

New and Existing Privacy Laws are a Trap for the Unwary.....

Christie Lyman Dowling, Esquire

Bean, Kinney & Korman, P.C.

"Last year, we proposed to protect every citizen's medical record. This year we will finalize those rules."

President William Jefferson Clinton,
State of the Union Address,
January 27, 2000.

The federal government is on the verge of issuing wide-ranging regulations on the handling and treatment of patient health information. A final regulation was due from the Department of Health and Human Services ("HHS") on February 17, 2000, but because of the overwhelming number of comments received, more than 53,000, the date of issuance has been postponed indefinitely. It would appear that in the spirit of compromise, HHS managed to achieve a result with which no one is satisfied.

For many years now, there have been efforts to pass comprehensive Federal legislation governing the privacy of all medical records in the nation. No such overarching legislation has passed, but new regulations governing health care providers and health plans are on the way. See 64 Fed. Reg. 59918 (1999) (proposed Nov. 3, 1999) (the "Proposed Rule or Regulations"). HHS (the Department responsible for proposing these regulations) has estimated that for the first year these rules are in effect the impact on the national economy will be more than one billion dollars and, further, the cost of compliance will be nearly four billion dollars in the first five years. Blue Cross Blue Shield has its own estimate: \$40 billion over five years for health plans alone! "Medical Privacy Rules Debated," Associated Press, February 17, 2000.

Once the final rule is issued, health care providers from doctors to dentists to psychotherapists and clinical social workers will have two years to come into compliance before the federal penalties kick in. While Virginia already has a relatively comprehensive set of statutes governing medical records, the Proposed Regulations include additional requirements for providers and health plans, and to the extent they are more protective

than existing state law, will impose new burdens.

VIRGINIA PROVIDERS MUST COME INTO COMPLIANCE

This bark may include a painful bite for Virginia providers in particular. The Proposed Regulations do not include a private right of action for individuals who believe that their privacy rights have been violated, and although the rule sets up a complaint procedure, HHS has not designated any federal office or department to deal with such claims. This should provide little comfort for Virginia providers.

The Virginia Supreme Court has already held that a patient in Virginia has a private right to sue for damages in tort, including purely emotional harm, where a provider makes an unauthorized disclosure of the patient's medical records. *Fairfax Hospital, by and through, Inova Health System Hospitals, Inc. v. Patricia Curtis*, 254 Va. 437 (1997). This concept was recently re-affirmed and expanded by a circuit court in connection with the computer privacy protection statutes. In *S.R. v. Inova Healthcare Services d/b/a Fairfax Hospital, et al.* 1999 WL 797192 (Va. Cir. Ct. Fairfax Cty. June 1, 1999), the court found that a cause of action against a hospital and its employees could be maintained for the unauthorized viewing in the hospital computer of the psychiatric records of a fellow employee. Virginia Code §§ 18.2-152.5 and 18.2-152.12 make the use of a computer to view personal records without authorization both a crime and actionable by recovery in tort.

Therefore, even if HHS is not gearing up to enforce their rigorous requirements, there is already a private right of action for violation of privacy in Virginia and the proposed federal regulations may provide the framework against which any provider's efforts to ensure confidentiality will be measured.

WHAT WILL PROVIDERS HAVE TO DO?

Among the affirmative duties to be leveled on

all covered entities and their business partners by the Proposed Regulations are the following:

A. Individual Authorization Form

Without obtaining an individual authorization, a provider may not use or disclose Protected Health Information ("PHI") for any purpose other than that compatible with or related to treatment, payment, health care operations or an explicit exception. A provider may not condition treatment or payment upon receipt of an individual authorization for greater use and disclosure. Proposed Rule § 164.508(a)(2)(iii). Additionally, a covered entity may not require authorization for the release of psychotherapy notes or the use of such notes by anyone but the creator thereof, nor under this subpart, may providers require authorization for research uses unrelated to treatment. Proposed Rule § 164.508(3).

An authorization for additional uses may not be in the same document as the initial authorization for or consent to treatment and payment. Proposed Rule § 164.508(b)(3). Acceptable forms of authorization are described in Proposed Rule § 164.508(c) and HHS has provided a model individual authorization. Luckily for providers already in compliance with Virginia law, this authorization is substantially similar to that described in Virginia Code § 32.1-127.1:03.

B. Notice of Information Practices

Each and every provider must prepare and distribute a Notice of Information Practices ("NIP") informing individuals of their rights under the Proposed Rule. Proposed Rule § 164.512. The NIP must set forth in plain language and sufficient detail the uses and disclosures that may be made of the individual's PHI without further authorization, and what uses and disclosures the entity makes that are required or permitted by law. Proposed Rule § 164.512(d)(1). The provider is thereafter limited to the disclosures described in the NIP, even if additional disclosures would otherwise be permitted under the Rule. Proposed Rule § 160.506(g). The NIP must also contain notification of numerous other rights and obligations set forth in the Proposed Rule. Finally, the NIP must include the name and telephone number of a contact person to whom questions may be directed. See Section D, below.

The NIP must be available upon request. Providers must also automatically provide a copy of the NIP to current patients or clients at the time of the first service delivery after the effective date of the Final Rule. Further, providers must also post a copy of the notice in a "clear and prominent location where it is reasonable to expect individuals seeking service from the provider to be able to read the notice." Proposed Rule § 164.512(e).

C. Individual Right of Access, Accounting, Amendment and Correction

1. Access

In addition to the rights of non-disclosure, the Proposed Rule creates extensive requirements for access and correction of an individual's records. An individual has a right to inspect and copy the individual's own PHI maintained by a health care provider, health plan, or the business partner of such entity. Proposed Rule § 164.514(a). This is substantially similar, but not identical to, current Virginia law, as set forth at Virginia Code § 37.1-84.1(8). A provider is further required to establish procedures to enable individuals to exercise this right including procedures for:

- (1) a means of request
- (2) a time limit for taking action on such requests (less than 30 days)
- (3) notification to individual of approval of the request and how to proceed on the request
- (4) provision of the information requested in the form requested
- (5) facilitation of the process of inspection and copying, including at the entity's discretion, a reasonable, cost-based fee for copying such information. Proposed Rule § 164.514(c)-(d).

Under Proposed Rule § 164.514(b), a covered entity may deny a request to the extent it falls into one of the following categories:

- (1) a licensed health care professional has determined that the access is reasonably likely to endanger the life or physical safety of the individual or someone else;
- (2) the information is about another person and access is likely to cause substantial harm to the other person;
- (3) the information was obtained under a promise of confidentiality from someone who is not a health care provider and the source is likely to be revealed;
- (4) in an ongoing clinical trial where the individual waived access;
- (5) the information was compiled in reasonable anticipation of or for use in a legal proceeding.

When a request is denied the provider must provide a written statement of the basis of the denial and describe how the individual may complain to the covered entity or to the Secretary. Proposed Rule § 164.514(d)(4).

2. Accounting

An individual also has a right to an accounting of disclosures that have been made by the provider. A covered entity must have procedures for giving, within 30 days of a

request, an accurate accounting, including the date, name and address of the recipient, a description of information disclosed, the purpose of the disclosure, and copies of all requests for disclosure at all times that PHI is maintained by a covered entity or business partner. Proposed Rule § 164.515

3. Correction and Amendment

The area likely to cause the most contention, administrative cost and frustration is the right of an individual to request an amendment or correction to PHI. Proposed Rule § 164.516(a)(1). A covered entity may deny such a request where it determines that the information was not created by that covered entity, would not be available for inspection or copying, or is accurate and complete. Proposed Rule § 164.516(a)(2). The covered entity must establish procedures for providing a means of requesting amendment or correction, take action within sixty (60) days on the request, and where accepted, make appropriate amendments or corrections, indicating in the record that an amendment or correction has been made. The provider must also make reasonable efforts to notify those entities identified by the individual, other entities that the covered entity knows have received the prior information and notify the individual that the covered entity is taking such steps. When a request is denied, the covered entity must provide the individual with a statement of the basis for denial, a description of how the individual may file a written statement of disagreement with the denial, and how the individual may complain. The procedures must further provide for the inclusion of any statement of disagreement with subsequent disclosure of the information.

D. Designated Privacy Official/Contact Person/Complaints

Each covered entity must designate a privacy official who is responsible for the development and implementation of the privacy policies required under the Proposed Rule. The covered entity must also designate a contact person or office responsible for receiving complaints and who is able to provide further information about the NIP. This can, but does not have to be, the same person as the privacy official. Proposed Rule § 164.518(a). A covered entity must also establish procedures for handling complaints and maintain copies of all complaints. Proposed Rule § 164.518(d)

E. Training and Sanctions for Workforce

Within two years of the effective date of a Final Rule, each covered entity must train and certify all members of its workforce who are likely to obtain access

to PHI. New workers after that date must be trained within a reasonable time after they begin working for the covered entity. The covered entity is further required to conduct additional training when it materially changes its privacy policies or procedures. Proposed Rule § 164.518(b). A covered entity must also establish and apply appropriate sanctions against employees and business partners who fail to comply with the policies and procedures related to PHI. Proposed Rule § 164.518(e)

F. Safeguards/Duty to Mitigate

A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of PHI, including procedures to reasonably verify the identity or authority of any requester of PHI. Proposed Rule § 164.518(c). A covered entity must further have procedures for mitigating the negative effects of a use or disclosure in violation of the Final Rule. Proposed Rule § 164.518(f).

F. Documentation of Policies Described Above

Compliance with and changes to all of the required policies and procedures described in the Proposed Rule must be documented and maintained by the covered entity. The Proposed Rule specifies several categories of documents that must be maintained for six years from creation. Proposed Rule § 164.520.

WHAT TO DO RIGHT NOW...

As described above, once finalized, the Proposed Regulations may become the blueprint for proving a violation of a patient's right to privacy under Virginia law. This is in addition to any mechanisms for enforcement which may be set up by HHS. Virginia already has several statutes in place detailing the limits on disclosure of medical information and the courts are ready to enforce those obligations. Within a few years, the new Federal Regulations will be enforceable as well.

Every provider must examine its current practices under existing law and begin to address how it will comply with the imminent Federal Regulations. For example:

- Review current confidentiality procedures in all departments, identify strengths and weaknesses, and existing violations and threats
- Prepare and distribute written policies as to how employees should treat patient records
- Make individual responsibility clear - know who responds to what requests and make sure

that person knows the applicable restrictions

- Train/refresh all employees with access to protected information
- Begin preparation of policies to come into compliance with the Proposed Rule
- Stay abreast of changes in law and enactment of State and Federal regulations and/or legislation

This article is meant only as an informational review and does not constitute legal advice. For assistance with bringing your practice into compliance with existing and new law, please contact the author.

Christie Lyman Dowling is an attorney practicing in Arlington, Virginia for the law firm of *Bean, Kinney & Korman, P.C.* She received her *Juris Doctor, cum laude*, from the Georgetown University Law Center and holds a *Bachelor of Science in Human Development and Family Studies* from Cornell University. Ms. Lyman Dowling has been involved in the formulation and evolution of health information privacy legislation since 1997 when she worked with the Georgetown Federal Legislation Clinic, in conjunction with the Health Privacy Project, on the drafting and analysis of the Federal Bills relating to this topic. Ms. Lyman Dowling can be contacted for further information at cdowling@beankinney.com

