

Requester:	Eric Chenier
-------------------	---------------------

AGENCY BILL ANALYSIS - 2025 REGULAR SESSION

WITHIN 24 HOURS OF BILL POSTING, UPLOAD ANALYSIS TO

AgencyAnalysis.nmlegis.gov and email to billanalysis@dfa.nm.gov

(Analysis must be uploaded as a PDF)

SECTION I: GENERAL INFORMATION

{Indicate if analysis is on an original bill, amendment, substitute or a correction of a previous bill}

Date Prepared: 2/21/20 *Check all that apply:*
Bill Number: HB430 Original Correction
 Amendment Substitute

Sponsor: Rep. Sariñana **Agency Name and Code** HCA 630
Short Title: Health Data Privacy Act **Number:** _____
Person Writing Mark Reynolds
Phone: 505-531-7790 **Email** mark.reynolds@hca.n

SECTION II: FISCAL IMPACT

APPROPRIATION (dollars in thousands)

Appropriation		Recurring or Nonrecurring	Fund Affected
FY25	FY26		
\$0.0	\$0.0	NA	

(Parenthesis () indicate expenditure decreases)

REVENUE (dollars in thousands)

Estimated Revenue			Recurring or Nonrecurring	Fund Affected
FY25	FY26	FY27		
\$0.0	\$0.0	\$0.0		

(Parenthesis () indicate revenue decreases)

ESTIMATED ADDITIONAL OPERATING BUDGET IMPACT (dollars in thousands)

	FY25	FY26	FY27	3 Year Total Cost	Recurring or Nonrecurring	Fund Affected
Total	\$0.0	\$0.0	\$0.0	\$0.0	NA	

(Parenthesis () Indicate Expenditure Decreases)

Duplicates/Conflicts with/Companion to/Relates to:
Duplicates/Relates to Appropriation in the General Appropriation Act

SECTION III: NARRATIVE

BILL SUMMARY

Synopsis:

HB430 would enact restrictions on the use and disclosure of personally identifiable consumer data related to health and wellness. “Regulated entities” and “service providers” are prohibited from “processing” (defined broadly as collecting, selling, sharing, and nearly every use) consumers’ health information without first obtaining consent through a clear and easily understood opt-in process.

“Regulated health information” is defined broadly as nearly everything connected to health and wellness, including the geographic location of health-related activities. Before any processing of health data can occur, prior authorization must be obtained from consumers, with consent obtained by clearly explaining the nature of that consent.

Requirements of consent include informing consumers about the types of information collected, the nature of any processing activity, the purpose of processing, the entities with whom the information will be shared, how consent can be revoked, and that use of the product or service will be unaffected by the failure to provide authorization. Consent must be obtained from consumers through a process separate from any other transaction. Processing of health information would generally only be permitted if it is strictly necessary to the provision or maintenance of a service or product.

Rights granted to individuals under the Act cannot be waived. Retaliation for individuals exercising their rights is prohibited. Provides for civil monetary penalties and a private cause of action for violation of the Act. The Attorney General and district attorneys may also enforce the Act.

FISCAL IMPLICATIONS

No fiscal impact to HCA.

SIGNIFICANT ISSUES

HB430 would extend protections over personal health information (PHI) beyond the scope of federal HIPAA laws. Currently, disclosures of PHI are permitted when health data is collected or maintained by an entity not covered by HIPAA. HIPAA only applies to “covered entities” and their “business associates.” A covered entity is a healthcare provider, health plan, or healthcare clearinghouse. A business associate is an entity that provides products or services to a covered entity that involves access to PHI.

Given the limitations of HIPAA, there are many entities that collect health information that are not subject to its provisions, such as health app companies, wearable devices such as fitness trackers and apps and devices that track heart patterns, menstrual cycles, respiratory conditions, sleep patterns and a myriad of other types of health data. These apps and devices collect a considerable amount of health-related information that would be subject to HIPAA rules if collected by a HIPAA covered entity. There have been unsuccessful attempts to address this privacy gap at the

federal level by expanding HIPAA to cover all health data regardless of the entity that collects the information. HB340 seeks to address the gap at the state level. At the time of this writing, three states (Washington, Nevada and Connecticut) have passed similar laws, and an act passed by the New York legislature in 2025 is awaiting the governor's signature.

Information processed by governmental entities is specifically excluded from the requirements of the Act. Therefore, HCA does not appear to be directly affected. However, HCA contracts with Medicaid managed care organizations, State of New Mexico health insurance carriers, and other health care entities that collect or maintain PHI. These are HIPAA covered entities but, because HB430 does not exempt HIPAA covered PHI or HIPAA covered entities, their obligations under the bill may be unclear. Presumably, they would be required to comply with HB340 to the extent they process health information outside of the HIPAA definition of PHI.

PERFORMANCE IMPLICATIONS

None

ADMINISTRATIVE IMPLICATIONS

HB430 states that nothing in the Health Data Privacy Act shall be interpreted or construed to apply to information processed by local, state or federal governments, or municipal corporations.

The bill does not require any changes to HCA IT systems. It should be noted, however, that the HCA is required to comply with the HIPAA security and privacy rules related to Protected Health Information (PHI) and Personally Identifiable Information (PII). This includes, but is not limited to encryption, access controls, automatic log-off, auditing and monitoring, data integrity controls, risk analysis, and physical security.

The public facing HCA Unified Portal (UP) is compliant with accessibility standards and does not process or retain geolocation information. The UP also already has privacy statements, obtains consent, and offers access for customers to their data. HCA already has data processing agreements in the form of Memoranda of Understanding (MOUs) with other agencies and entities.

CONFLICT, DUPLICATION, COMPANIONSHIP, RELATIONSHIP

None

TECHNICAL ISSUES

None

OTHER SUBSTANTIVE ISSUES

Although the bill introduces privacy protections, there could be potential impacts on innovation in the health technology sector. Strict compliance requirements could pose challenges for emerging health tech companies and consumer data-driven services. It is unclear if the bill balances between safeguarding privacy and fostering technological advancements that rely on health data to enhance services and improve health outcomes.

ALTERNATIVES

None

WHAT WILL BE THE CONSEQUENCES OF NOT ENACTING THIS BILL

Status quo

SUGGESTED AMENDMENTS:

To clarify the relationship between this bill and HIPAA, it is suggested that language be added, in Section 7, to make it clear that its provisions do not apply to:

“A covered entity or business associate and protected health information that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the united states department of health and human services, parts 160 and 164 of title 45 of the code of federal regulations, established pursuant to the health insurance portability and accountability act of 1996 (public law 104-191) and the health information technology for economic and clinical health act (public law 111-5).”