GOBIERNO DE PUERTO RICO

20ma. Asamblea Legislativa — 3 ra. Sesión Ordinaria

SENADO DE PUERTO RICO

P. del S. 1041

2 de febrero de 2026

Presentado por la señora *Soto Aguilú*

Referido a

LEY

Para establecer la "Ley para la Protección de Datos Personales en Aplicaciones de Salud y Servicios de Telemedicina"; definir términos relacionados con consentimientos explícitos y auditorías en el contexto de la telemedicina y telesalud; requerir la obtención de consentimientos explícitos para el procesamiento de datos personales de salud en aplicaciones y servicios de telemedicina; exigir auditorías periódicas anuales de sistemas de seguridad y privacidad por parte de proveedores; enmendar el Artículo 2 de la Ley Núm. 168-2018, según enmendada, conocida como la "Ley para Reglamentar la Práctica de la Telemedicina en Puerto Rico", a los fines de incorporar definiciones de "consentimiento explícito", "auditoría" y "datos personales de salud"; enmendar el Artículo 3 de la Ley Núm. 168-2018 para incluir requisitos de consentimiento y auditorías en los deberes de los proveedores; enmendar el Artículo 2 de la Ley Núm. 48-2020, conocida como la "Ley para Reglamentar la Práctica de la Telesalud y Ciberterapia en Puerto Rico", a los fines de incorporar las mismas definiciones; enmendar el Artículo 4 de la Ley Núm. 48-2020 para integrar obligaciones de consentimiento y auditorías; establecer sanciones por incumplimiento conforme a la Ley Núm. 111 de 2005; delegar fiscalización al Departamento de Salud sin impacto presupuestario adicional; y para otros fines relacionados.

EXPOSICIÓN DE MOTIVOS

En el contexto actual de avance tecnológico en Puerto Rico, la telemedicina y las aplicaciones de salud han transformado radicalmente la prestación de servicios médicos, facilitando el acceso remoto a consultas, monitoreo y tratamientos, y mejorando la

eficiencia operativa del sistema de salud. Esta evolución ha sido particularmente crucial en escenarios de emergencia, como la pandemia de COVID-19, donde la telesalud permitió mantener la continuidad de la atención médica sin exponer a pacientes y profesionales a riesgos innecesarios, y en regiones rurales o de difícil acceso geográfico, donde el acceso a especialistas es limitado.

Según datos del Departamento de Salud, durante la pandemia, el uso de plataformas de telemedicina aumentó en más del 500% en Puerto Rico, demostrando su potencial para reducir brechas en la cobertura sanitaria y promover modelos innovadores como el "Patient-Centered Medical Home" y "Hospital sin Paredes", que enfatizan la atención integrada y remota. Es preciso, destacar que la base legal para estos avances se encuentra en la Ley Núm. 168-2018, según enmendada, por la Ley Núm. 8-2025, conocida como la "Ley para el Uso de la Telemedicina y la Telesalud en Puerto Rico", que faculta a profesionales de la salud licenciados a ofrecer servicios remotos sin barreras administrativas adicionales, eliminando la necesidad de certificaciones especiales para la práctica de telemedicina, telesalud o ciberterapia, siempre que se mantenga una licencia vigente.

Complementariamente, la Ley Núm. 48-2020, conocida como la "Ley para Regular la Práctica de la Telesalud y Ciberterapia en Puerto Rico", define y regula la ciberterapia como la práctica a distancia de disciplinas como psicología, trabajo social y terapia ocupacional, extendiendo los beneficios de la salud digital a áreas de salud mental y rehabilitación. Estas leyes han impulsado la adopción de tecnologías como plataformas digitales para consultas en tiempo real, monitoreo remoto de pacientes crónicos y almacenamiento electrónico de historiales médicos, alineándose con estándares federales como HIPAA (Health Insurance Portability and Accountability Act), que protegen la portabilidad y responsabilidad en seguros de salud.

Sin embargo, este progreso tecnológico conlleva riesgos significativos para la privacidad y la seguridad de los datos personales de los pacientes, clasificados como información sensible bajo la Ley Núm. 111 de 2005, conocida como la "Ley de Información al Ciudadano sobre la Seguridad de Bancos de Información", que obliga a las entidades a

notificar brechas de seguridad que involucren datos como números de seguro social, licencias de conducir, información médica protegida por HIPAA, cuentas bancarias o datos biométricos. Estos datos de salud incluyen detalles íntimos como diagnósticos médicos, tratamientos farmacológicos, historiales clínicos, resultados de pruebas de laboratorio y datos genéticos o biométricos, cuya exposición no autorizada puede generar consecuencias graves, tales como discriminación laboral o social, fraudes financieros mediante el robo de identidad, estigmatización personal, o incluso riesgos para la seguridad física si se revelan datos sensibles sobre vulnerabilidades de salud.

En Puerto Rico, la Ley Núm. 111 de 2005 establece que cualquier entidad propietaria o custodia de bancos de información debe implementar medidas de seguridad razonables y notificar a los afectados en caso de brechas, con multas por incumplimiento, pero carece de disposiciones específicas para el ecosistema de salud digital en expansión. Recientes escándalos y brechas de seguridad han subrayado la urgencia de fortalecer estas protecciones. En nuestra Isla, incidentes como el ataque cibernético al Hospital Auxilio Mutuo en 2023, que potencialmente comprometió datos de pacientes hasta agosto de 2022.

Así también, se han reportaron alertas del FBI y el Departamento de Salud en 2024 sobre más de 40 hospitales locales afectados por intentos de hackeo mensuales, ilustran la vulnerabilidad del sector. Más recientemente, reportajes en el periódico, El Vocero en octubre de 2025 detallaron brechas en aplicaciones de telemedicina que expusieron datos de miles de pacientes, incluyendo historiales médicos y resultados de pruebas, generando interrupciones en servicios y pérdidas económicas estimadas en millones de dólares.

A nivel regional, América Latina ha visto un aumento alarmante de ciberataques en salud: en Argentina, un ciberataque en mayo de 2025 filtró más de 500,000 estudios médicos, incluyendo imágenes de rayos X y evaluaciones clínicas; en Brasil, el grupo ransomware KillSec atacó proveedores de software médico en septiembre de 2025, robando 34 GB de datos sensibles como resultados de laboratorio y registros de menores, afectando a instituciones en múltiples países; y en Colombia, brechas en 2022 expusieron

datos de miles de pacientes, destacando costos promedio de US$3.81 millones por incidente en la región, según informes de IBM.

Estos eventos, combinados con un incremento del 110% en brechas de salud en 2025 a nivel global (según datos de la Oficina para Derechos Civiles del HHS), resaltan cómo los ataques como ransomware y phishing no solo comprometen la privacidad, sino que interrumpen operaciones críticas, retrasan tratamientos y erosionan la confianza pública en el sistema de salud.

Esta medida se alinea con estándares internacionales y regionales para mitigar estos riesgos. El Reglamento General de Protección de Datos (RGPD) de la Unión Europea enfatiza el consentimiento explícito, voluntario e informado para datos sensibles como los de salud, requiriendo notificaciones de brechas en 72 horas y auditorías regulares para garantizar la integridad y confidencialidad, principios que esta propuesta incorpora directamente. En América Latina, la Organización Panamericana de la Salud (OPS) ha documentado que, aunque 19 países regulan la telesalud (90.5% de la región, con 78.9% de regulaciones pre-2019), solo un puñado aborda explícitamente la ciberseguridad y la confidencialidad, recomendando marcos éticos que incluyan el secreto profesional en telesalud (mencionado en 11 países) y la interoperabilidad de historias clínicas electrónicas (HCE, reguladas en 16 países).

La OPS urge a los gobiernos a priorizar protecciones para datos personales en salud digital, promoviendo el uso secundario anónimo para investigación mientras se asegura la revocabilidad del consentimiento y la notificación de brechas, alineándose con las recomendaciones del Diálogo Empresarial de las Américas para armonizar definiciones y fomentar flujos transfronterizos seguros de datos.

El proyecto propone requerir consentimientos explícitos —voluntarios, informados, específicos y revocables en cualquier momento, detallando propósitos, destinatarios, riesgos y medidas de seguridad— para el procesamiento de datos en aplicaciones de salud y servicios de telemedicina, abordando directamente las vulnerabilidades expuestas en brechas recientes al empoderar a los pacientes con control sobre su información. De otra parte, se exigen auditorías anuales independientes o

internas de sistemas de seguridad, cubriendo encriptación, controles de acceso, detección de brechas y cumplimiento con HIPAA y normativas locales, con reportes al Departamento de Salud para una fiscalización proactiva que prevenga incidentes antes de que ocurran.

Estas obligaciones se integran mediante enmiendas específicas a las Leyes Núm. 168- 2018 y 48-2020, fortaleciendo la fiscalización sin alterar la cobertura de servicios ni requerir certificaciones adicionales, y estableciendo sanciones escaladas bajo la Ley Núm. 111 de 2005 para disuadir incumplimientos.

La implementación de esta Ley no generará impacto presupuestario adicional, ya que delega los costos de consentimientos y auditorías en los proveedores privados —quienes ya operan bajo estructuras regulatorias existentes del Departamento de Salud y la Oficina de Reglamentación y Certificación de Profesionales de la Salud (ORCPS)— y utiliza mecanismos de fiscalización vigentes, como revisiones anuales sin necesidad de nuevos recursos fiscales, promoviendo eficiencia y responsabilidad compartida.

DECRÉTASE POR LA ASAMBLEA LEGISLATIVA DE PUERTO RICO:

Sección 1**.-** Titulo.

Esta Ley se conocerá como la "Ley para la Protección de Datos Personales en Aplicaciones de Salud y Servicios de Telemedicina".

Sección 2. – Definiciones.

Para los fines de esta Ley, los siguientes términos tendrán el significado que a continuación se indica:

(a) "Aplicación de Salud": Cualquier software, programa informático, plataforma digital o aplicación móvil que ofrezca servicios de telemedicina, telesalud, monitoreo de salud, almacenamiento de datos médicos o consultas remotas, regulados bajo la Ley Núm. 168-2018 y/o la Ley Núm. 48-2020.

(b) "Consentimiento Explícito": Autorización voluntaria, informada y específica del paciente para el procesamiento de sus datos personales de salud, otorgada por escrito o electrónicamente, con opción de revocación en cualquier momento. Deberá incluir detalles sobre el propósito, duración, destinatarios, riesgos y medidas de seguridad.

(c) "Auditoría": Evaluación anual de los sistemas de seguridad y privacidad de datos en aplicaciones de salud, realizada por entidades independientes acreditadas por el Departamento de Salud o internas, verificando cumplimiento con estándares de encriptación, acceso controlado y detección de brechas, conforme a HIPAA y normativas locales.

(d) "Datos Personales de Salud": Información sensible relacionada con la salud física o mental de una persona, incluyendo diagnósticos, tratamientos, historiales médicos y datos biométricos, conforme a la Ley Núm. 111 de 2005 y HIPAA.

(e) "Proveedor": Cualquier entidad, profesional o empresa licenciada que ofrezca servicios de telemedicina o aplicaciones de salud en Puerto Rico, sujeto a las Leyes Núm. 168-2018 y Núm. 48-2020.

Sección 3. Requerimiento de Consentimientos Explícitos.

(a) Todo proveedor deberá obtener un consentimiento explícito del paciente antes de recolectar, procesar, almacenar o compartir datos personales de salud.

(b) El consentimiento será claro, accesible y separado de otros términos, informando sobre: tipo de datos, fines (ej. diagnóstico, investigación anónima), destinatarios (ej. aseguradoras), medidas de seguridad y derechos del paciente, incluyendo, pero sin limitarse a la revocación, acceso, corrección.

(c) En emergencias, se permite procesamiento sin consentimiento previo, con notificación inmediata posterior y obtención retroactiva.

(d) Violaciones se sancionarán con multas de hasta $10,000 por incidente, conforme a la Ley Núm. 111 de 2005, aplicadas por el Departamento de Salud o la Oficina del Contralor.

Sección 4. Requerimiento de Auditorías Periódicas.

(a) Los proveedores realizarán auditorías anuales cubriendo encriptación, controles de acceso, detección de brechas y cumplimiento normativo.

(b) Auditorías serán por terceros acreditados o internas, reportadas al Departamento de Salud sin costo fiscal adicional.

(c) Vulnerabilidades detectadas se corregirán en 30 días, con notificación a pacientes afectados en brechas.

(d) Incumplimientos se sancionarán con multas de hasta $25,000 por auditoría omitida, aplicadas por mecanismos existentes.

Sección 5. Enmiendas a la Ley Núm. 168-2018.

(a) Se enmienda el Artículo 2 de la Ley Núm. 168-2018 para añadir las definiciones de "consentimiento explícito", "auditoría" y "datos personales de salud" establecidas en la Sección 2 de esta Ley.

(b) Se enmienda el Artículo 3 de la Ley Núm. 168-2018 para añadir un inciso (f) que requiera a los proveedores cumplir con los consentimientos explícitos y auditorías anuales dispuestos en las Secciones 3 y 4 de esta Ley, integrándolos como deberes esenciales para la licencia y operación.

Sección 6. - Enmiendas a la Ley Núm. 48-2020.

(a) Se enmienda el Artículo 2 de la Ley Núm. 48-2020 para añadir las definiciones de "consentimiento explícito", "auditoría" y "datos personales de salud" establecidas en la Sección 2 de esta Ley.

(b) Se enmienda el Artículo 4 de la Ley Núm. 48-2020 para añadir un inciso (g) que obligue a los proveedores de telesalud y ciberterapia a adherirse a los requisitos de consentimientos y auditorías de las Secciones 3 y 4 de esta Ley, como condición para la práctica regulada.

Sección 7. - Implementación.

Los proveedores autorizados bajo las Leyes Núm. 168-2018 y Núm. 48-2020 adaptarán sus prácticas contados ciento ochenta (180) días a partir de la vigencia de esta Ley. El Departamento de Salud fiscalizará mediante estructuras existentes, sin asignaciones presupuestarias nuevas.

Sección 8. - Clausula de Separabilidad.

Si cualquier disposición de esta Ley fuera declarada inconstitucional, nula o inválida por un tribunal competente, dicha declaración no afectará las demás disposiciones de esta Ley, las cuales continuarán en pleno vigor y efecto.

Sección 9.- Vigencia.

Esta Ley comenzará a regir inmediatamente después de su aprobación.