10102011D

SENATE BILL NO. 224

Senate Amendments in [ ] — February 1, 2010

A BILL to amend the Code of Virginia by adding a section numbered 32.1-127.1:05, relating to notification of breach of medical information.

Patron Prior to Engrossment—Senator Barker

Referred to Committee on Education and Health

Be it enacted by the General Assembly of Virginia:

1. That the Code of Virginia is amended by adding a section numbered 32.1-127.1:05 as follows:

§ 32.1-127.1:05. Breach of medical information notification.

A. As used in this section:

"Breach of the security of the system" means unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security, confidentiality, or integrity of medical information maintained by an individual or entity. Good faith acquisition of medical information by an employee or agent of an individual or entity for the purposes of the individual or entity is not a breach of the security of the system, provided that the medical information is not used for a purpose other than a lawful purpose of the individual or entity or subject to further unauthorized disclosure.

"Encrypted" means the transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without the use of a confidential process or key, or the securing of the information by another method that renders the data elements unreadable or unusable.

"Entity" includes corporations, business trusts, estates, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures, governments, governmental subdivisions, agencies, or instrumentalities or any other legal entity, whether for profit or not for profit.

"Individual" means a natural person.

"Medical information" means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted:

1. Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or

2. An individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

The term does not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public.

"Notice" means:

1. Written notice to the last known postal address in the records of the individual or entity;

2. Telephone notice;

3. Electronic notice; or

4. Substitute notice, if the individual or the entity required to provide notice demonstrates that the cost of providing notice will exceed $50,000, the affected class of Virginia residents to be notified exceeds 100,000 residents, or the individual or the entity does not have sufficient contact information or consent to provide notice as described in subdivisions 1, 2, or 3 of this definition. Substitute notice consists of the following:

a. E-mail notice if the individual or the entity has e-mail addresses for the members of the affected class of residents;

b. Conspicuous posting of the notice on the website of the individual or the entity if the individual or the entity maintains a website; and

c. Notice to major statewide media.

Notice required by this section shall include a description of the following:

(1) The incident in general terms;

(2) The type of medical information that was subject to the unauthorized access and acquisition;

(3) The general acts of the individual or entity to protect the personal information from further unauthorized access; and

(4) A telephone number that the person may call for further information and assistance, if one exists.

"Redact" means alteration or truncation of data such that no information regarding an individual's

medical history, mental or physical condition, or medical treatment or diagnosis or no more than four digits of a health insurance policy number, subscriber number, or other unique identifier are accessible as part of the medical information.

B. If unencrypted or unredacted medical information was or is reasonably believed to have been accessed and acquired by an unauthorized person, an individual or entity that owns or licenses computerized data that includes medical information shall disclose any breach of the security of the system following discovery or notification of the breach of the security of the system to the Office of the Attorney General and any affected resident of the Commonwealth without unreasonable delay. Notice required by this section may be reasonably delayed to allow the individual or entity to determine the scope of the breach of the security of the system and restore the reasonable integrity of the system. Notice required by this section may be delayed if, after the individual or entity notifies a law-enforcement agency, the law-enforcement agency determines and advises the individual or entity that the notice will impede a criminal or civil investigation, or homeland or national security. Notice shall be made without unreasonable delay after the law-enforcement agency determines that the notification will no longer impede the investigation or jeopardize national or homeland security.

C. An individual or entity shall disclose the breach of the security of the system if encrypted information is accessed and acquired in an unencrypted form, or if the security breach involves a person with access to the encryption key.

D. An individual or entity that maintains computerized data that includes medical information that the individual or entity does not own or license shall notify the owner or licensee of the information of any breach of the security of the system without unreasonable delay following discovery of the breach of the security of the system, if the medical information was accessed and acquired by an unauthorized person or the individual or entity reasonably believes the medical information was accessed and acquired by an unauthorized person.

E. In the event an individual or entity provides notice to more than 1,000 persons at one time, pursuant to this section, the individual or entity shall notify, without unreasonable delay, the Office of the Attorney General of the timing, distribution, and content of the notice.

F. This section shall not apply to (i) a person or entity who is a "covered entity" under the Health Insurance Portability and Accountability Act of 1996 (42 USC § 1320d et seq.) and is subject to requirements for notification in the case of a breach of protected health information (42 USC 17932 et seq.), [~~*or (ii)*~~ *(ii) a "business associate" of a HIPAA covered entity that is subject to requirements for notification in the case of a breach of protected health information (42 USC 17932 et seq.), or (iii)*] *a person or entity who is a non-HIPAA-covered entity subject to the Health Breach Notification Rule promulgated by the Federal Trade Commission pursuant to 42 USC § 17937 et seq.*

G. An entity that complies with the notification requirements or procedures pursuant to the rules, regulations, procedures, and guidelines established by the entity's primary or functional state or federal regulator shall be in compliance with this section.

H. Pursuant to the enforcement duties and powers of the Office of the Attorney General, the Attorney General may bring an action to address violations of this section. The Office of the Attorney General may impose a civil penalty not to exceed $150,000 per breach of the security of the system or a series of similar breaches of a similar nature that are discovered in a single investigation. Nothing in this section shall limit an individual from recovering direct economic damages from a violation of this section.

[2. That the provisions of this act shall become effective on January 1, 2011.]