ASSEMBLY, No. 5075

STATE OF NEW JERSEY
220th LEGISLATURE

INTRODUCED JANUARY 19, 2023

Sponsored by:
Assemblyman PAUL D. MORIARTY
District 4 (Camden and Gloucester)
Assemblywoman PAMELA R. LAMPTITT
District 6 (Burlington and Camden)

SYNOPSIS
Prohibits acquisition or disclosure of certain personal health information without consent.

CURRENT VERSION OF TEXT
As introduced.
AN ACT concerning the acquisition and disclosure of certain personal health information and supplementing Title 26 of the Revised Statutes.

BE IT ENACTED by the Senate and General Assembly of the State of New Jersey:

1. As used in P.L. , c. (C.) (pending before the Legislature as this bill):
   “Acquire” or “acquisition” means to collect, obtain, generate, or store any information from a person through any means.
   “Biometric data” means individually identifiable information concerning the physical, physiological, or behavioral characteristics of a person, including, but not limited to, heart rate, blood type, menstrual or ovulation cycle, sleep patterns, fingerprint, voice print, retina or iris image, or any other physical characteristics.
   “Consent” means an informed and unambiguous affirmative authorization freely given by a person through a written statement or any other clear affirmative action.
   “Disclose” or “disclosure” means to transmit, release, transfer, share, disseminate, distribute, make available, rent, sell, or otherwise communicate any information to a third party.
   “Health care provider” means a physician, advanced practice nurse, or physician assistant acting within the scope of a valid license or certification issued pursuant to Title 45 of the Revised Statutes.
   “Health data” means information that relates to a past, present, or future physical or mental health condition or diagnosis of a person or the past, present, or future payment for the provision of health care to a person.
   “Mobile application” means a software program that runs on the operating system of a mobile device.
   “Mobile application developer” means any person or entity that owns or maintains a mobile application and makes that application available for the use of customers, whether for a fee or otherwise.
   “Person” means a natural person, estate of a natural person, or a child in the custody of a natural person.
   “Protected health information” has the same meaning as defined under the federal “Health Insurance Portability and Accountability Act of 1996,” Pub.L.104-191, and any regulations promulgated thereunder by the Secretary of the United States Department of Health and Human Services.
“Third party” means any person or entity other than the person from whom the biometric data, health data, or protected health information was acquired.

“Wearable device” means an electronic device that is worn by a person, that tracks, analyzes, or transmits the person’s biometric data or health data, or both, that is capable of collecting the person’s location data.

2. a. No health care provider, mobile application developer, or third party shall acquire or disclose the biometric data, health data, or protected health information of a person who is a resident of this State, which information is acquired through the use of in-person or telephone communication, a mobile application, an Internet website, or a wearable device, without obtaining the consent of the person pursuant to subsection b. of this section.

b. (1) Before acquiring the biometric data, health data, or protected health information of a person who is a resident of this State, a health care provider, mobile application developer, or third party shall obtain consent from the person to acquire such information. After obtaining the consent of the person, a health care provider, mobile application developer, or third party shall not be required to obtain a separate and distinct form of consent before each subsequent acquisition of biometric data, health data, or protected health information from the person, provided that the consent obtained from the person has explicitly authorized such acquisition.

(2) No more than three calendar days before each disclosure of the biometric data, health data, or protected health information of a person who is a resident of this State, a health care provider, mobile application developer, or third party shall obtain consent from the person to disclose such information. Each disclosure of the biometric data, health data, or protected health information of a person shall constitute a separate and distinct disclosure, which shall require a health care provider, mobile application developer, or third party to obtain a separate and distinct form of consent from the person from whom the biometric data, health data, or protected health information was acquired.

(3) The provisions of this subsection shall not apply to a health care provider that discloses or acquires the biometric data, health data, or protected health information of a person, who is a resident of this State, to or from another health care provider for the purposes of medical treatment or medical diagnosis.

c. Nothing contained herein shall be construed to limit, diminish, or abrogate the rights of a person under HIPAA or the obligations of a health care provider or third party under HIPAA.

d. (1) If a court of competent jurisdiction finds that a health care provider, mobile application developer, or third party has violated this section, the court may award damages, computed at a
rate of $1,000 per violation, reasonable attorney’s fees, and the
costs incurred in maintaining that civil action.

(2) The private right of action authorized pursuant to this
section does not supplant any other claim or cause of action
available to a person under common law or by statute. The
provisions of this subsection apply in addition to any other common
law and statutory remedies.

3. This act shall take effect immediately.

STATEMENT

This bill prohibits a health care provider, mobile application
developer, or third party from acquiring or disclosing a person’s
biometric data, health data, or protected health information
(collectively hereinafter referred to as “personal health
information”), which information is acquired through the use of in-
person or telephone communication, a mobile application, an
Internet website, or a wearable device, without obtaining the
person’s consent.

The bill requires the health care provider, mobile application
developer, or third party to obtain the person’s consent before
acquiring a person’s personal health information and no more than
three calendar days before each disclosure of the person’s personal
health information. After obtaining the consent of the person, a
health care provider, mobile application developer, or third party
would not be required to obtain a separate and distinct form of
consent before each subsequent acquisition of personal health
information, provided that the consent obtained from the person has
explicitly authorized such acquisition. However, each disclosure of
the personal health information would constitute a separate and
distinct disclosure, which would require a separate and distinct
grant of consent from the person from whom the personal health
information was acquired.

Under the bill, the term “acquire” means to collect, obtain,
generate, or store any information from a person through any
means. In contrast, the term “disclose” means to transmit, release,
transfer, share, disseminate, distribute, make available, rent, sell, or
otherwise communicate any information to a third party.

The provisions of this bill would not apply to a health care
provider that discloses or acquires the personal health information
of a person to or from another health care provider for the purposes
of medical treatment or medical diagnosis. Moreover, nothing
contained in the bill may be construed to limit, diminish, or
abrogate the rights of a person under the “Health Insurance
Portability and Accountability Act of 1996,” and any regulations
promulgated thereunder by the Secretary of the U.S. Department of
The bill further provides that if a court of competent jurisdiction finds a health care provider, mobile application developer, or third party has violated the provisions of the bill, the court may award damages, computed at a rate of $1,000 per violation, reasonable attorney’s fees, and costs incurred in maintaining that civil action; and the private right of action authorized pursuant to this bill does not supplant any other claim or cause of action available to a person under common law or by statute.