are reserved to settle investigations with more serious outcomes. When HHS has not been able to reach a satisfactory resolution through the covered entity's demonstrated compliance or corrective action through other informal means, civil money penalties (CMPs) may be imposed for noncompliance against a covered entity. To date, HHS has entered into 21 resolution agreements and issued CMPs to one covered entity.

Since 2013, the following Resolution Agreements and CMPs have been enforced:

1. $800,000 HIPAA Settlement in Medical Records Dumping Case

As reported on June 23, 2014, Parkview Health System, Inc. (Parkview) agreed to settle potential violations of the HIPAA Privacy Rule with the OCR. Parkview will pay $800,000 and adopt a corrective action plan to correct deficiencies in its HIPAA compliance program. OCR opened an investigation after receiving a complaint from a retiring physician alleging that Parkview had violated the HIPAA Privacy Rule. In September 2008, Parkview took custody of medical records pertaining to approximately 5,000 to 8,000 patients while assisting the retiring physician to transition her patients to new providers, and while considering the possibility of purchasing some of the physician's practice. On June 4, 2009, Parkview employees, with notice that the physician was not at home, left 71 cardboard boxes of these medical records unattended and accessible to unauthorized persons on the driveway of the physician's home, within 20 feet of the public road and a short distance away from a heavily trafficked public shopping venue.As a covered entity under the HIPAA Privacy Rule, Parkview must appropriately and reasonably safeguard all protected health information in its possession, from the time it is acquired through its disposition."All too often we receive complaints of records being discarded or transferred in a manner that puts patient information at risk," said Christina Heide, acting deputy director of health information privacy at OCR.

2. Data Breach Results in $4.8 Million HIPAA Settlements

As reported on May 7, 2014, two health care organizations agreed to settle charges that they potentially violated HIPAA by failing to secure thousands of patients' electronic protected health information (ePHI) held on their network. New York and Presbyterian Hospital (NYP) agreed to pay OCR $3,300,000 to settle potential violations of the HIPAA Privacy and Security Rules, and to adopt a corrective action plan to evidence their remediation of these findings. NYP and CU are separate covered entities that participate in a joint arrangement in which CU faculty members serve as attending physicians at NYP. The entities generally refer to their affiliation as"New York Presbyterian Hospital/Columbia University Medical Center." NYP and CU operate a shared data network and a shared network firewall that is administered by employees of both entities. The shared network links to NYP patient information systems containing ePHI.

The investigation revealed that the breach was caused when a physician employed by CU who developed applications for both NYP and CU attempted to deactivate a personally-owned computer server on the network containing NYP patient ePHI. Because of a lack of technical safeguards, deactivation of the server resulted in ePHI being accessible on internet search engines. The entities learned of the breach after receiving a complaint by an individual who found the ePHI of the individual's deceased partner, a former patient of NYP, on the internet.In addition to the impermissible disclosure of ePHI on the internet, OCR's investigation found that neither NYP nor CU made efforts prior to the breach to assure that the server was secure and that it contained appropriate software protections. Moreover, OCR determined that neither entity had conducted an accurate and thorough risk analysis that identified all systems that access NYP ePHI. As a result, neither entity had developed an adequate risk management plan that addressed the potential threats and hazards to the security of ePHI. Lastly, NYP failed to implement appropriate policies and procedures for authorizing access to its databases and failed to comply with its own policies on information access management.

3. Concentra Settles HIPAA Case for $1,725,220

As reported on April 22, 2014, Concentra Health Services (Concentra) agreed to pay OCR $1,725,220 to settle potential violations of HIPAA Privacy and Security Rules, and to adopt a corrective action plan to evidence their remediation of these findings. OCR opened a compliance review of Concentra upon receiving a breach report that an unencrypted laptop was stolen from one of its facilities. OCR's investigation revealed that Concentra had previously recognized in multiple risk analyses that a lack of encryption on its laptops, desktop computers, medical equipment, tablets and other devices containing electronic protected health information (ePHI) was a critical risk. While steps were taken to begin encryption, Concentra's efforts were incomplete and inconsistent over time leaving patient PHI vulnerable throughout the organization. OCR's investigation further found Concentra had insufficient security management processes in place to safeguard patient information.

4. QCA Settles HIPAA Case for $250,000

As reported on April 22, 2014, QCA Health Plan, Inc., of Arkansas, agreed to settle potential violations of the HIPAA Privacy and Security Rules, agreeing to pay a $250,000 monetary settlement and to correct deficiencies in its HIPAA compliance program. OCR received a breach notice in February 2012 from QCA reporting that an unencrypted laptop computer containing the ePHI of 148 individuals was stolen from a workforce member's car. While QCA encrypted their devices following discovery of the breach, OCR's investigation revealed that QCA failed to comply with multiple requirements of the HIPAA Privacy and Security Rules, beginning from the compliance date of the Security Rule in April 2005 and ending in June 2012. QCA agreed to a $250,000 monetary settlement and is required to provide HHS with an updated risk analysis and corresponding risk management plan that includes specific security measures to reduce the risks to and vulnerabilities of its ePHI. QCA is also required to retrain its workforce and document its ongoing compliance efforts.

5. County Government Settles Potential HIPAA Violations

As reported on March 7, 2014, Skagit County, Washington, agreed to settle potential violations of the HIPAA Privacy, Security, and Breach Notification Rules by paying a $215,000 monetary settlement and agreeing to work closely with HHS to correct deficiencies in its HIPAA compliance program. OCR opened an investigation of Skagit County upon receiving a breach report that money receipts with electronic protected health information (ePHI) of seven individuals were accessed by unknown parties after the ePHI had been inadvertently moved to a publicly accessible server. OCR's investigation revealed a broader exposure of protected health information involved in the incident, which included the ePHI of 1,581 individuals. Many of the accessible files involved sensitive information, including protected health information concerning the testing and treatment of infectious diseases. OCR's investigation further uncovered general and widespread non-compliance by Skagit County with the HIPAA Privacy, Security, and Breach Notification Rules.

6. Resolution Agreement with Adult & Pediatric Dermatology, P.C. of Massachusetts

Reported on December 20, 2013, Adult & Pediatric Dermatology, P.C., of Concord, Massachusetts (APDerm) agreed to settle potential violations of the HIPAA Privacy, Security and Breach Notification Rules with HHS, including a $150,000 payment. APDerm agreed also to implement a corrective action plan to correct deficiencies in its HIPAA compliance program. This case marks the first settlement with a covered entity for not having policies and procedures in place to address the breach notification provisions of the HITECH Act.

OCR opened an investigation of APDerm upon receiving a report that an unencrypted thumb drive containing the electronic protected health information (ePHI) of approximately 2,200 individuals was stolen from a vehicle of one its staff members. The thumb drive was never recovered. The investigation revealed that APDerm had not conducted an accurate and thorough analysis of the potential risks and vulnerabilities to the confidentiality of ePHI as part of its security management process. Further, APDerm did not fully comply with requirements of the Breach Notification Rule to have in place written policies and procedures and to train workforce members.

7. HHS Settles with Health Plan in Photocopier Breach Case

Reported on August 14, 2013, Affinity Health Plan, Inc. paid $1,215,780 to settle potential violations of the HIPAA Privacy and Security Rules. OCR's investigation indicated that Affinity impermissibly disclosed the protected health information of up to 344,579 individuals when it returned multiple photocopiers to a leasing agent without erasing the data contained on the copier hard drives. In addition, the investigation revealed that Affinity failed to incorporate the electronic protected health information stored in copier's hard drives in its analysis of risks and vulnerabilities as required by the Security Rule, and failed to implement policies and procedures when returning the hard drives to its leasing agents.

8. WellPoint Settles HIPAA Security Case for $1,700,000

July 11, 2013. This case sends an important message to HIPAA-covered entities to take caution when implementing changes to their information systems, especially when those changes involve updates to Web-based applications or portals that are used to provide access to consumers' health data using the Internet. As reported on July 11, 2013, OCR began its investigation following a breach report submitted by WellPoint as required by the HITECH Act.

The HITECH Breach Notification Rule requires HIPAA-covered entities to notify HHS of a breach of unsecured protected health information.

The report indicated that security weaknesses in an online application database left the electronic protected health information (ePHI) of 612,402 individuals accessible to unauthorized individuals over the Internet. OCR's investigation indicated that WellPoint did not implement appropriate administrative and technical safeguards as required under the HIPAA Security Rule.

The investigation indicated WellPoint did not:

- adequately implement policies and procedures for authorizing access to the on-line application database
- perform an appropriate technical evaluation in response to a software upgrade to its information systems
- have technical safeguards in place to verify the person or entity seeking access to electronic protected health information maintained in its application database.

As a result, beginning on Oct. 23, 2009, until Mar. 7, 2010, the investigation indicated that WellPoint impermissibly disclosed the ePHI of 612,402 individuals by allowing access to the ePHI of such individuals maintained in the application database. This data included names, dates of birth, addresses, Social Security numbers, telephone numbers and health information. Whether systems upgrades are conducted by covered entities or their business associates, HHS expects organizations to have in place reasonable and appropriate technical, administrative and physical safeguards to protect the confidentiality, integrity and availability of electronic protected health information – especially information that is accessible over the Internet. HHS points out that beginning Sept. 23, 2013, liability for many of HIPAA's requirements extend directly to business associates that receive or store protected health information, such as contractors and subcontractors.

9. Shasta Regional Medical Center Settles HIPAA Privacy Case for $275,000

Reported on June 13, 2013, SRMC has agreed to pay $275,000, to implement a comprehensive corrective action plan to update its policies and procedures on safeguarding PHI from impermissible uses and disclosures, and to train its workforce members. OCR's investigation indicated that SRMC failed to safeguard the patient's protected health information (PHI) from impermissible disclosure by intentionally disclosing PHI to multiple media outlets on at least three separate occasions, without a valid written authorization. OCR's review indicated that senior management at SRMC impermissibly shared details about the patient's medical condition, diagnosis and treatment in an email to the entire workforce. In addition, SRMC failed to sanction its workforce members for impermissibly disclosing the patient's records pursuant to its internal sanctions policy.

According to OCR Director Leon Rodriguez,"When senior level executives intentionally and repeatedly violate HIPAA by disclosing identifiable patient information, OCR will respond quickly and decisively to stop such behavior. Senior leadership helps define the culture of an organization and is responsible for knowing and complying with the HIPAA privacy and security requirements to ensure patients' rights are fully protected."

10. Idaho State University Settles HIPAA Security Case for $400,000

Reported on May 21, 2013,this settlement involved the breach of unsecured electronic protected health information (ePHI) of 17,500 individuals who were patients at an ISU clinic. The ePHI was unsecured for at least 10 months, due to the disabling of firewall protections at servers maintained by ISU. OCR's investigation indicated that ISU's risk analyses and assessments of its clinics were incomplete and inadequately identified potential risks or vulnerabilities. ISU also failed to assess the likelihood of potential risks occurring. OCR concluded that ISU did not apply proper security measures and policies to address risks to ePHI and did not have procedures for routine review of their information system in place, which could have detected the firewall breach much sooner.

According to OCR Director Leon Rodriguez,"Risk analysis, ongoing risk management, and routine information system reviews are the cornerstones of an effective HIPAA security compliance program. Proper security measures and policies help mitigate potential risk to patient information."

OCR'S HIPAA Audit Program

Background on the OCR Pilot Privacy, Security, and Breach Notification Audit Program

The use of health information technology continues to expand in health care. Although these new technologies provide many opportunities and benefits for consumers, they also pose new risks to consumer privacy. Because of these increased risks, the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) include national standards for the privacy of protected health information, the security of electronic protected health information, and breach notification to consumers. HITECH also requires HHS to perform periodic audits of covered entity and business associate compliance with the HIPAA Privacy, Security, and Breach Notification Rules. HHS Office for Civil Rights (OCR) enforces these rules, and in 2011, OCR established a pilot audit program to assess the controls and processes covered entities have implemented to comply with them. Through this program, OCR developed a protocol, or set of instructions, it then used to measure the efforts of covered entities.

The audit program began with an audit of 20 entities in 2011, with 95 more added in 2012. In the summer of 2012 the OCR published the audit protocols that OCR, through KPMG, is using to audit the healthcare industry. The audit program analyzes processes, controls, and policies of selected covered entities pursuant to the HITECH Act audit mandate. The audit protocol is organized around modules, representing separate elements of privacy, security, and breach notification. The combination of these multiple requirements may vary based on the type of covered entity selected for review. There are a total of 169 protocols- 78 for HIPAA security, 81 for HIPAA privacy and 10 for HIPAA breach. The protocols are published online at:

http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html.

OCR's HIPAA Audit Protocols

- The audit protocol covers Privacy Rule requirements for (1) notice of privacy practices for PHI, (2) rights to request privacy protection for PHI, (3) access of individuals to PHI, (4) administrative requirements, (5) uses and disclosures of PHI, (6) amendment of PHI, and (7) accounting of disclosures.
- The protocol covers Security Rule requirements for administrative, physical, and technical safeguards
- The protocol covers requirements for the Breach Notification Rule.

Consulting firm KPMG conducted the pilot audits and assessed compliance with the 169 requirements of the protocol. Now, OCR is learning which gaps in protecting health information cause the most breaches, and has stated an intention to focus on those areas that are causing the most breaches. One big target area, if not the biggest target, is an organization's risk analysis. Covered entities audited in the pilot program often had conducted a shallow analysis that wasn't updated as events warranted, such as new business strategies or new information systems, or no risk analysis of their internal operations at all. Organizations must have a complete and accurate risk analysis to be compliant.

Another top area of focus is the use of data encryption. Under the security rule, encryption is an"addressable" requirement. An organization deciding not to encrypt must, through documentation, justify its decision and select a reasonable alternative. What is being found in the pilot program is that an organization either implemented encryption or did nothing at all in justifying and documenting reasonable alternatives. According to OCR's senior advisor for health information privacy, Linda Sanches, her best piece of advice about preparing for audits is to actually be in compliance and to conduct comprehensive risk analysis. Sanches acknowledged that it requires heavy-lifting to perform such an analysis but that it's better to have one in hand than scramble and pull it together come audit time.

OCR originally planned to conduct 400 desk audits and"a large number of on-site audits," in the coming year, but are now said they're looking at"fewer than 200 desk audits" and they haven't confirmed a specific number of on-site audits for covered entities, or the number of Business Associate audits that will follow those.

Updated November 25, 2014.

The above information was compiled from publicly available data by
Linda Hunt Mullany, RN, JD, partner, Health Care Practice Group, Gordon Rees Scully Mansukhani LLP.