

**Comments of Virginia Hospital & Healthcare Association to the
Privacy Advisory Committee of the
Joint Commission on Technology and Science
August 3, 2005**

The Virginia Hospital & Healthcare Association appreciates the opportunity to address the committee as it considers requirements for notification of database breaches (HB 2721 – 2005). We will describe for you the existing privacy and security protections provided under federal and state law, which we believe more than adequately protect electronic health records maintained by hospitals and other institutional and individual health care providers.

The “Administrative Simplification” provisions of the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) were enacted in part to protect the privacy and security of individually identifiable “protected health information” (PHI) while promoting electronic health information management and its many advantages. HIPAA imposes extensive requirements on “covered entities,” which include (i) all providers of medical or other health care services or supplies that transmits any health information in electronic form, (ii) health plans, (ii) health care clearinghouses that process another entity’s health care transactions, and (iv) Medicare prescription drug sponsors.

The two sections of the law that address the issues before the Privacy Advisory Committee are the “**privacy rule**,” with which “covered entities” have complied since April 2003, and the “**security rule**,” which has been enforced since April 2005. Generally, the **privacy rule** includes standards for who may have access to PHI while the **security rule** sets standards to ensure that only those individuals actually have access to such information.

Privacy Provisions

The **privacy rule** sets forth the rights of individuals with respect to their PHI, procedures for the exercise of those rights and the authorized and required uses and disclosures of PHI, including the following:

- **Access To Medical Records.** Patients generally may see and obtain copies of their medical records and request corrections if they identify errors and mistakes.
- **Notice of Privacy Practices.** Covered entities must provide a notice to their patients about how they may use personal medical information and their rights under the new privacy regulation, including the process for filing complaints.
- **Limits on Use of Personal Medical Information.** To promote the best quality care for patients, the rule does not restrict the ability of doctors, nurses and other providers to share information needed to treat their patients. In other situations, though, personal health information generally may not be used for purposes not related to health care, and covered entities may use or share only the minimum amount of

protected information needed for a particular purpose. In addition, patients must sign a specific authorization before a covered entity may release their medical information to a life insurer, a bank, a marketing firm or another outside business for purposes not related to their health care.

- **Prohibition on Marketing.** The final privacy rule sets new restrictions and limits on the use of patient information for marketing purposes.
- **Right to an Accounting of Disclosures.** At the individual's request, the entity must provide details of disclosures of PHI that occurred up to 6 years prior to the date of the request.
- **Confidential communications.** Under the privacy rule, patients can request that their doctors, health plans and other covered entities take reasonable steps to ensure that their communications with the patient are confidential. For example, a patient could ask a doctor to call his or her office rather than home, and the doctor's office should comply with that request if it can be reasonably accommodated.
- **Complaints.** Consumers may file a formal complaint regarding the privacy practices of a covered entity. Complaints can be made directly to the covered provider or health plan or to HHS' Office for Civil Rights (OCR), which is charged with investigating complaints and enforcing the privacy regulation.

These federal privacy protections are in addition to protections provided under state law, primarily in § 32.1-127.1:03. HIPAA preemption provisions ensure that state privacy laws are preempted only to the degree that they are less stringent than federal law in their privacy protections.

Security Provisions

The HIPAA **security standards** are divided into 3 categories – administrative, physical and technical safeguards – that require covered entities to take the actions listed below:

Administrative safeguards require:

- Assignment or delegations of security responsibility to an individual and security training requirements
- Limits on who has access to information
- Analysis and management of potential risks and vulnerabilities to confidentiality and integrity of PHI
- Use of audit logs and security incident tracking systems
- Protection from malicious software
- Security incident procedures that identify and respond to suspected or known security breaches, mitigate harmful effects of known security incidents and document incidents and their outcomes
- Procedures for recovering PHI access during an emergency such as a power outage

Physical safeguards require:

- Limits on physical access to facilities where information systems are housed to protect electronic systems, equipment and the data they hold from threats, environmental hazards and unauthorized intrusion.
- Protection of workstations that access PHI to restrict unauthorized users
- Control of movement of hardware and media containing PHI into and out of a facility

Technical safeguards require:

- Automated processes to protect data and control access to data such as authentication controls and data encryption
- Hardware and software that audits activity in the information system
- Electronic mechanisms to protect PHI from alteration or destruction

Covered entities not only are required to implement the foregoing privacy and security measures with respect to their own operations, but they also must execute contracts with their external business associates, such as software vendors or records copying services, that perform functions on the covered entities' behalf that involve the use or disclosure of PHI. Through these contracts, the covered entity assures that the business associate will implement safeguards to protect PHI. If the business entity does not meet its obligations under the contract, the covered entity must take steps to cure the breach, terminate the contract, or report a violation to Centers for Medicare & Medicaid Services (CMS), the enforcement authority.

Enforcement – Civil and Criminal Penalties

For civil violations of the HIPAA standards, monetary penalties may be imposed up to \$100 per violation, to a maximum of \$25,000 per year, for each requirement or prohibition violated. Criminal penalties apply for certain actions such as knowingly obtaining protected health information in violation of the law. Criminal penalties can range up to \$50,000 and one year in prison for certain offenses; up to \$100,000 and up to five years in prison if the offenses are committed under "false pretenses"; and up to \$250,000 and up to 10 years in prison if the offenses are committed with the intent to sell, transfer or use protected health information for commercial advantage, personal gain or malicious harm.