S. 3097, Health Information Privacy Reform Act

Section 1. Short Title.
This Act may be cited as the "Health Information Privacy Reform Act."

Section 2. Protections for Applicable Health Information.
This section would direct the Department of Health and Human Services (HHS), in consultation with the Federal Trade Commission (FTC), to establish privacy, security, and breach notification requirements for identifiable health information held by entities that generally are not covered by the Health Insurance Portability and Accountability Act (HIPAA), such as certain health applications, wearable-device platforms, and other consumer health technology companies. The requirements would include limits on uses and disclosures, individual rights, data-security standards, and civil penalties modeled on HIPAA.

Section 3. Rights and Requirements Regarding Access to Certain Protected Health Information.
This section would establish requirements when an individual directs a HIPAA covered entity or business associate to send the individual's protected health information to a regulated entity outside of HIPAA. It would permit certain fees and recipient-use conditions for these transfers and clarify when HIPAA's cost-based fee limitations apply.

Section 4. Confidentiality of Records.
This section would amend the Federal confidentiality statute for substance use disorder records, commonly known as Part 2, to generally apply HIPAA disclosure rules in place of the statute's separate consent provisions.

Section 5. NAS Study on Compensation to Patients for Sharing Identifiable Data for Research Purposes.
This section would direct the National Academies of Sciences, Engineering, and Medicine to conduct a study on the risks and benefits of compensating patients for sharing identifiable health data for research.

Section 6. Patient Notification Requirements Under the HIPAA Privacy Regulations.
This section would require regulated entities and service providers that receive protected health information through an individual's HIPAA right of access to notify the individual that the information will no longer be protected by HIPAA and explain how it may be redisclosed. It would also require the individual's authorization before the information may be sold to a third party.

Section 7. Minimum Necessary Guidance.
This section would direct HHS to issue guidance on applying HIPAA's minimum necessary standard to health data used for artificial intelligence and other machine-learning applications.

Section 8. De-Identified Information.
This section would direct HHS to establish unified national standards for de-identifying applicable health information.

Section 9. Preemption.
This section would apply HIPAA's existing Federal-state preemption framework to the requirements established under this Act, generally preserving State laws that provide more stringent privacy protections.