REPORT OF THE
JOINT COMMISSION ON HEALTH CARE

NOTIFICATION FOR BREACHES OF PERSONAL HEALTH RECORDS

TO THE GOVERNOR AND
THE GENERAL ASSEMBLY OF VIRGINIA

REPORT DOCUMENT NO. 128

COMMONWEALTH OF VIRGINIA
RICHMOND
2012

Code of Virginia § 30-168.

The Joint Commission on Health Care (the Commission) is established in the legislative branch of state government. The purpose of the Commission is to study, report and make recommendations on all areas of health care provision, regulation, insurance, liability, licensing, and delivery of services. In so doing, the Commission shall endeavor to ensure that the Commonwealth as provider, financier, and regulator adopts the most cost-effective and efficacious means of delivery of health care services so that the greatest number of Virginians receive quality health care. Further, the Commission shall encourage the development of uniform policies and services to ensure the availability of quality, affordable and accessible health services and provide a forum for continuing the review and study of programs and services.

The Commission may make recommendations and coordinate the proposals and recommendations of all commissions and agencies as to legislation affecting the provision and delivery of health care.

For the purposes of this chapter, "health care" shall include behavioral health care.

Members of the Joint Commission on Health Care

Chairman
The Honorable Benjamin L. Cline

Vice-Chair
The Honorable Linda T. Puller

Virginia House of Delegates
The Honorable Robert H. Brink
The Honorable David L. Bulova
The Honorable Rosalyn R. Dance
The Honorable T. Scott Garrett
The Honorable Algie T. Howell, Jr.
The Honorable Harvey B. Morgan
The Honorable David A. Nutter
The Honorable John M. O'Bannon, III
The Honorable Christopher K. Peace

Senate of Virginia
The Honorable George L. Barker
The Honorable Harry B. Blevins
The Honorable R. Edward Houck
The Honorable L. Louise Lucas
The Honorable Ralph S. Northam
The Honorable Patricia S. Ticer
The Honorable William C. Wampler, Jr.

The Honorable William A. Hazel, Jr.
Secretary of Health and Human Resources

JCHC Staff

Kim Snead
Executive Director

Stephen W. Bowman
Senior Staff Attorney/Methodologist

Michele L. Chesser, PhD
Senior Health Policy Analyst

Jaime H. Hoyle
Senior Staff Attorney/Health Policy Analyst

Sylvia A. Reid
Publication/Operations Manager

Preface

Senate Bill 1229, introduced by Senator George L. Barker during the 2009 General Assembly Session, sought to provide additional protections for medical information by requiring that individuals be notified of security breaches involving databases containing their health information. SB 1229 was referred by the Senate Committee for Courts of Justice to the Joint Commission on Technology and Science (JCOTS) and the Joint Commission on Health Care (JCHC) for study.

Individually-identifiable health information is collected or retained by numerous public and private entities. When the Health Insurance Portability and Accountability Act (HIPAA) was enacted, stringent standards were established to protect the privacy of health information maintained by health care providers, health insurers, and health care clearinghouses. Recently, new entities called personal health record vendors have emerged. These personal health record vendors are not subject to HIPAA requirements even though the vendors maintain sensitive identifiable health information that has been provided by consumers. SB 1229 sought to add personal health record vendors within the definition of health care providers that are subject to Virginia's privacy provisions in *Code of Virginia* § 32.1-127.1:03 and to create within *Code* § 18.2-186.6 a notification requirement for breaches of individually-identifiable health information.

Since the time that SB 1229 was referred to JCOTS and JCHC, additional federal notification requirements were enacted pursuant to the privacy provisions contained within the Health Information Technology for Economic and Clinical Health Act (of the American Recovery and Reinvestment Act of 2009). Although these notification requirements addressed the objectives of SB 1229, the JCOTS/JCHC study determined that some collections of individually-identifiable health information maintained by State government entities were not covered by the new federal requirements. Consequently during the 2010 General Assembly Session, three bills (HB 525, HB 1039, and SB 224) were introduced to create breach notification requirements for State and local governmental entities; HB 1039 was enacted (2010 *Acts of Assembly*, Chapter 852).

On behalf of the Joint Commission and staff, I would like to thank representatives of the Health Law Section of the Virginia State Bar, the Joint Commission on Technology and Science, and the Office of the Attorney General for their participation and assistance in this study.

Kim Snead
Executive Director
April 2012

Table of Contents

Notification for Breaches of Personal Health Records

Senate Bill 1229, introduced by Senator George L. Barker during the 2009 General Assembly Session, sought to provide additional protections for medical information by requiring that individuals be notified of security breaches involving databases containing their health information. Pursuant to Senate Rule 20(l), SB 1229 was referred by the Senate Committee for Courts of Justice to the Joint Commission on Technology and Science (JCOTS) and the Joint Commission on Health Care (JCHC) for study.

Background

Individually-identifiable health information is collected or retained by numerous public and private entities. When the Health Insurance Portability and Accountability Act (HIPAA) was enacted, stringent standards were established to protect the privacy of health information maintained by health care providers, health insurers, and health care clearinghouses. Recently, new entities called personal health record (PHR) vendors have emerged. These PHR vendors are not subject to HIPAA requirements even though the vendors maintain sensitive identifiable health information that has been provided by consumers. SB 1229 sought to add PHR vendors within the definition of health care providers that are subject to Virginia's privacy provisions in *Code of Virginia* § 32.1-127.1:03 and to create within *Code* § 18.2-186.6 a notification requirement for breaches of individually-identifiable health information.

Newly-Enacted Federal Requirements. Since the time that SB 1229 was referred for study, additional federal notification requirements were enacted by the Federal Trade Commission and the U. S. Department of Health and Human Services. The new regulations, which became effective in September 2009, address notification requirements for breaches of individually-identifiable health information pursuant to the privacy provisions contained within the Health Information Technology for Economic and Clinical Health Act (HITECH) of the American Recovery and Reinvestment Act of 2009. These regulations cover PHR vendors; such as Google Health and Microsoft Vault, PHR business associates and third-party providers, and the entities that have historically been subject to HIPAA.

Under the new law, health information was protected if it met the following three criteria; specifically that the health information:

- Includes individual health information
- Is provided by or on behalf of the individual and
- Identifies the individual or can be used to identify the individual.

In the event of a breach, the consumer must be notified "without unreasonable delay and in no case later than 60 days following discovery of the breach…."[1] The federal law defined the method of notice and what must be included in the notice. Slides 20-30 in the attached presentation provide details of the Federal Trade Commission's new breach notification requirements in the following areas:

1. Type of Entities Covered
2. Health Information Covered
3. Definition of a Breach

[1] www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html

4. When Breaches Are Discovered
5. Timing for Notification
6. Notice Method to Individuals
7. Notice to Media and the Federal Trade Commission
8. Content of Notice
9. Miscellaneous Provisions: Enforcement and Effective Date

While breach notification requirements included in the HITECH Act and HIPAA cover many health records, these requirements do not apply to some records containing individually-identifiable health information that are maintained by State and local government entities. The significance of this gap in coverage was underscored in April 2009, when the Prescription Monitoring Program (PMP) database was breached. Although the PMP database held 35 million individually-identifiable prescription records, the HITECH requirements did not apply.[2] The Virginia Department of Health Professions, which maintains the PMP, was not required to provide notification because the database did not collect information provided for or on behalf of an individual.[3]

Review by Joint JCOTS/JCHC Subcommittee

A joint JCOTS/JCHC Subcommittee was formed to review the provisions of SB 1229; Delegate O'Bannon and Senator Barker were appointed to serve on behalf of JCHC and Delegate Nixon and Senator Wampler were appointed to serve on behalf of JCOTS. On September 16, 2009, the Subcommittee met to review "recent changes to federal law that would require entities subject to the Health Insurance Portability and Accountability Act and certain Federal Trade Commission regulations to provide notice of breaches involving medical information….[In the course of the review,] it became apparent that certain entities – such as state and local government agencies – may not be subject to these federal requirements."[4] The joint Subcommittee directed staff to conduct a limited review of the government collections that were not subject to breach notification requirements and if appropriate to draft legislation for the 2010 Session.

Joint Subcommittee Actions. The Subcommittee made no formal legislative recommendations regarding SB1229. However, staff was directed to conduct a limited review of the State government collections that were not subject to breach notification requirements and if appropriate to draft legislation that would create breach notification requirements for State and local governmental entities with individually identifiable health information not currently covered under HIPPAA.

Following the Subcommittee meeting, an electronic survey was sent to 16 State agencies to determine the magnitude of their electronic records containing individually-identifiable health information that did not require breach notification. In analyzing the survey responses, staff found:

[2] http://www.dhp.state.va.us/misc_docs/DHPNewsRelease20090603.pdf
[3] In this specific instance, some individuals were notified of the possible breach, as required by *Code of Virginia* §18.2-186.6 because their Social Security numbers were included in the database and may have been compromised. http://www.dhp.state.va.us/misc_docs/DHPNewsRelease20090603.pdf
[4] Executive Summary, *Annual Report of the Joint Commission on Technology and Science (2009)* RD No. 93 (2011).

- Most of the responding agencies, which had established breach notification requirements for their individually-identifiable health information, were subject to the Family Education Rights and Privacy Act or the HITECH Act's modification of HIPAA.
- There were also State agencies that maintained records with individually-identifiable health information that did not require breach notification; including the Workers' Compensation Program, the Department of Health Professions' Prescription Monitoring Program, the Virginia Department of Health's National Electronic Disease Surveillance System and its Cancer Registry, and Department of Social Services databases for Benefits, Family Services, Licensing, Child Care, and Child Support Enforcement Programs.
    - These collections of individually-identifiable health information varied in size, the largest being the Prescription Monitoring Program with more than 4 million records.
- While some of the surveyed agencies collected contact information, two agencies indicated some of the contact information was likely to be incomplete or out-of-date.

Actions Taken by JCHC and the 2010 General Assembly

JCHC members reviewed the recommendations of the Joint Subcommittee and approved including study of breach notification requirements for State and local governmental entities in the JCHC 2010 Work Plan, if the issue could not be resolved during 2010 Session. During the 2010 General Assembly Session, three bills, HB 525 (Delegate Nixon), HB 1039 (Delegate Byron), and SB 224 (Senator Barker) were introduced to create breach notification requirements for State and local government entities.

- HB 525 was incorporated into HB 1039, which was enacted as Chapter 852 of the 2010 *Acts of Assembly*. HB 1039 requires Virginia residents to be notified of breaches involving their individually-identifiable health information, when the breach involves the database of State or local government entities and the database does not have notification requirements under HIPAA or the HITECH Act.

- SB 224 differed from HB 525 in that its breach notification requirements included public and private entities that have individually-identifiable health information which are not covered by breach notification laws or regulations. SB 224 ultimately was not enacted.

JCHC Staff for this Report

Stephen W. Bowman
Senior Staff Attorney/Methodologist

Attachments

Notification for Breaches of Personal Health Records

Joint JCOTS/JCHC Study

October 7, 2009

Stephen W. Bowman
Senior Staff Attorney/Methodologist
Joint Commission on Health Care

Agenda

- Senate Bill 1229
- Virginia's Database Breach Law
- Federal Health Information Breach Notification Laws
- Joint JCOTS/JCHC Subcommittee Conclusions
- Policy Options

Senate Bill 1229 (Barker) was referred to JCOTS and JCHC for study

- Modifies Virginia's Database Breach Law to include notification for breaches of health information
  - Patron's intent - protecting health information not covered by Health Insurance Portability and Accountability Act (HIPAA)
  - Non-HIPAA covered entities with individually identifiable health information were **not** required to protect such information or notify when a breach occurred. Examples include:
    - Google Health
    - Microsoft Vault
    - Regional Health Information Organizations (RHIOs)
    - Other entities that collect personal health records

Virginia's Database Breach Law (2008)

- §18.2-186.6 of the *Code of Virginia* was adopted after four years of discussion and compromise. Entities involved:
  - Debt collection agencies,
  - Banking industry,
  - Consumer groups,
  - State Police, and
  - Other interested stakeholders.
- Law's purpose is to address instances of identity theft or other fraud

Virginia's Database Breach Law (2008)

"Personal information" is a person's first name or first initial and last name, in combination with one or more of the following:

1. Social Security Number
2. Driver's license number or state-issued ID number
3. Financial account number, credit card or debit card number, in combination with required security code, password, or access code
4. Medical information
5. Health insurance information

SB 1229 would add these

5

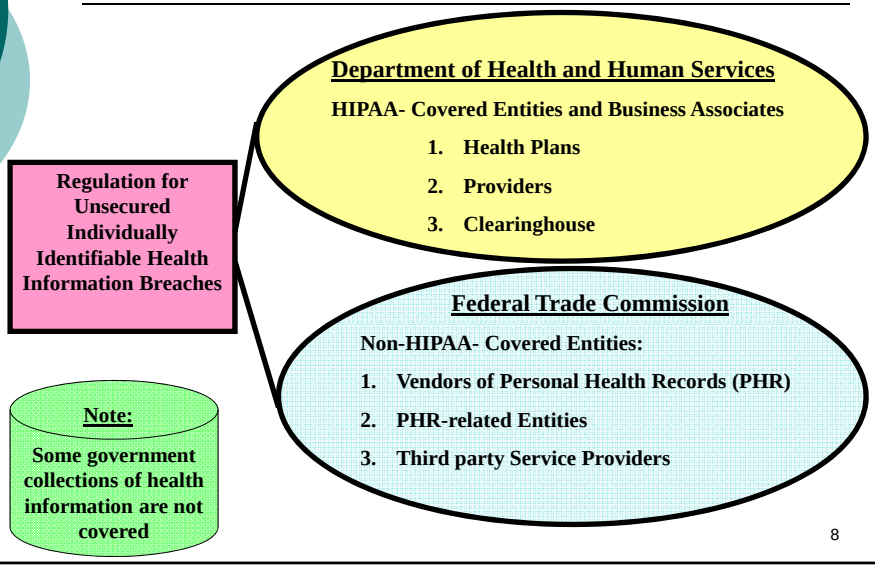
Recent Federal Health Information Protection Changes

HITECH Act Increase Health Information Protections

- HITECH Act passed February 17, 2009
  - Includes significant breach notification requirements for entities that have individually identifiable health information
  - Agencies that will promulgate regulations
    - Center for Medicare and Medicaid Services
    - Department of Health and Human Services (HHS)
    - Federal Trade Commission (FTC)
    - Office for Civil Rights

7

HHS and FTC Cover Entities that Possess Unsecured Individually Identifiable Health Information



8

Purpose of SB 1229 is Addressed by New FTC Regulations

- FTC regulations address non-HIPAA covered entities that collect personal health information, such as:
  - Examples of Vendors
    - Google Health
    - Microsoft Vault
    - RHIOs
  - Vendor's business associates
  - Vendor's third-party providers

Note: Non-profit organizations that have such identifiable information must comply with new regulations.

9

FTC Regulation Definitions: Health Information and Breaches Covered

- Elements for covered health information:
  1. Individual health information,
  2. Provided by or on behalf of the individual, and
  3. Identifies the individual or can be used to identify the individual.

- Elements triggering breach notification:
  1. Unauthorized acquisition,
  2. Unsecured information, and
  3. Identifies or could identify an individual

Title 16 of the *Code of Federal Regulations* Part 318.2

10

FTC Notification Regulations: Timing and Method

- Timing:
  - Notification must be made without unreasonable delay and in no case later than 60 days following discovery.
- Method:
  - Written notice by first-class mail unless individual intentionally opts to receive email notification
  - If more than 10 individuals cannot be contacted then:
    - Notice posted on website for 90 days, or
    - Notice in print or broadcast media where affected individuals reside

Title 16 of the *Code of Federal Regulations* Part 318.4 and 318.5 11

FTC Regulations: Content of Notice

- Notice shall describe:
  1. What happened
  2. Types of information breached
  3. Steps individuals should take to protect themselves
  4. Actions taken to investigate, mitigate harm, and protect against further breaches; and
  5. Contact procedures to learn additional information

Title 16 of the *Code of Federal Regulations* Part 318.6 12

Not All Individually Identifiable Health Information is Covered

- Some government collections of individually identifiable health information are outside of new regulations
  - Information must be ”provided by or on behalf of the individual”
- Example of governmental database not covered:
  - Prescription Monitoring Program
    - Virginia’s Department of Health Professions

13

Joint JCOTS/JCHC Subcommittee Conclusions

Joint Subcommittee

Delegate Nixon	Senator Barker
Delegate O’Bannon	Senator Wampler

Joint JCOTS/JCHC Subcommittee Conclusions

- No action is needed pursuant to SB 1229
  - Objectives of SB 1229 have been satisfied by HITECH Act
- However, it would be useful for JCHC and JCOTS staff to review state and local government collections of individually identifiable health information that do not require breach notification
  - If appropriate, draft legislation to address this issue for 2010 Session

Policy Options

Policy Options

Option 1: Take no action.

Option 2: JCHC continue the study and include a report in the 2010 Workplan, if the current JCOTS/JCHC review is not completed in time for 2010 Session.

- Review focus: electronic individually identifiable health information records held by state and local government entities that do have legal requirements to notify individuals in the event of a breach.

17

Public Comment

- Written public comments on the proposed options may be submitted to JCHC by close of business on November 4, 2009.
- Comments may be submitted via:
  - E-mail: sreid@jchc.virginia.gov
  - Fax: 804-786-5538
  - Mail: Joint Commission on Health Care
P.O. Box 1322
Richmond, Virginia 23218
- Comments will be summarized and presented to JCHC during its November 12th meeting.

18

Additional Slides

Detailed Analysis: Federal Trade Commission Regulations on Health Information Breach Notification

FTC Regulations for Health Information Breaches for Non-HIPAA Covered Entities

1) Type of Entities Covered
2) Health Information Covered
3) Definition of a Breach
4) When Breaches Are Discovered
5) Timing for Notification
6) Notice Method to Individuals
7) Notice to Media and FTC
8) Content of Notice
9) Miscellaneous Provisions: Enforcement and Effective Date

1. Types of Entities Covered by FTC Regulations

1. ***Vendors of personal health records***
   a. Non-HIPAA covered entity that offers or maintains a personal health record.

2. ***PHR related entity - Non-HIPAA covered entity that***
   a. Offers products or services through the Web site of a vendor of personal health records
   b. Offers products or services through the Web sites of HIPAA-covered entities that offer individuals personal health records
   c. Accesses information in a personal health record or sends information

3. ***Third party service provider that***
   a. Provides services to a vendor of personal health records in connection with the offering or maintenance of a personal health record or to a PHR related entity in connection with a product or service offered by that entity; and
   b. Accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured PHR identifiable health information as a result of such services.

Note: FTC regulations explicitly exclude HIPAA covered entities and HIPAA covered business associates.

Includes organizations outside of typical FTC purview, for example non-profits

Title 16 of the *Code of Federal Regulations* Part 318.2

21

2. Health Information Covered by FTC Regulations

PHR identifiable health information means:

''***individually identifiable health information***,'' as defined in section 1171(6) of the Social Security Act (42 U.S.C. 1320d(6)), and, with respect to an individual, information:

(1) That is provided by or on behalf of the individual; and

(2) That identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

Note: Health Information definition extends to even search-engine queries if search-engine on PHR website

Title 16 of the *Code of Federal Regulations* Part 318.2

22

3. What is a Breach?

- **Breach of security -** Acquisition of ***unsecured PHR identifiable health information*** of an individual in a personal health record without the authorization of the individual.
- Unauthorized acquisition will be ***presumed*** to include unauthorized access to unsecured PHR identifiable health information unless … reliable evidence shows … there has not been, or could not reasonably have been, ***unauthorized acquisition*** of such information.

Breach of PHR health information requires 3 main components:

1. ***Unauthorized acquisition***
2. ***Unsecured information***
3. ***Identifies or could identify an individual***

Title 16 of the *Code of Federal Regulations* Part 318.2

4. When Breaches Are Discovered

- A breach of security ***shall be treated as discovered*** as of the first day on which such breach is known or reasonably should have been known to the:
  - Vendor of personal health records,
  - PHR related entity, or
  - Third party service provider.
- Knowledge of breach is deemed if such breach ***is known, or reasonably should have been known***, to any person, other than the person committing the breach, who is an employee, officer, or other agent of such vendor of personal health records, PHR related entity, or third party service provider.

Note: Time begins when breach should have been or is discovered

Title 16 of the *Code of Federal Regulations* Part 318.3

5. Timing for Notification

- Notification must be made without unreasonable delay and in no case later than 60 days following discovery.
  - 60 days outer limit for notice
  - Unreasonable delay can be found
- Burden of proof - entities have burden to show that appropriate and timely notifications were made
- Law enforcement exception for impeding criminal investigation or cause damage to national security

Title 16 of the *Code of Federal Regulations* Part 318.4

6. Notice Method to Individuals

- Written notice, by first-class mail to the individual at the last known address
  - May instead use email if "the individual is given a clear, conspicuous, and reasonable opportunity to receive notification by first-class mail, and the individual does not exercise this choice"
- If 10 or more individuals contact information is out of date, substitute notice shall be given by
  - Conspicuous posting for 90 days on the home page of the website, or
  - Major print or broadcast media in areas where individuals affected by breach are likely to reside
- In urgent situations when there is possible imminent misuse of unsecured PHR identifiable information, in addition to normal notifications, contact may be made by telephone and other means

Note: To opt out of mail notice individual has to intentionally chose email as preference

Title 16 of the *Code of Federal Regulations* Part 318.5

7. Notice to Media and FTC

- State and local media to be notified if breach involves more than 500 records
  - Includes if reasonable belief of breach
- FTC notification
  - All breaches of less than 500 records must be logged and reported annually
  - Breaches for 500 records or more require
    - Notice to FTC as soon as possible
    - 10 days is the maximum time to notify

Note: Breaches of secured data do not require notification

Title 16 of the Code of Federal Regulations Part 318.5

27

8. Content of Notice

Notice shall include in plain language:

A. Description of what happened
   - Includes: date of the breach and date of the discovery of the breach

B. Description of the types of unsecured PHR identifiable health information that were involved in the breach
   - For example: full name, social security number, date of birth, home address, account number, or disability code

C. Steps individuals should take to protect themselves

D. Description of actions taken to investigate, mitigate harm, and protect against any further breaches; and

E. Contact procedures
   - Includes: a toll-free telephone number, an email address, website, or postal address.

Title 16 of the *Code of Federal Regulations* Part 318.6

28

9. Miscellaneous Provisions: Enforcement and Effective Date

- Enforcement: Violation of FTC regulations are treated as "unfair or deceptive practice"
- Effective date: Late September 2009

Title 16 of the *Code of Federal Regulations* Part 318.7 and 318.8

29

Additional Health Information Regulations Pursuant to the HITECH Act

- Extending security rule applied to HIPAA Business Associates
  - Will define uses and disclosures of protected health information for business associates of HIPAA-covered entities
  - Will be similar to protections for HIPAA-covered entities
- Prohibited sale of electronic health information and allowed exceptions
  - Generally prohibits exchanging health information for remuneration without the individual's authorization

30

094032201

SENATE BILL NO. 1229

Offered January 14, 2009

Prefiled January 13, 2009

A BILL to amend and reenact §§ 18.2-186.6 and 32.1-127.1:03 of the Code of Virginia, relating to privacy of medical information; penalty.

Patron—Barker

Referred to Committee for Courts of Justice

Be it enacted by the General Assembly of Virginia:

1. That §§ 18.2-186.6 and 32.1-127.1:03 of the Code of Virginia are amended and reenacted as follows:

§ 18.2-186.6. Breach of personal information notification.

A. As used in this section:

"Breach of the security of the system" means the unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes, or the individual or entity reasonably believes has caused, or will cause, identity theft or other fraud to any resident of the Commonwealth. Good faith acquisition of personal 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 personal 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.

"Financial institution" has the meaning given that term in 15 U.S.C. § 6809(3).

"Health insurance information" means 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.

"Individual" means a natural person.

"Medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

"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 all 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 not be considered a debt communication as defined by the Fair Debt Collection Practices Act in 15 U.S.C. § 1692a.

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

(1) The incident in general terms;

(2) The type of personal 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;

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

(5) Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.

"Personal 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. Social security number;

2. Driver's license number or state identification card number issued in lieu of a driver's license number; ~~or~~

3. Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts~~.~~*;*

4. Medical information; or

5. Health insurance information.

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.

"Redact" means alteration or truncation of data such that no more than the following are accessible as part of the personal information:

1. Five digits of a social security number; or

2. The last four digits of a driver's license number, state identification card number, or account number.

B. If unencrypted or unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and causes, or the individual or entity reasonably believes has caused or will cause, identity theft or another fraud to any resident of the Commonwealth, an individual or entity that owns or licenses computerized data that includes personal 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 and the individual or entity reasonably believes that such a breach has caused or will cause identity theft or other fraud to any resident of the Commonwealth.

D. An individual or entity that maintains computerized data that includes personal 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 personal information was accessed and acquired by an unauthorized person or the individual or entity reasonably believes the personal 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 and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. § 1681(a)(p), of the timing, distribution, and content of the notice.

F. An entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information that are consistent with the timing requirements of this section shall be deemed to be in compliance with the notification requirements of this section if it notifies residents of the Commonwealth in accordance with its procedures in the event of a breach of the security of the system.

G. An entity that is subject to Title V of the Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq.) and maintains procedures for notification of a breach of the security of the system in accordance with the provision of that Act and any rules, regulations, or guidelines promulgated thereto shall be deemed to be in compliance with this section.

H. An entity that complies with the notification requirements or procedures pursuant to the rules, regulations, procedures, or guidelines established by the entity's primary or functional state or federal

regulator shall be in compliance with this section.

I. Except as provided by subsections J and K, 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 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.

J. A violation of this section by a state-chartered or licensed financial institution shall be enforceable exclusively by the financial institution's primary state regulator.

K. A violation of this section by an individual or entity regulated by the State Corporation Commission's Bureau of Insurance shall be enforced exclusively by the State Corporation Commission.

L. The provisions of this section shall not apply to criminal intelligence systems subject to the restrictions of 28 C.F.R. Part 23 that are maintained by law-enforcement agencies of the Commonwealth and the organized Criminal Gang File of the Virginia Criminal Information Network (VCIN), established pursuant to Chapter 2 (§ 52-12 et seq.) of Title 52.

§ 32.1-127.1:03. Health records privacy.

A. There is hereby recognized an individual's right of privacy in the content of his health records. Health records are the property of the health care entity maintaining them, and, except when permitted or required by this section or by other provisions of state law, no health care entity, or other person working in a health care setting, may disclose an individual's health records.

Pursuant to this subsection:

1. Health care entities shall disclose health records to the individual who is the subject of the health record, except as provided in subsections E and F of this section and subsection B of § 8.01-413.

2. Health records shall not be removed from the premises where they are maintained without the approval of the health care entity that maintains such health records, except in accordance with a court order or subpoena consistent with subsection C of § 8.01-413 or with this section or in accordance with the regulations relating to change of ownership of health records promulgated by a health regulatory board established in Title 54.1.

3. No person to whom health records are disclosed shall redisclose or otherwise reveal the health records of an individual, beyond the purpose for which such disclosure was made, without first obtaining the individual's specific authorization to such redisclosure. This redisclosure prohibition shall not, however, prevent (i) any health care entity that receives health records from another health care entity from making subsequent disclosures as permitted under this section and the federal Department of Health and Human Services regulations relating to privacy of the electronic transmission of data and protected health information promulgated by the United States Department of Health and Human Services as required by the Health Insurance Portability and Accountability Act (HIPAA) (42 U.S.C. § 1320d et seq.) or (ii) any health care entity from furnishing health records and aggregate or other data, from which individually identifying prescription information has been removed, encoded or encrypted, to qualified researchers, including, but not limited to, pharmaceutical manufacturers and their agents or contractors, for purposes of clinical, pharmaco-epidemiological, pharmaco-economic, or other health services research.

B. As used in this section:

"Agent" means a person who has been appointed as an individual's agent under a power of attorney for health care or an advance directive under the Health Care Decisions Act (§ 54.1-2981 et seq.).

"Certification" means a written representation that is delivered by hand, by first-class mail, by overnight delivery service, or by facsimile if the sender obtains a facsimile-machine-generated confirmation reflecting that all facsimile pages were successfully transmitted.

"Guardian" means a court-appointed guardian of the person.

"Health care clearinghouse" means, consistent with the definition set out in 45 C.F.R. § 160.103, a public or private entity, such as a billing service, repricing company, community health management information system or community health information system, and "value-added" networks and switches, that performs either of the following functions: (i) processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction; or (ii) receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

"Health care entity" means any health care provider, health plan or health care clearinghouse.

"Health care provider" means those entities listed in the definition of "health care provider" in § 8.01-581.1, except that state-operated facilities shall also be considered health care providers for the purposes of this section. Health care provider shall also include *(i)* all persons who are licensed, certified, registered or permitted or who hold a multistate licensure privilege issued by any of the health

regulatory boards within the Department of Health Professions, except persons regulated by the Board of Funeral Directors and Embalmers or the Board of Veterinary Medicine *and (ii) any corporation organized for the primary purpose of maintaining medical information in order to make the information available to an individual, or to a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage his information, or for the diagnosis and treatment of the individual.*

"Health plan" means an individual or group plan that provides, or pays the cost of, medical care. "Health plan" shall include any entity included in such definition as set out in 45 C.F.R. § 160.103.

"Health record" means any written, printed or electronically recorded material maintained by a health care entity in the course of providing health services to an individual concerning the individual and the services provided. "Health record" also includes the substance of any communication made by an individual to a health care entity in confidence during or in connection with the provision of health services or information otherwise acquired by the health care entity about an individual in confidence and in connection with the provision of health services to the individual.

"Health services" means, but shall not be limited to, examination, diagnosis, evaluation, treatment, pharmaceuticals, aftercare, habilitation or rehabilitation and mental health therapy of any kind, as well as payment or reimbursement for any such services.

"Individual" means a patient who is receiving or has received health services from a health care entity.

"Individually identifying prescription information" means all prescriptions, drug orders or any other prescription information that specifically identifies an individual.

"Parent" means a biological, adoptive or foster parent.

"Psychotherapy notes" means comments, recorded in any medium by a health care provider who is a mental health professional, documenting or analyzing the contents of conversation during a private counseling session with an individual or a group, joint, or family counseling session that are separated from the rest of the individual's health record. "Psychotherapy notes" shall not include annotations relating to medication and prescription monitoring, counseling session start and stop times, treatment modalities and frequencies, clinical test results, or any summary of any symptoms, diagnosis, prognosis, functional status, treatment plan, or the individual's progress to date.

C. The provisions of this section shall not apply to any of the following:

1. The status of and release of information governed by §§ 65.2-604 and 65.2-607 of the Virginia Workers' Compensation Act;

2. Except where specifically provided herein, the health records of minors; or

3. The release of juvenile health records to a secure facility or a shelter care facility pursuant to § 16.1-248.3.

D. Health care entities may, and, when required by other provisions of state law, shall, disclose health records:

1. As set forth in subsection E, pursuant to the written authorization of (i) the individual or (ii) in the case of a minor, (a) his custodial parent, guardian or other person authorized to consent to treatment of minors pursuant to § 54.1-2969 or (b) the minor himself, if he has consented to his own treatment pursuant to § 54.1-2969, or (iii) in emergency cases or situations where it is impractical to obtain an individual's written authorization, pursuant to the individual's oral authorization for a health care provider or health plan to discuss the individual's health records with a third party specified by the individual;

2. In compliance with a subpoena issued in accord with subsection H, pursuant to a search warrant or a grand jury subpoena, pursuant to court order upon good cause shown or in compliance with a subpoena issued pursuant to subsection C of § 8.01-413. Regardless of the manner by which health records relating to an individual are compelled to be disclosed pursuant to this subdivision, nothing in this subdivision shall be construed to prohibit any staff or employee of a health care entity from providing information about such individual to a law-enforcement officer in connection with such subpoena, search warrant, or court order;

3. In accord with subsection F of § 8.01-399 including, but not limited to, situations where disclosure is reasonably necessary to establish or collect a fee or to defend a health care entity or the health care entity's employees or staff against any accusation of wrongful conduct; also as required in the course of an investigation, audit, review or proceedings regarding a health care entity's conduct by a duly authorized law-enforcement, licensure, accreditation, or professional review entity;

4. In testimony in accordance with §§ 8.01-399 and 8.01-400.2;

5. In compliance with the provisions of § 8.01-413;

6. As required or authorized by law relating to public health activities, health oversight activities, serious threats to health or safety, or abuse, neglect or domestic violence, relating to contagious disease, public safety, and suspected child or adult abuse reporting requirements, including, but not limited to, those contained in §§ 32.1-36, 32.1-36.1, 32.1-40, 32.1-41, 32.1-127.1:04, 32.1-276.5, 32.1-283,

32.1-283.1, 37.2-710, 37.2-839, 53.1-40.10, 54.1-2400.6, 54.1-2400.7, 54.1-2403.3, 54.1-2506, 54.1-2966, 54.1-2966.1, 54.1-2967, 54.1-2968, 63.2-1509, and 63.2-1606;

7. Where necessary in connection with the care of the individual;

8. In connection with the health care entity's own health care operations or the health care operations of another health care entity, as specified in 45 C.F.R. § 164.501, or in the normal course of business in accordance with accepted standards of practice within the health services setting; however, the maintenance, storage, and disclosure of the mass of prescription dispensing records maintained in a pharmacy registered or permitted in Virginia shall only be accomplished in compliance with §§ 54.1-3410, 54.1-3411, and 54.1-3412;

9. When the individual has waived his right to the privacy of the health records;

10. When examination and evaluation of an individual are undertaken pursuant to judicial or administrative law order, but only to the extent as required by such order;

11. To the guardian ad litem and any attorney representing the respondent in the course of a guardianship proceeding of an adult patient who is the respondent in a proceeding under Chapter 10 (§ 37.2-1000 et seq.) of Title 37.2;

12. To the guardian ad litem and any attorney appointed by the court to represent an individual who is or has been a patient who is the subject of a commitment proceeding under § 19.2-169.6, 19.2-176, or 19.2-177.1, Article 5 (§ 37.2-814 et seq.) of Chapter 8 of Title 37.2, Article 16 (§ 16.1-335 et seq.) of Chapter 11 of Title 16.1, or a judicial authorization for treatment proceeding pursuant to Chapter 11 (§ 37.2-1100 et seq.) of Title 37.2;

13. To a magistrate, the court, the evaluator or examiner required under § 16.1-338, 16.1-339, 16.1-342, or 37.2-815, a community services board or behavioral health authority or a designee of a community services board or behavioral health authority, or a law-enforcement officer participating in any proceeding under Article 16 (§ 16.1-335 et seq.) of Chapter 11 of Title 16.1, § 19.2-169.6, 19.2-176, or 19.2-177.1, or Chapter 8 (§ 37.2-800 et seq.) of Title 37.2 regarding the subject of the proceeding, and to any health care provider evaluating or providing services to the person who is the subject of the proceeding or monitoring the person's adherence to a treatment plan ordered under those provisions. Health records disclosed to a law-enforcement officer shall be limited to information necessary to protect the officer, the person, or the public from physical injury or to address the health care needs of the person. Information disclosed to a law-enforcement officer shall not be used for any other purpose, disclosed to others, or retained;

14. To the attorney and/or guardian ad litem of a minor who represents such minor in any judicial or administrative proceeding, if the court or administrative hearing officer has entered an order granting the attorney or guardian ad litem this right and such attorney or guardian ad litem presents evidence to the health care entity of such order;

15. With regard to the Court-Appointed Special Advocate (CASA) program, a minor's health records in accord with § 9.1-156;

16. To an agent appointed under an individual's power of attorney or to an agent or decision maker designated in an individual's advance directive for health care or for decisions on anatomical gifts and organ, tissue or eye donation or to any other person consistent with the provisions of the Health Care Decisions Act (§ 54.1-2981 et seq.);

17. To third-party payors and their agents for purposes of reimbursement;

18. As is necessary to support an application for receipt of health care benefits from a governmental agency or as required by an authorized governmental agency reviewing such application or reviewing benefits already provided or as necessary to the coordination of prevention and control of disease, injury, or disability and delivery of such health care benefits pursuant to § 32.1-127.1:04;

19. Upon the sale of a medical practice as provided in § 54.1-2405; or upon a change of ownership or closing of a pharmacy pursuant to regulations of the Board of Pharmacy;

20. In accord with subsection B of § 54.1-2400.1, to communicate an individual's specific and immediate threat to cause serious bodily injury or death of an identified or readily identifiable person;

21. Where necessary in connection with the implementation of a hospital's routine contact process for organ donation pursuant to subdivision B 4 of § 32.1-127;

22. In the case of substance abuse records, when permitted by and in conformity with requirements of federal law found in 42 U.S.C. § 290dd-2 and 42 C.F.R. Part 2;

23. In connection with the work of any entity established as set forth in § 8.01-581.16 to evaluate the adequacy or quality of professional services or the competency and qualifications for professional staff privileges;

24. If the health records are those of a deceased or mentally incapacitated individual to the personal representative or executor of the deceased individual or the legal guardian or committee of the incompetent or incapacitated individual or if there is no personal representative, executor, legal guardian or committee appointed, to the following persons in the following order of priority: a spouse, an adult

son or daughter, either parent, an adult brother or sister, or any other relative of the deceased individual in order of blood relationship;

25. For the purpose of conducting record reviews of inpatient hospital deaths to promote identification of all potential organ, eye, and tissue donors in conformance with the requirements of applicable federal law and regulations, including 42 C.F.R. § 482.45, (i) to the health care provider's designated organ procurement organization certified by the United States Health Care Financing Administration and (ii) to any eye bank or tissue bank in Virginia certified by the Eye Bank Association of America or the American Association of Tissue Banks;

26. To the Office of the Inspector General for Mental Health, Mental Retardation and Substance Abuse Services pursuant to Article 3 (§ 37.2-423 et seq.) of Chapter 4 of Title 37.2;

27. To an entity participating in the activities of a local health partnership authority established pursuant to Article 6.1 (§ 32.1-122.10:001 et seq.) of Chapter 4 of this title, pursuant to subdivision 1 of this subsection;

28. To law-enforcement officials by each licensed emergency medical services agency, (i) when the individual is the victim of a crime or (ii) when the individual has been arrested and has received emergency medical services or has refused emergency medical services and the health records consist of the prehospital patient care report required by § 32.1-116.1;

29. To law-enforcement officials, in response to their request, for the purpose of identifying or locating a suspect, fugitive, person required to register pursuant to § 9.1-901 of the Sex Offender and Crimes Against Minors Registry Act, material witness, or missing person, provided that only the following information may be disclosed: (i) name and address of the person, (ii) date and place of birth of the person, (iii) social security number of the person, (iv) blood type of the person, (v) date and time of treatment received by the person, (vi) date and time of death of the person, where applicable, (vii) description of distinguishing physical characteristics of the person, and (viii) type of injury sustained by the person;

30. To law-enforcement officials regarding the death of an individual for the purpose of alerting law enforcement of the death if the health care entity has a suspicion that such death may have resulted from criminal conduct;

31. To law-enforcement officials if the health care entity believes in good faith that the information disclosed constitutes evidence of a crime that occurred on its premises;

32. To the State Health Commissioner pursuant to § 32.1-48.015 when such records are those of a person or persons who are subject to an order of quarantine or an order of isolation pursuant to Article 3.02 (§ 32.1-48.05 et seq.) of Chapter 2 of this title; and

33. To the Commissioner of the Department of Labor and Industry or his designee by each licensed emergency medical services agency when the records consist of the prehospital patient care report required by § 32.1-116.1 and the patient has suffered an injury or death on a work site while performing duties or tasks that are within the scope of his employment.

Notwithstanding the provisions of subdivisions 1 through 33 of this subsection, a health care entity shall obtain an individual's written authorization for any disclosure of psychotherapy notes, except when disclosure by the health care entity is (i) for its own training programs in which students, trainees, or practitioners in mental health are being taught under supervision to practice or to improve their skills in group, joint, family, or individual counseling; (ii) to defend itself or its employees or staff against any accusation of wrongful conduct; (iii) in the discharge of the duty, in accordance with subsection B of § 54.1-2400.1, to take precautions to protect third parties from violent behavior or other serious harm; (iv) required in the course of an investigation, audit, review, or proceeding regarding a health care entity's conduct by a duly authorized law-enforcement, licensure, accreditation, or professional review entity; or (v) otherwise required by law.

E. Requests for copies of health records shall (i) be in writing, dated and signed by the requester; (ii) identify the nature of the information requested; and (iii) include evidence of the authority of the requester to receive such copies and identification of the person to whom the information is to be disclosed. The health care entity shall accept a photocopy, facsimile, or other copy of the original signed by the requestor as if it were an original. Within 15 days of receipt of a request for copies of health records, the health care entity shall do one of the following: (i) furnish such copies to any requester authorized to receive them; (ii) inform the requester if the information does not exist or cannot be found; (iii) if the health care entity does not maintain a record of the information, so inform the requester and provide the name and address, if known, of the health care entity who maintains the record; or (iv) deny the request (a) under subsection F, (b) on the grounds that the requester has not established his authority to receive such health records or proof of his identity, or (c) as otherwise provided by law. Procedures set forth in this section shall apply only to requests for health records not specifically governed by other provisions of state law.

F. Except as provided in subsection B of § 8.01-413, copies of an individual's health records shall not be furnished to such individual or anyone authorized to act on the individual's behalf when the

individual's treating physician or the individual's treating clinical psychologist has made a part of the individual's record a written statement that, in the exercise of his professional judgment, the furnishing to or review by the individual of such health records would be reasonably likely to endanger the life or physical safety of the individual or another person, or that such health record makes reference to a person other than a health care provider and the access requested would be reasonably likely to cause substantial harm to such referenced person. If any health care entity denies a request for copies of health records based on such statement, the health care entity shall inform the individual of the individual's right to designate, in writing, at his own expense, another reviewing physician or clinical psychologist, whose licensure, training and experience relative to the individual's condition are at least equivalent to that of the physician or clinical psychologist upon whose opinion the denial is based. The designated reviewing physician or clinical psychologist shall make a judgment as to whether to make the health record available to the individual.

The health care entity denying the request shall also inform the individual of the individual's right to request in writing that such health care entity designate, at its own expense, a physician or clinical psychologist, whose licensure, training, and experience relative to the individual's condition are at least equivalent to that of the physician or clinical psychologist upon whose professional judgment the denial is based and who did not participate in the original decision to deny the health records, who shall make a judgment as to whether to make the health record available to the individual. The health care entity shall comply with the judgment of the reviewing physician or clinical psychologist. The health care entity shall permit copying and examination of the health record by such other physician or clinical psychologist designated by either the individual at his own expense or by the health care entity at its expense.

Any health record copied for review by any such designated physician or clinical psychologist shall be accompanied by a statement from the custodian of the health record that the individual's treating physician or clinical psychologist determined that the individual's review of his health record would be reasonably likely to endanger the life or physical safety of the individual or would be reasonably likely to cause substantial harm to a person referenced in the health record who is not a health care provider.

Further, nothing herein shall be construed as giving, or interpreted to bestow the right to receive copies of, or otherwise obtain access to, psychotherapy notes to any individual or any person authorized to act on his behalf.

G. A written authorization to allow release of an individual's health records shall substantially include the following information:

AUTHORIZATION TO RELEASE CONFIDENTIAL HEALTH
RECORDS
Individual's Name .....
Health Care Entity's Name .....
Person, Agency, or Health Care Entity to whom disclosure is to
be made .....
Information or Health Records to be disclosed .....
Purpose of Disclosure or at the Request of the Individual .....
As the person signing this authorization, I understand that I am giving my
permission to the above-named health care entity for disclosure of
confidential health records. I understand that the health care entity may not
condition treatment or payment on my willingness to sign this authorization
unless the specific circumstances under which such conditioning is permitted
by law are applicable and are set forth in this authorization. I also
understand that I have the right to revoke this authorization at any time,
but that my revocation is not effective until delivered in writing to the
person who is in possession of my health records and is not effective as to
health records already disclosed under this authorization. A copy of this
authorization and a notation concerning the persons or agencies to whom
disclosure was made shall be included with my original health records. I
understand that health information disclosed under this authorization might
be redisclosed by a recipient and may, as a result of such disclosure, no
longer be protected to the same extent as such health information was
protected by law while solely in the possession of the health care entity.
This authorization expires on (date) or (event) .....
Signature of Individual or Individual's Legal Representative if Individual is
Unable to Sign .....

Relationship or Authority of Legal Representative .....
Date of Signature .....

H. Pursuant to this subsection:

1. Unless excepted from these provisions in subdivision 9 of this subsection, no party to a civil, criminal or administrative action or proceeding shall request the issuance of a subpoena duces tecum for another party's health records or cause a subpoena duces tecum to be issued by an attorney unless a copy of the request for the subpoena or a copy of the attorney-issued subpoena is provided to the other party's counsel or to the other party if pro se, simultaneously with filing the request or issuance of the subpoena. No party to an action or proceeding shall request or cause the issuance of a subpoena duces tecum for the health records of a nonparty witness unless a copy of the request for the subpoena or a copy of the attorney-issued subpoena is provided to the nonparty witness simultaneously with filing the request or issuance of the attorney-issued subpoena.

No subpoena duces tecum for health records shall set a return date earlier than 15 days from the date of the subpoena except by order of a court or administrative agency for good cause shown. When a court or administrative agency directs that health records be disclosed pursuant to a subpoena duces tecum earlier than 15 days from the date of the subpoena, a copy of the order shall accompany the subpoena.

Any party requesting a subpoena duces tecum for health records or on whose behalf the subpoena duces tecum is being issued shall have the duty to determine whether the individual whose health records are being sought is pro se or a nonparty.

In instances where health records being subpoenaed are those of a pro se party or nonparty witness, the party requesting or issuing the subpoena shall deliver to the pro se party or nonparty witness together with the copy of the request for subpoena, or a copy of the subpoena in the case of an attorney-issued subpoena, a statement informing them of their rights and remedies. The statement shall include the following language and the heading shall be in boldface capital letters:

NOTICE TO INDIVIDUAL

The attached document means that (insert name of party requesting or causing issuance of the subpoena) has either asked the court or administrative agency to issue a subpoena or a subpoena has been issued by the other party's attorney to your doctor, other health care providers (names of health care providers inserted here) or other health care entity (name of health care entity to be inserted here) requiring them to produce your health records. Your doctor, other health care provider or other health care entity is required to respond by providing a copy of your health records. If you believe your health records should not be disclosed and object to their disclosure, you have the right to file a motion with the clerk of the court or the administrative agency to quash the subpoena. If you elect to file a motion to quash, such motion must be filed within 15 days of the date of the request or of the attorney-issued subpoena. You may contact the clerk's office or the administrative agency to determine the requirements that must be satisfied when filing a motion to quash and you may elect to contact an attorney to represent your interest. If you elect to file a motion to quash, you must notify your doctor, other health care provider(s), or other health care entity, that you are filing the motion so that the health care provider or health care entity knows to send the health records to the clerk of court or administrative agency in a sealed envelope or package for safekeeping while your motion is decided.

2. Any party filing a request for a subpoena duces tecum or causing such a subpoena to be issued for an individual's health records shall include a Notice in the same part of the request in which the recipient of the subpoena duces tecum is directed where and when to return the health records. Such notice shall be in boldface capital letters and shall include the following language:

NOTICE TO HEALTH CARE ENTITIES

A COPY OF THIS SUBPOENA DUCES TECUM HAS BEEN PROVIDED TO THE INDIVIDUAL WHOSE HEALTH RECORDS ARE BEING REQUESTED OR HIS COUNSEL. YOU OR THAT INDIVIDUAL HAS THE RIGHT TO FILE A MOTION TO QUASH (OBJECT TO) THE ATTACHED SUBPOENA. IF YOU ELECT TO FILE A MOTION TO QUASH, YOU MUST FILE THE MOTION WITHIN 15 DAYS OF THE DATE OF THIS SUBPOENA.

YOU MUST NOT RESPOND TO THIS SUBPOENA UNTIL YOU HAVE RECEIVED WRITTEN CERTIFICATION FROM THE PARTY ON WHOSE BEHALF THE SUBPOENA WAS ISSUED THAT THE TIME FOR FILING A MOTION TO QUASH HAS ELAPSED AND THAT:

NO MOTION TO QUASH WAS FILED; OR

ANY MOTION TO QUASH HAS BEEN RESOLVED BY THE COURT OR THE ADMINISTRATIVE AGENCY AND THE DISCLOSURES SOUGHT ARE CONSISTENT WITH SUCH RESOLUTION.

IF YOU RECEIVE NOTICE THAT THE INDIVIDUAL WHOSE HEALTH RECORDS ARE BEING REQUESTED HAS FILED A MOTION TO QUASH THIS SUBPOENA, OR IF YOU FILE A MOTION TO QUASH THIS SUBPOENA, YOU MUST SEND THE HEALTH RECORDS ONLY TO THE CLERK OF THE COURT OR ADMINISTRATIVE AGENCY THAT ISSUED THE SUBPOENA

OR IN WHICH THE ACTION IS PENDING AS SHOWN ON THE SUBPOENA USING THE FOLLOWING PROCEDURE:

PLACE THE HEALTH RECORDS IN A SEALED ENVELOPE AND ATTACH TO THE SEALED ENVELOPE A COVER LETTER TO THE CLERK OF COURT OR ADMINISTRATIVE AGENCY WHICH STATES THAT CONFIDENTIAL HEALTH RECORDS ARE ENCLOSED AND ARE TO BE HELD UNDER SEAL PENDING A RULING ON THE MOTION TO QUASH THE SUBPOENA. THE SEALED ENVELOPE AND THE COVER LETTER SHALL BE PLACED IN AN OUTER ENVELOPE OR PACKAGE FOR TRANSMITTAL TO THE COURT OR ADMINISTRATIVE AGENCY.

3. Upon receiving a valid subpoena duces tecum for health records, health care entities shall have the duty to respond to the subpoena in accordance with the provisions of subdivisions 4, 5, 6, 7, and 8 of this subsection.

4. Except to deliver to a clerk of the court or administrative agency subpoenaed health records in a sealed envelope as set forth, health care entities shall not respond to a subpoena duces tecum for such health records until they have received a certification as set forth in subdivision 5 or 8 of this subsection from the party on whose behalf the subpoena duces tecum was issued.

If the health care entity has actual receipt of notice that a motion to quash the subpoena has been filed or if the health care entity files a motion to quash the subpoena for health records, then the health care entity shall produce the health records, in a securely sealed envelope, to the clerk of the court or administrative agency issuing the subpoena or in whose court or administrative agency the action is pending. The court or administrative agency shall place the health records under seal until a determination is made regarding the motion to quash. The securely sealed envelope shall only be opened on order of the judge or administrative agency. In the event the court or administrative agency grants the motion to quash, the health records shall be returned to the health care entity in the same sealed envelope in which they were delivered to the court or administrative agency. In the event that a judge or administrative agency orders the sealed envelope to be opened to review the health records in camera, a copy of the order shall accompany any health records returned to the health care entity. The health records returned to the health care entity shall be in a securely sealed envelope.

5. If no motion to quash is filed within 15 days of the date of the request or of the attorney-issued subpoena, the party on whose behalf the subpoena was issued shall have the duty to certify to the subpoenaed health care entity that the time for filing a motion to quash has elapsed and that no motion to quash was filed. Any health care entity receiving such certification shall have the duty to comply with the subpoena duces tecum by returning the specified health records by either the return date on the subpoena or five days after receipt of the certification, whichever is later.

6. In the event that the individual whose health records are being sought files a motion to quash the subpoena, the court or administrative agency shall decide whether good cause has been shown by the discovering party to compel disclosure of the individual's health records over the individual's objections. In determining whether good cause has been shown, the court or administrative agency shall consider (i) the particular purpose for which the information was collected; (ii) the degree to which the disclosure of the records would embarrass, injure, or invade the privacy of the individual; (iii) the effect of the disclosure on the individual's future health care; (iv) the importance of the information to the lawsuit or proceeding; and (v) any other relevant factor.

7. Concurrent with the court or administrative agency's resolution of a motion to quash, if subpoenaed health records have been submitted by a health care entity to the court or administrative agency in a sealed envelope, the court or administrative agency shall: (i) upon determining that no submitted health records should be disclosed, return all submitted health records to the health care entity in a sealed envelope; (ii) upon determining that all submitted health records should be disclosed, provide all the submitted health records to the party on whose behalf the subpoena was issued; or (iii) upon determining that only a portion of the submitted health records should be disclosed, provide such portion to the party on whose behalf the subpoena was issued and return the remaining health records to the health care entity in a sealed envelope.

8. Following the court or administrative agency's resolution of a motion to quash, the party on whose behalf the subpoena duces tecum was issued shall have the duty to certify in writing to the subpoenaed health care entity a statement of one of the following:

a. All filed motions to quash have been resolved by the court or administrative agency and the disclosures sought in the subpoena duces tecum are consistent with such resolution; and, therefore, the health records previously delivered in a sealed envelope to the clerk of the court or administrative agency will not be returned to the health care entity;

b. All filed motions to quash have been resolved by the court or administrative agency and the disclosures sought in the subpoena duces tecum are consistent with such resolution and that, since no health records have previously been delivered to the court or administrative agency by the health care

entity, the health care entity shall comply with the subpoena duces tecum by returning the health records designated in the subpoena by the return date on the subpoena or five days after receipt of certification, whichever is later;

c. All filed motions to quash have been resolved by the court or administrative agency and the disclosures sought in the subpoena duces tecum are not consistent with such resolution; therefore, no health records shall be disclosed and all health records previously delivered in a sealed envelope to the clerk of the court or administrative agency will be returned to the health care entity;

d. All filed motions to quash have been resolved by the court or administrative agency and the disclosures sought in the subpoena duces tecum are not consistent with such resolution and that only limited disclosure has been authorized. The certification shall state that only the portion of the health records as set forth in the certification, consistent with the court or administrative agency's ruling, shall be disclosed. The certification shall also state that health records that were previously delivered to the court or administrative agency for which disclosure has been authorized will not be returned to the health care entity; however, all health records for which disclosure has not been authorized will be returned to the health care entity; or

e. All filed motions to quash have been resolved by the court or administrative agency and the disclosures sought in the subpoena duces tecum are not consistent with such resolution and, since no health records have previously been delivered to the court or administrative agency by the health care entity, the health care entity shall return only those health records specified in the certification, consistent with the court or administrative agency's ruling, by the return date on the subpoena or five days after receipt of the certification, whichever is later.

A copy of the court or administrative agency's ruling shall accompany any certification made pursuant to this subdivision.

9. The provisions of this subsection have no application to subpoenas for health records requested under § 8.01-413, or issued by a duly authorized administrative agency conducting an investigation, audit, review or proceedings regarding a health care entity's conduct.

The provisions of this subsection shall apply to subpoenas for the health records of both minors and adults.

Nothing in this subsection shall have any effect on the existing authority of a court or administrative agency to issue a protective order regarding health records, including, but not limited to, ordering the return of health records to a health care entity, after the period for filing a motion to quash has passed.

A subpoena for substance abuse records must conform to the requirements of federal law found in 42 C.F.R. Part 2, Subpart E.

I. Health care entities may testify about the health records of an individual in compliance with §§ 8.01-399 and 8.01-400.2.

J. If an individual requests a copy of his health record from a health care entity, the health care entity may impose a reasonable cost-based fee, which shall include only the cost of supplies for and labor of copying the requested information, postage when the individual requests that such information be mailed, and preparation of an explanation or summary of such information as agreed to by the individual. For the purposes of this section, "individual" shall subsume a person with authority to act on behalf of the individual who is the subject of the health record in making decisions related to his health care.

COMMONWEALTH OF VIRGINIA

SUSAN CLARKE SCHAAR
CLERK OF THE SENATE
P.O. BOX 396
RICHMOND, VIRGINIA 23218

SENATE

March 20, 2009

Ms. Kim Snead, Executive Director
Joint Commission on Health Care
900 E. Main Street, 1st Floor West
P.O. Box 1322
Richmond, Virginia 23219

Dear Ms. Snead: Kim

This is to inform you that, pursuant to Rule 20 (l) of the Rules of the Senate of Virginia, the subject matter contained in Senate Bill 1229 has been referred by the Senate Committee for Courts of Justice to the Joint Commission on Health Care for study. It is requested that the appropriate committee chair and bill patron receive a written report, with a copy to this office, by November 2, 2009.

With kind regards, I am

Sincerely yours,

Susan Clarke Schaar

SCS:jdm

cc: Sen. R. Edward Houck, Chair, Joint Commission on Health Care
Sen. Henry L. Marsh, III, Chair, Senate Committee for Courts of Justice
Sen. Sen. George L. Barker, Patron of SB 1229

Joint Commission on Health Care
900 East Main Street, 1st Floor West
P. O. Box 1322
Richmond, VA 23218
804.786.5445
804.786.5538 (fax)

Website: http://jchc.virginia.gov