

# New Rules Governing Protected Health Information: A Law Enforcement and Health Oversight Perspective

*Daniel R. Anderson<sup>1</sup>  
Senior Counsel, Healthcare Fraud  
United States Department of Justice  
Commercial Litigation Branch  
Civil Division*

## I. Introduction

On April 14, 2003, the new privacy rule ("privacy rule") governing patient health information went into effect. *See* 45 C.F.R. §§ 164.102–164.534. The privacy rule governs when and how "covered entities," defined as health care providers, health care clearinghouses, and health plans, will be permitted to disclose protected health information. It effects the Department of Justice in at least three ways. First, it will limit the disclosure of health information that can be made by DOJ components that generate medical records, such as the Bureau of Prisons and the United States Marshal Service. Second, it limits the access of the Department to patient health information in certain of its law enforcement functions. Third, the privacy rule will govern the access of the Department when conducting health oversight functions, such as investigations of fraud against the Medicare program.<sup>2</sup>

## II. Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), among

other things, authorized the Secretary of the Department of Health and Human Services (HHS) to develop and submit to Congress privacy standards for medical information, including the uses and disclosures of such information that should be authorized or required. *See* 42 U.S.C. 1320d-8; 42 U.S.C. 1320a-7c. On November 3, 1999, HHS published a notice of proposed privacy rulemaking dealing with medical privacy. *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 221, 59917 (Nov. 3, 1999) (to be codified at 45 C.F.R. pt. 160, 164). After receiving over 60,000 comments, HHS published a final privacy rule. *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 250, 82462 (Dec. 28, 2000) (to be codified at 45 C.F.R. pt. 160, 164). Proposed changes to the rule were published on March 27, 2002 in the Standards for Privacy of Individually Identifiable Health Information: Proposed Rule 67 Fed. Reg. 14776-14815 (to be codified at 45 C.F.R. pt. 160, 164), and final changes were issued in August, 2002.

Although this privacy rule lacked force and effect until April 14, 2003, healthcare providers and other covered entities were free to implement the privacy rule at any time until then. Fearing that unscrupulous providers may use early implementation of the rule as a pretext to forestall production of records in health oversight investigations, a technical correction to the privacy rule was published on December 29, 2000 that states that healthcare providers and others could not interpose the new privacy rule as a defense to the production of medical records in the interim. *See* Technical Corrections to the Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 251, 82944 (Dec. 29, 2000) (to be codified at 45 C.F.R. pt. 160, 164).

---

<sup>1</sup> *The views expressed in this article are solely those of the author and should not be construed as the official views of the Department of Justice.*

<sup>2</sup> *The Department also defends civil suits brought against various federal agencies and parties. This article does not deal with those defensive cases.*

### III. What information does the rule cover?

The privacy rule restricts disclosure of any information, in whatever form, that can identify the recipient of medical services. Protected patient information as defined by the rule extends far beyond the traditional notion of a patient's medical chart or subjective notations in a file. It includes recollections and memories of workforce members of healthcare providers, as well as information that merely provides a connection between an individual and the receipt of health care. *See* 45 C.F.R. § 164.501. For example, a patient's name contained in a directory at a hospital switchboard constitutes protected health information under the rule and may not be disclosed to a caller absent that patient's consent.

In understanding the privacy rule, it is important to grasp two fundamental points. First, the privacy rule provides only a limited number of circumstances under which protected health information may be disclosed by a health care provider or a government healthcare program without the patient's consent. These permissive disclosures are contained in 45 C.F.R. 164.512 and include disclosures for law enforcement and health oversight purposes.

The second fundamental point to remember in understanding the privacy rule is that it governs only covered entities and their business associates — typically *not* the Department of Justice (exceptions are those instances already indicated, in which components of the Department may generate medical records, such as the Bureau of Prisons and the Marshal's Service). The term "covered entities" is defined to include all entities from whom we typically obtain health care records: government healthcare programs, insurance plans, and healthcare providers and suppliers. *See* 45 C.F.R. § 160.103. The Centers for Medicare and Medicaid Services (CMS), state Medicaid agencies, the Federal Employees Health Benefits Program (FEHBP), and the TRICARE program all are covered entities.

"Business associates" of covered entities are defined as all persons or entities who "assist with the performance of, or perform on behalf of, a function or activity" for an agency, insurance plan or medical provider, including lawyers and consultants. 45 C.F.R. § 160.103. A Medicare fiscal intermediary or Part B carrier are examples of business associates under the privacy rule.

Covered entities are required to enter into contracts with these business associates, subjecting them to the same rules of non-disclosure as covered entities. These business associates must assure that their own subcontractors and agents comply with the same requirements.

Note, however, that the Department of Justice is not performing a service for or on behalf of government health plans when it conducts its investigations. Rather, it is performing its mandated role of enforcing the laws of the United States. Hence, the Department is not required to enter into a business associate arrangement with CMS, private health plans, or other covered entities and their agents in order to obtain data or other patient health information. *See* Standards for Privacy of Individually Identifiable Health Information: Final Rule, 65 Fed. Reg. 250, 82476 (Dec. 28, 2000) (to be codified at 45 C.F.R. pt. 160, 164).

Because the Department is neither a covered entity (except as previously noted) nor a business associate, the privacy rule does not govern our ability to redisclose health information we may obtain in the course of law enforcement or oversight activities. Certain privacy advocates viewed this as a flaw in the privacy rule. In response, an Executive Order was issued on December 28, 2000 which, among other things, requires that protected health information concerning an individual discovered during the course of our health oversight activities shall not be used against that individual in an unrelated civil, administrative, or criminal investigation of a non-health oversight matter unless the Deputy Attorney General has authorized such use. *See* Exec. Order No. 13181, 65 Fed. Reg. 248, 81321 (Dec. 20, 2000). If the protected health information involves members of the Armed Forces, the General Counsel of the Department of Defense must authorize the reuse. *See id.* Nothing in this Executive Order, however, places any additional limitations on the Department's derivative use of records obtained by an administrative subpoena pursuant to 18 U.S.C. § 3486.

#### IV. Permitted disclosures

The privacy rule requires that the consent of the patient be obtained before a disclosure can be made, unless that disclosure is expressly permitted under the privacy rule. It provides only a limited number of circumstances under which disclosures of health information may be made absent a patient's consent. *See* 45 C.F.R. § 164.512. For example, if the disclosure is "required by law", the covered entity is permitted to make the disclosure regardless of a lack of patient's consent. Any "mandate contained in law that compels a covered entity to make a disclosure of protected health information and that is enforceable in a court of law" is considered a disclosure required by law, under the rule. 45 C.F.R. § 164.501.

Required by law includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits."

*Id.*

The only restriction placed on this required by law disclosure is that the disclosure "complies with and is limited to the relevant requirements of such law." 45 C.F.R. § 164.512(a)(1). However, a caveat in § 164.512(a)(2) states "[a] covered entity must meet the requirements described in paragraph (c), (e), or (f) of this section for uses or disclosures required by law." Hence, even if a disclosure is otherwise required by law, it must nevertheless meet the conditions contained in § 164.512(c) (relating to adult abuse and neglect or domestic violence), § 164.512(e) (disclosures in judicial or administrative proceedings), or § 164.512(f) (disclosures for law enforcement).

Another disclosure permitted without patient consent is for "public health activities" as defined in 45 C.F.R. § 164.512(b). This includes

disclosures for purposes of disease prevention or control (§ 164.512(b)(1)(i)), for purposes of reporting child abuse or neglect (§164.512(b)(1)(ii)), for potential Food and Drug violations (§ 164.512(b)(1)(iii)), and for purposes of reporting that a person may have been exposed to a communicable disease, if such disclosure is permitted by law (§ 164.512(b)(1)(iv)).

The privacy rule permits disclosure of health information in instances relating to adult abuse and neglect and domestic violence, but only in specifically defined and limited circumstances. *See* 45 C.F.R. § 164.512(c)(1). Although a state may have reporting statutes in place for these types of crimes, the disclosure is not necessarily required by law because the privacy rule's definition expressly defers to the restrictions contained in § 164.512(c). 45 C.F.R. § 164.512(a)(2). Specifically, if the state *mandates* the reporting of such a crime, the covered entity is permitted under the privacy rule to make the disclosure. 45 C.F.R. § 164.512(c)(1)(i). However, if the state merely *authorizes* a disclosure, then the covered entity may make a disclosure only if it concludes, in the exercise of its best judgment, that the disclosure is necessary to prevent future harm to the individual or other victims *or*, if the victim is incapacitated and unable to provide consent, only when the authorized law enforcement officer represents that the protected health information will not be used against the victim, *and* that immediate enforcement activity will be harmed unless the information is obtained before the patient may regain capacity to consent. 45 C.F.R. § 164.512(c)(1)(iii)(A)-(B).

The next area of permissible disclosure is for "specialized government functions," including military personnel, national security and intelligence activities, protective services for the President or heads of state, medical suitability determinations made by the Department of State, and, in specified circumstances, to correctional institutions. *See* 45 C.F.R. § 164.512(k)(1)-(5).

Finally, the privacy rule provides two additional areas of permissible disclosures that affect the Department: disclosures are permitted in some circumstances to "health oversight" and "law enforcement" agencies. To understand these provisions of the privacy rule, however, one must

first understand the distinction drawn in the privacy rule between these two functions.

## V. Health oversight vs. law enforcement

It seems counterintuitive to assert that the Department is not acting in a law enforcement capacity when investigating health care fraud or other health care related offenses. Indeed, in a literal sense we are. However, the privacy rule grants greater right of access to oversight agencies performing health oversight functions than is provided to general law enforcement.

### A. Health oversight

Covered entities and their business associates, generally, are permitted to disclose health information to a health oversight agency, as defined in 45 C.F.R. § 164.501:

oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for appropriate oversight of: (i) The health care system; (ii) Government benefit programs for which health information is relevant to beneficiary eligibility; (iii) Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or (iv) Entities subject to civil rights laws for which health information is necessary for determining compliance. *See id.*

A health oversight agency is defined as

an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

45 C.F.R. § 164.501(6)(v).

The preamble of the privacy rule states that the Department of Justice qualifies as a health oversight agency when performing health oversight functions. *See* Standards for Privacy of Individually Identifiable Health Information: Final Rule, 65 Fed. Reg. 250, 82492 (Dec. 28, 2000) (to be codified at 45 C.F.R. pt. 160, 164). However, a health oversight function does *not* include instances where

the individual is the subject of the investigation ... and such investigation ... does not arise out of and is not directly related to: (i) The receipt of health care; (ii) A claim for public benefits related to health; or (iii) Qualification for, or receipt of, public benefits or services when a patient's health is integral to the claim for public benefits or services.

45 C.F.R. § 164.512(d)(2).

### B. Law enforcement

If a law enforcement agency is seeking protected health information for purposes other than health oversight, its request likely will be categorized as a law enforcement request. *See* 45 C.F.R. § 164.512(f). Law enforcement disclosures include those that are required by law (§ 164.512(f)(1)(i)), those required under a court order, court-ordered warrant, or subpoena or summons issued by a judicial officer (§ 164.512(f)(1)(ii)(A)), a grand jury subpoena (§ 164.512(f)(1)(ii)(B)), or an administrative subpoena or civil investigative demand (CID). Information sought by an administrative subpoena or CID must meet an additional three-pronged test: (1) the request must be "relevant and material" to a "legitimate law enforcement inquiry," (2) the request must be "specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought," *and* (3) the request must be such that "de-identified information could not reasonably be used." 45 C.F.R.

§ 164.512(f)(1)(ii)(C). The preamble clarifies this section to state that "where law enforcement officials choose to obtain protected health information through administrative process, they must meet the three pronged test required by this regulation." Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 250, 82681 (Dec. 28, 2000) (to be codified at 45 C.F.R. pt. 160, 164).

This provision of the rule dealing with law enforcement access to records is distinct from the authority the Department possesses when conducting health oversight investigations. An administrative subpoena arising from a health oversight investigation need not meet the three-pronged test imposed on law enforcement administrative subpoenas.

Disclosure may be made to law enforcement when the patient consents, the disclosure is required by law, or legal process is issued that meets this three-pronged test. Absent those criteria, the privacy rule permits disclosure for law enforcement only in the following circumstances:

- For the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, only the following can be disclosed: Name, address, date and place of birth; social security number; ABO blood type and Rh factor; type of injury; date and time of treatment; date and time of death, if applicable; and a description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos. The covered entity may not disclose the individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue identification or location information. 45 C.F.R. § 164.512(f)(2).
- Information about victims of crime, but only with the victim's consent or, if without consent, by reason of incapacity or emergency, and then only if "the law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim," and also represents "that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure," and "the disclosure is in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment." 45 C.F.R. § 164.512(f)(3). Of course, to the extent this information is required by law to be reported, this privacy rule does not preclude the

disclosure. Examples may include information concerning victims of child or elder abuse, or victims of gunshot wounds. In these cases, even in the absence of the victim's consent or the representations of law enforcement, the disclosure may be made.

- Information about people who have died, but *only* "if the covered entity has a suspicion that such death may have resulted from criminal conduct." 45 C.F.R. § 164.512(f)(4).
- Information about crimes on the premises of the health care provider, but only if "the covered entity believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the covered entity." 45 C.F.R. § 164.512(f)(5). If the health care provider is rendering emergency care off its premises, it may disclose protected health information to a law enforcement official, but only to an extent necessary to alert law enforcement to the crime or the location of such crime or of the victim(s) of such crime, and the identity, description, and location of the perpetrator of such crime. 45 C.F.R. § 164.512(f)(6). This permitted disclosure does not extend to information about abuse, neglect, or domestic violence emergency cases. *Id.* In those cases, disclosure cannot be made without complying with 45 C.F.R. § 164.512(c)(1).
- Disclosures to a coroner or medical examiner for purposes of identifying a deceased person, determining a cause of death, or for other duties as authorized by law. 45 C.F.R. § 164.512(g).
- Disclosures "to avert a serious threat to health or safety," if the health care provider, "consistent with applicable law and standards of ethical conduct," and in good faith, believes the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public. 45 C.F.R. § 164.512(j)(1)(i)(A). Such disclosure can be made, though, only to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat. 45 C.F.R. § 164.512(j)(1)(i)(B). Such disclosures also are permitted if they are necessary for law enforcement authorities to identify or apprehend an individual because of a statement by an individual admitting

participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to the victim. 45 C.F.R. § 164.512(j)(1)(ii)(A); or

- Where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody. 45 C.F.R. § 164.512(j)(1)(ii)(B).
- Where the health care provider intends to tell law enforcement about an individual admitting participation in a violent crime, the disclosure may contain only the statement itself and the identification and location information listed in § 164.512(f)(2)(i). On the other hand, even if a patient makes a "statement admitting participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to the victim," the disclosure may *not* be made if the information was "learned by the covered entity" in the course of treatment to affect the propensity to commit the criminal conduct that is the basis for the disclosure, or counseling or therapy; or through a request by the individual to initiate or to be referred for the treatment, counseling, or therapy. 45 C.F.R. § 164.512(j)(2)(i).

## VI. Confidentiality of investigations

The privacy rule provides that patients should be told when a disclosure of their health information is made. 45 C.F.R. § 164.528(a). All covered entities are required to maintain an "accounting" or log of each disclosure of health information, in the affected patient's file. 45 C.F.R. § 164.528(a)(i). The entity must then disclose that log to the patient on request unless certain conditions exist. Among these conditions is a written request from law enforcement or health oversight indicating that a disclosure would impede the requesting agency's activities. 45 C.F.R. § 164.528(a)(2)(i). In urgent circumstances, this request from law enforcement may be made orally but will be effective for no longer than thirty days unless a written statement is received within that time. 45 C.F.R. § 164.528(a)(2)(ii)(C).

This provision in the privacy rule requires that law enforcement and health oversight agencies, whenever requesting protected health information,

take affirmative steps to assure the confidentiality of the investigation.

## VII. Special privacy rules relating to psychotherapy notes

Psychotherapy notes are

notes 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 or a group, joint, or family counseling session . . . Psychotherapy notes *excludes* medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: Diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

45 C.F.R. § 164.501.

Notwithstanding any other provision of the privacy rule, and except as stated below, a covered entity must obtain an authorization from the patient for any use or disclosure of psychotherapy notes. 45 C.F.R. § 164.508(a)(2). This authorization is specific to the psychotherapy notes and is in addition to the consent the patient may have given for other purposes, such as treatment, payment and health care operations. *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 250, 82652 (Dec. 28, 2000) (to be codified at 45 C.F.R. pt. 160, 165).

A covered entity need not obtain patient authorization to disclose the records when disclosure is required by law; when disclosure is needed for the oversight of the provider who created the psychotherapy notes; or when disclosure is needed to avert a serious and imminent threat to health or safety. 45 C.F.R. § 164.508(a)(2)(ii).

## VIII. Disclosures for administrative and judicial proceedings

The drafters of the privacy rule concluded that the current system governing disclosures and uses of medical records in the course of litigation, as exemplified by the Federal Rules of Civil Procedure, "does not provide sufficient protection for protected health information." Standards for

Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 250, 82596 (Dec. 28, 2000). Accordingly, 45 C.F.R. § 164.512(e) was drafted to govern use and disclosure of protected health information in most litigation arenas.

Covered entities are permitted to disclose protected health information in an administrative or judicial proceeding pursuant to an order of a court or of an administrative tribunal. Unless an order is issued, covered entities may disclose protected health information in response to a subpoena, discovery request, or other lawful process only after one of the following two conditions have been met: (1) the covered entities receive “satisfactory assurance” from the party seeking the information that reasonable efforts have been made to give notice to the individual who is the subject of the protected health information, 45 C.F.R. § 164.512(e)(1)(ii)(A); *or* (2) the covered entities receive satisfactory assurance from the party seeking the information that the parties to the litigation have entered into a qualified protective order, or that the party seeking the information has requested a qualified protective order from the court, 45 C.F.R. § 164.512(e)(1)(vi).

This protective order must prohibit the parties from using the information for any purpose other than the litigation or proceeding for which the information was requested. 45 C.F.R. § 164.512(e)(1)(v)(A). The protective order also must require that all protected health information either be returned to the covered entity at the end of the litigation or proceeding or be destroyed. 45 C.F.R. § 164.512(e)(1)(v)(B).

Nothing in this section dealing with disclosures in administrative or judicial proceedings supercedes other provisions of the privacy rule permitting disclosures to health oversight or law enforcement agencies. *See* 45 C.F.R. § 164.512(e)(2). The preamble of the privacy rule makes clear that if a covered entity is otherwise permitted to make the disclosure, a request that arises in a litigation context does not convert the request to the stricter privacy rules governing administrative or judicial proceedings. *See Standards for Privacy of Individually Identifiable Health Information*, 65 Fed. Reg. 250, 82530 (Dec. 28, 2000) (to be codified at 45 C.F.R. pt. 160, 164).

## **IX. Whistle-blower protections**

The privacy rule provides that a covered entity is not in violation of the privacy rule when a member of its workforce, or a person associated with a business associate of the covered entity, discloses, in good faith, protected health information to a health oversight agency or public health agency authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the covered entity; a health care accreditation organization; or an attorney, for the purpose of developing a *qui tam* lawsuit. *See* 45 C.F.R. § 164.502(j)(1).

The privacy rule does not regulate the activities of whistle blowers. Rather, it regulates the behavior of covered entities and holds them responsible for the whistle blowing activity of their workforce. *See Standards for Privacy of Individually Identifiable Health Information*, 65 Fed. Reg. 250, 82636 (Dec. 28, 2000) (to be codified at 45 C.F.R. pt. 160, 164). 45 C.F.R. § 164.530(g) prohibits covered entities from sanctioning members of its workforce who file a complaint with the Secretary of HHS alleging a violation of this privacy rule, testify, assist, or participate in an investigation, compliance review, proceeding, or hearing, and who reasonably disclose protected health information in good faith and in compliance with the privacy rule to oppose an act of the covered entity made unlawful by the privacy rule. The preamble to the privacy rule makes clear that it is not intended as a new barrier to whistle blowing, nor does it permit covered entities to employ the privacy rule as a mechanism for sanctioning workforce members or business associates for whistle-blowing activities. *See Standards for Privacy of Individually Identifiable Health Information*, 65 Fed. Reg. 250, 82636 (Dec. 28, 2000).

## **X. Interplay with other statutes**

### **A. State statutes**

As a general rule, state law provisions that are in conflict with the privacy rule are preempted by the federal requirements. The three exceptions to this are: (1) If the Secretary of HHS determines that the state law is necessary to prevent fraud and abuse, ensure appropriate regulation of state health and insurance plans, for state reporting on health delivery, and “other purposes;” (2) if the state law is more stringent in protecting protected health information; or (3) if the state law addresses controlled dangerous substances. *See*

Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 250, 82480 (Dec. 28, 2000) (to be codified at 45 C.F.R. pt. 160, 164).

The preamble to the privacy rule states that where *The Privacy Act of 1974* (5 U.S.C. § 552a) allows a federal agency the discretion to make a routine use disclosure, and the medical records privacy rule prohibits the disclosure, the agency will have to comply with the medical records privacy rule. This means not making the disclosure. *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 250, 82462-01 (Dec. 28, 2000) (to be codified at 45 C.F.R. pt. 160, 164).

### **B. The Freedom of Information Act**

The Freedom of Information Act (5 U.S.C. § 552) provides for public disclosure, upon request, of many types of information in the possession of the Federal Government, subject to nine exemptions and three exclusions. One exemption permits the Federal Government to withhold “personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.” 5 U.S.C. § 552(b)(6). When a FOIA request seeks information that includes protected health information, the preamble of the privacy rule states that this FOIA exemption should be used to deny the request. *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 250, 82482 (Dec. 28, 2000) (to be codified at 45 C.F.R. pt. 160, 164). 65 Fed. Reg. 82482.

### **C. The Federal Substance Abuse Confidentiality Act**

The Federal Substance Abuse Confidentiality Act provides for the confidentiality of health records that are maintained in connection with the performance of any federally-assisted, specialized alcohol or drug abuse treatment program. *See* 42 U.S.C. § 290dd-2, 42 C.F.R. Part 2. In most instances in which law enforcement or oversight agencies are seeking these types of records, the privacy rule will contain the more lenient requirements. Nevertheless, because disclosure to law enforcement and oversight agencies under the privacy rule is permissive, covered entities will not be in violation of the privacy rule for failing to make disclosures where the substance abuse

statute precludes it. *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 250, 82482 (Dec. 28, 2000) (to be codified at 45 C.F.R. pt. 160, 164).

### **XI. Minimum necessary**

The regulation places an affirmative burden on a covered entity to “make reasonable efforts to limit [the disclosure of] protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.” Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 250, 82715 (Dec. 28, 2000). This “minimum necessary” principle applies to all government requests unless the government can demonstrate that the request is required by law. 45 C.F. R. Reg. § 164.502(b)(2)(v). When a disclosure is required by law, the minimum necessary standard does not apply. *Id.* *See* also Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 250, 82715 (Dec. 28, 2000) (45 C.F.R. 164). As stated, *supra*, “required by law means a mandate contained in law that compels a covered entity to make a disclosure of protected health information and that is enforceable in a court of law.” 45 C.F. R. §164.501. Providers may question whether the various statutes and regulations permitting the Secretary of HHS and others access to protected health information for purposes of ensuring program integrity constitutes a required exception. A complete discussion of the required by law standard is contained in the privacy rule’s preamble at Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 250, 82666 (Dec. 28, 2000) (to be codified at 45 C.F.R. pt. 160, 164).

The regulation allows the covered entity to rely on government representations that the information requested is the minimum necessary for the stated purpose. *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 250, 82715 (Dec. 28, 2000) (to be codified at 45 C.F.R. pt. 160, 164); Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 250, 82530 (Dec. 28, 2000) (to be codified at 45 C.F.R. pt. 160, 164).

### **XII. Department of Justice suggested practices**

On August 30, 2000, the Deputy Attorney General issued Suggested Practices for

Maintaining Confidentiality of Medical Records. Department personnel are expected to take all practicable steps to protect the confidentiality of individually identifiable protected health information. Requests for such records should be narrowed to specific providers or patients. Care should be taken to assure that such records are handled and maintained in a manner that assures their confidentiality. Confidentiality Agreements should be employed when, in the course of litigation or investigation, such records are shared with government experts, defense counsel, and other third parties outside the government. Protective orders should be obtained when such records are produced in discovery and, when such records are to be made public in the course of litigation, steps should be taken to obscure patient identification, if practicable. As the April 2003 effective date draws near, these guidelines will be modified to accommodate the new privacy rule.

### **XIII. Conclusion**

The privacy rule and its preamble consume 367 pages in the Federal Register. As with any overview, this article can provide only a general guide to the rule with a focus on how the rule will effect the functions of the Department of Justice. Department personnel confronting issues under this rule are welcome to contact the author or Ian DeWaal, Senior Counsel in the Criminal Division, for additional guidance. ❖

### **ABOUT THE AUTHOR**

□ **Dan Anderson** is the Senior Counsel for Health Care Fraud at the Civil Division of the United States Department of Justice. Prior to joining the Department in 1996, Mr. Anderson was the Director of Maryland's Medicaid Fraud Control Unit. Mr. Anderson has testified before numerous committees of the United States Congress on issues germane to health care fraud and elder abuse and neglect. He is the co-author of the book "Effective Fraud Control Tactics for Insurers and Managed Care Plans," as well as numerous articles on that topic. ❖