Comparison of Insurance Data Security Model Law (proposed v. 3) "Data Breach" Definition / Harm Trigger with HIPAA and California Laws

Model - "Data Breach" Definition	HIPAA	California
Section 3. Definitions C. "Data breach" means the unauthorized acquisition, release or use of personal information that is reasonably likely to result in harm or inconvenience to a Consumer. The term "data breach" does not include: (1) the unauthorized acquisition, release or use of encrypted personal information if the encryption, process or key is not also acquired, released or used without authorization. (2) good faith acquisition by an employee if not subject to further disclosure; or (3) unauthorized disclosure to an employee of another licensee if no further disclosure.	**45 C.F.R. § 164.402** As used in this subpart, the following terms have the following meanings: Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information. (1) Breach excludes: (i) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part. (ii) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part. (iii) A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information. (2) Except as provided in paragraph (1) of this definition, an acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates	**Cal.Civ.Code § 1798.82(a)** A person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

Model - "Data Breach" Definition	HIPAA	California
	that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors: (i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification; (ii) The unauthorized person who used the protected health information or to whom the disclosure was made; (iii) Whether the protected health information was actually acquired or viewed; and (iv) The extent to which the risk to the protected health information has been mitigated. Unsecured protected health information means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111–5.	

