An Unintended Impact of HIPAA on Estate Planning

Eugene Tomine*

* 1972 graduate of the University of Caifornia, Boalt Hall School of Law. Admitted to practice in the State of California in December 1972. Private practice since 1975 initially practicing in the area of immigration law during which time Mr. Tomine taught Immigration Law & Procedure at Golden Gate University Law School in San Francisco and was a contributing author to a book entitled, *Immigration Law and Defense*, 2nd Edition (Clark Boardman Company, N.Y.) More recently, Mr. Tomine's practice has focussed on the area of estate planning and probate. Mr. Tomine currently is of Counsel to Teraoka & Partners, LLP.

Introduction

On August 21, 1996 then President of the United States, William J. (Bill) Clinton, signed into law landmark legislation known as the Health Insurance Portability and Accountability Act of 1996 (HIPAA). [1] The primary purpose of HIPAA was threefold: 1) to facilitate the continuation of health insurance for those persons who changed their jobs, started their own businesses, or became disabled; 2) to facilitate the efficiencies and cost savings of the increasing use of electronic technology in the health care industry; and, 3) to protect the security and confidentiality of individually identifiable health information of patients in the health care system. What was not contemplated by Congress when the statute and subsequent regulations were promulgated was the impact that the privacy provisions of HIPAA would have on the preparation of the basic instruments which typically make up a comprehensive estate plan. This article will address the unintended byproduct of those privacy provisions in the context of an estate planning practice.

Background

The average American, today, is inundated almost daily with requests for personal information via internet retail sales, telemarketers, email solicitations, employment application forms, insurance claim forms, financial institutions, credit applications, and countless others. As a consequence, there appears to be a growing public concern over the unauthorized use of this type of information and the resulting potential for fraud, deceit, and identity theft. With the ever-expanding utilization of interconnected electronic media applications in business, public anxiety over its misuse is well founded. And, what could be more private and more personal than one's confidential medical records. In the medical industry, with the evolution of electronic technology and its application to the storage, retrieval, and transmission of records and data, an understandably growing concern has begun to emerge among the consuming public over the protection of their most private and sensitive personal health care information.

In this age of electronic data storage and transmission, rarely a day goes by without a report of some sort appearing in the media of a computer glitch or human error in the handling of such data, resulting in the inadvertent release of this most confidential and personal medical information. The following are just a few such examples cited in the Federal Register, Vol. 65, No. 250, page 82467,

1) Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, 1996, codified as 42 USC Sec 1320d.

December 28, 2000:

- A Michigan-based health system accidentally posted the medical records of thousands of patients on the Internet (The Ann Arbor News, February 10, 1999).
- A Utah-based pharmaceutical benefits management firm used patient data to solicit business for its owner, a drug store (Kiplingers, February 10, 1999).
- An employee of the Tampa, Florida, health department took a computer disk containing the names of 4,000 people who had tested positive for HIV, the virus that causes AIDS (USA Today, October 10, 1996).
- The health insurance claim forms of thousands of patients blew out of a truck on its way to a recycling center in East Hartford, Connecticut (The Hartford Courant, May 14, 1999).
- A patient in a Boston-Area hospital discovered that her medical record had been read by more than 200 of the hospital's employees (The Boston Globe, August 1, 2000).
- A Nevada woman who purchased a used computer discovered that the computer still contained the prescription records of the customers of the pharmacy that had preciously owned the computer. The pharmacy data base included names, addresses, social security numbers, and a list of all the medicines the customers had purchased (The New York Times, April 4, 1997 and April 12, 1997).
- A speculator bid $4,000 for the patient records of a family practice in South Carolina. Among the businessman's uses of the purchased records was selling them back to the former patients (The New York Times, August 14, 1991).
- In 1993, the Boston Globe reported that Johnson and Johnson marketed a list of 5 million names and addresses of elderly incontinent women (ACLU Legislative Update, April 1998).
- A few weeks after an Orlando woman had her doctor perform some routine tests, she received a letter from a drug company promoting a treatment for her high cholesterol (Orlando Sentinel, November 30, 1997).

Right of Privacy

Americans have long been obsessed with the notion of privacy and the right to be free from governmental intrusion into their lives. Yet, interestingly, nothing in the U.S. Constitution explicitly accords such a right of privacy to its citizens. Rather, the concept of privacy has evolved over a long line of cases dating back to Union Pacific R. Co. v. Botsford, 141 U.S. 250, 251, 11 S.Ct. 1000, 1001 (1891) in which the court has recognized a right of personal privacy and a guarantee of certain zones of privacy (penumbras) emanating from the guarantees contained in the Bill of Rights. Griswold v.

Connecticut, 381 U.S. 479, 484 (1965). In Roe v. Wade, 410 U.S. 113 (1973), the landmark case in which the Court upheld a woman's right to choose, the Court emphasized that only personal rights that are deemed "fundamental" or "implicit in the concept of ordered liberty" [Palko v. Connecticut, 302 U.S. 319, 325, 58 S.Ct. 149, 152 (1937)] are included in this guarantee of personal privacy.

The Supreme Court has deemed other personal rights as fundamental or implicit in the concept of ordered liberty and thus has expanded the right of privacy to include the marriage relationship, Loving v. Virginia, 388 U.S. 1, 12, 87 S.Ct. 1817, 1823 (1967); procreation, Skinner v. Oklahoma, 316, U.S. 535, 541-542, 62 S.Ct. 1110, 1113-1114 (1942); contraception, Eisenstadt v. Baird, 405 U.S. at 453-454, 92 S.Ct. at 1038-1039; family relationships, Prince v. Massachusetts, 321 U.S. 158, 166, 64 S.Ct. 438, 442 (1944); and child rearing and education, Pierce v. Society of Sisters, 268 U.S. 510, 535, 45 S.Ct. 571, 573 (1925).

The Court, however, has made it known in cases acknowledging the right to privacy that the right is not absolute. The states may assert their own interests in safeguarding health, maintaining high medical standards, and regulating activities within their borders. In fact, the Court had in the past rejected the unrestricted right of this kind, Jacobson v. Massachusetts, 197, U.S. 11, 25 S.Ct. 358 (1905) (regarding vaccinations); Buck v. Bell, 274 U.S. 200, 47 S.Ct. 584 (1927) (regarding sterilization).

Where certain "fundamental rights" are involved, the Court has held that regulation limiting these rights may be justified only by a "compelling state interest." Kramer v. Union Free School District, 395 U.S. 621, 627, 89 S.Ct. 1886, 1890, (1967); Sharpiro v. Thompson, 394 U.S., 618, 634, 89 S.Ct. 1322, 1331 (1969); Sherbert v. Verner, 374 U.S. 398, 406, 83 S.Ct. 1790, 1795 (1963), and that legislative enactments must be narrowly drawn to express only the legitimate state interest at stake. Griswold v. Connecticut, 381 U.S. at 485, 85 S.Ct. at 1682; Aptheker v. Secretary of State, 370 U.S. 500, 508, 84 S.Ct. 1659, 1664 (1964); Cantwell v. Connecticut, 310 U.S. 296, 307-308, 60 S.Ct. 900, 904-905 (1940).

The Court in Roe v. Wade, supra, thus concluded that the right of personal privacy which includes a women's right to choose, is not unqualified and must be considered against important state interest in regulation. Roe v. Wade 410 U.S. at 154.

In light of Roe v. Wade, supra, it is not surprising that in Whalen v. Roe 429 U.S. 589 (1977), a case involving electronically stored medical data, the U.S. Supreme Court upheld the New York State Controlled Substances Act of 1972 despite claims by Appellee physicians that electronically

stored information naming patients and physicians relating to prescriptions for drugs having a potential for abuse as violative of the Appellees' constitutionally protected right to privacy.

In Whalen, supra, the State of New York, following the lead of California and Illinois, promulgated the New York State Controlled Substances Act of 1972. That statute categorized drugs into five schedules. Schedule I consisted of drugs such as heroin that were highly abused and had no recognized medical use and could not be prescribed under any circumstances. Schedules II-V consisted of drugs that had a recognized medical use, were generally prescribed by physicians, but had potential for abuse in progressively lesser degrees.

The New York Statute required that all prescriptions for Schedule II drugs be prepared in triplicate on an official Department of Health form. The completed form named the prescribing physician, dispensing pharmacy, the name of the drug and dosage, and the name, address, and age of the patient. One copy of the prescription remained with the prescribing physician; one copy was retained by the dispensing pharmacist; and, one copy was forwarded to the New York State Department of Health where it was coded and inputted into the State's electronic database for a period of five years.

The computer tapes on which the data was stored were kept under lock and key in a room surrounded by a locked wire fence equipped with an alarm system. If and when the tapes were used to retrieve information, they were run "off line." The statute specifically prohibited unauthorized disclosure of names and identities of patients, violations for which were criminally punishable by a monetary fine and imprisonment.

Shortly before the effective date of the New York statute, an action was brought in the Federal District Court by a group of physicians, patients, and professional associations alleging that the reporting requirements of the statute constituted a violation of their right to privacy. The District Court, after a one day trial, agreed, holding that:

> "The doctor-patient relationship is one of the zones of privacy accorded constitutional protection and that the patient-identification provisions of the Act invaded this zone with a needlessly broad sweep, and enjoined enforcement of the provisions of the Act which deal with the reporting of patients' names and addresses." 429 U.S. at 596.

On appeal, the U.S. Supreme Court reversed the District Court. The Supreme Court, while recognizing a patient's right to privacy, found that the disclosure requirements coupled with the

security provisions of the New York Statute were not violative of the patient's constitutional rights. The Court, there, held:

> "Disclosures of private medical information to doctors, to hospital personnel, to insurance companies, and to public health agencies are often an essential part of modern medical practice even when the disclosure may reflect unfavorably on the character of the patient. Requiring such disclosures to representatives of the State having responsibility for the health of the community, does not automatically amount to an impermissible invasion of privacy." 429 U.S. at 603.

The Court in Whalen thus held that neither the immediate nor the threatened impact of the patient-identification requirements in the New York State Controlled Substances Act of 1972 on either the reputation or the independence of patients for whom Schedule II drugs were medically indicated was sufficient to constitute an invasion of any right or liberty protected by the Fourteenth Amendment. 429 U.S. at 604.

Health Insurance Portability and Accountability Act of 1996

> No matter how or why a disclosure of personal information is made, the harm to the individual is the same. In the face of industry evolution, the potential benefits of our changing health care system, and the real risks and occurrences of harm, protection of privacy must be built into the routine operations of our health care systems. Office of the Secretary of Health and Human Services, "Standards for Privacy of Individually Identifiable Health Information," Federal Register, Vol. 65, No. 250, page 82465, December 28, 2000.

Health care information has never been completely private. And, while breaches of confidentiality have no doubt occurred in the past, such breaches usually took the form of exchanges of hard copy documents or verbal exchanges of information. Today, however, with the increasing number of health care providers relying on electronic technology to store, retrieve, and transmit medical records, the release of information may only require the mere push of a button. In a matter of seconds, a person's most profoundly private information may be shared with countless others. Unfortunately, it does not matter that the disclosure was made intentionally or inadvertently, or as a result of human error, the harm to the individual is the same.

So it seems the advances in computer and electronic technology that have greatly benefited the

health care industry, have at the same time threatened to undermine the confidentiality of millions of patients in the health care system. In this context, then, in 1996 the Congress of the United States enacted the Health Insurance Portability and Accountability Act (HIPAA).

> An act to amend the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes. Prologue, Public Law 104-191, 1996 (now 42 USC §1320d).

A major component of this legislation was the Administrative Simplification provisions found in Sections 261-264 of the Act. Section 264(b) of the Act required the Secretary of Health and Human Services to submit to Congress within twelve months after the passage of HIPAA (August 21, 1996), recommendations for:

- The rights that an individual who is the subject of individually identifiable health information should have.
- The procedures that should be established for the exercise of such rights.
- The uses and disclosures of such information that should be authorized or required.

The Secretary of HHS submitted recommendations to Congress on September 11, 1997. Section 264 of the Act further provided that:

> "If legislation governing standards with respect of the privacy of individually identifiable health information transmitted in connection with the transactions described in section 1173(a) of the Social Security Act (as added by Section 262) is not enacted by the date that is 36 months after the date of the enactment of this Act, the Secretary of Health and Human Services shall promulgate final regulations containing such standards not later than the date that is 42 months after the date of the enactment of this Act."

Congress failed to enact the legislation referenced in Section 264 within the three year window, and, thus, as mandated in that Section, the Secretary of HHS promulgated and published its final regulations, which became effective on April 14, 2003. It was not, however, until well over a year after implementation of the Secretary of HHS' final regulations that estate planning practitioners began to recognize the import of HIPAA on the way they had been drafting estate documents prior to its enactment.

Relevant HIPAA Provisions

For purposes of this article, the relevant provisions of the Health Insurance Portability and Accountability Act are found in Section 262 which amended the Social Security Act by adding a new Part C of Title XI, and specifically, Section 1177 which provides as follows:

> Section 1177(a) OFFENSE – A person who knowingly and in violation of this part [without valid authorization as defined in 45 CFR 164.508(c)(1)] [2)]
>
> (1) uses or causes to be used a unique health identifier;
> (2) obtains individually identifiable health information relating to an individual; or
> (3) discloses individually identifiable health information to another person, [emphasis added],
> shall be punished as provided in subsection (b).
>
> (b) PENALTIES – A person described in subsection (a) shall –
> (1) be fined no more than $50,000, imprisoned not more than 1 year, or both;
> (2) if the offense is committed under false pretenses, be fined not more than $100,000, imprisoned not more than 5 years, or both; and
> (3) if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, be fined not more than $250,000, imprisoned not more than 10 years, or both.

Thus, under Section 1177, if a covered entity such as a physician or medical provider discloses protected health information without an authorization valid under 45 CFR §164.508(c)(1), that physician or medical provider would be, if convicted, subject to a fine of $50,000 and imprisonment of up to 1 year, or both. If the offense were committed under false pretenses, the fine could be increased to $100,000 with imprisonment of 5 years. And, if the offense were committed with the intent to use the protected information for commercial advantage, personal gain, or malicious harm, the fine could be increased to $250,000 with imprisonment of 10 years. The penalties authorized under §1177 have already had a chilling effect on the free flow of information between physicians and lawyers. In the face of these statutory criminal sanctions, physicians and health care providers have become increasingly reluctant to provide attorneys with medical information about the

2) 45 CFR §164.508(a) "Except as otherwise permitted or required by this subchapter, a covered entity may not use of disclose protected health information without an authorization that is valid under this section."

attorney's client without the client's consent.

So what is the problem? Perhaps the following hypothetical will help to put the issue into context.

Hypothetical

Mr. Smith is your long time client. Several years ago, you prepared an estate plan for him that among other instruments included a revocable intervivos trust. A term of the trust provides that upon Mr. Smith's incapacity as certified by a physician licensed in the State of California, Mr. Smith's daughter, Ann, will assume the role of trustee and take over the management of the affairs of the trust. You last met with Mr. Smith six months ago, and, while his short term memory appeared to be fading slightly, he seemed to be in excellent health and perfectly capable of managing his trust. Mr. Smith's daughter called you last week and informed you that her father has "lost it" and that she should take over management of the trust in accordance with the terms of the trust.

You call Mr. Smith into your office to ascertain his mental fitness to continue as trustee of the trust. In your meeting, it is obvious to you that Mr. Smith no longer has the mental acuity to handle the affairs of the trust. But, when you suggest that he step down as trustee, he declares himself to be fit and able to continue as trustee, and, moreover, refuses to give his consent to have his physician disclose any information regarding his mental condition.

The next day, you call Mr. Smith's personal physician, Dr. Jones, and explain that you need a certificate from the good doctor certifying to Mr. Smith's incompetency. Dr. Jones, coincidentally, had just finished reading his copy of the Health Insurance Portability Act and Accountability Act of 1996 and tells you that without the written authorization of Mr. Smith, he cannot disclose any individually identifiable health information about his patient.

Here, then, is the dilemma for the attorney. You know that your client is incapable of managing his trust. And, if your client continues as trustee, he may squander his estate away or possibly become a victim of fraud, the end result of which may be the same – total loss of his estate. You believe that your client's daughter should take over the affairs of the estate. But, without the physician's certificate, the daughter cannot assume the office of successor trustee.

The above factual situation, although hypothetical, is already becoming reality and soon may be

repeated with regularity in exchanges between lawyers and doctors everywhere as the HIPAA regulations take hold and become better understood by doctors and lawyers.

This hypothetical addresses the situation where the client refuses to admit to being incompetent. The result is the same if the client is so debilitated that he/she is unable to give informed consent to the physician to release the required certificate certifying to the incapacity of the client.

Prior to HIPAA, physicians routinely disclosed individually identifiable health information about their patients to attorneys without their patient's consent and without blinking an eye. And, attorneys routinely prepared estate planning documents containing language authorizing the replacement of a principal with a successor upon certification of the principal's incapacity by a physician.

The typical estate plan today consists of, in almost every instance, a trust instrument, a pour over will, a durable power of attorney, and an advance health care directive. Without fail, each of these instruments will contain a provision for the replacement of the principal by a successor when the principal is determined to be incompetent. A standard clause in a declaration of trust will read as follows:

> "If the Settlor cannot administer the trust because of physical or mental incapacity, or otherwise cannot act, during any period of incapacity, the successor Trustee named herein shall act as Trustee, having all rights granted to the Trustee by this instrument. Physical or mental incapacity shall be conclusively established if two physicians, authorized to practice medicine in the State of California, issue written certificates to that effect. In the absence of the certificates, a successor trustee may petition the court having jurisdiction over this trust to remove the Trustee and replace the Trustee with the successor Trustee."

On its face, such a provision in a declaration of trust does not appear to present any major obstacle to having a successor appointed. In plain English, if the successor cannot get a physician to certify that the principal is incompetent, the successor can go to court and get a judge to order the substitution of the successor trustee for the incapacitated trustee. Unfortunately, the solution is not that simple. First of all, one of the primary motivating factors in establishing a living trust is to avoid the enormous time and expense of having to go to court to resolve estate matters. If, under HIPAA, a successor must now resort to the courts as a result of a physician's reluctance to provide health information, then at least one of the essential benefits of establishing the trust is removed.

From a procedural prospective, petitioning the court, in light of HIPAA, does not appear to be a

viable alternative. In order for the court to grant the petition to replace the trustee with the successor trustee, the court must make a finding of incapacity. That finding must be based on competent evidence in the record. Competent evidence generally would take the form of medical records of the trustee or the treating physician's testimony. If the trustee refuses to give his consent to release his medical records, cognizant of the sanctions imposed by the HIPAA privacy provisions, it is unlikely that the physician would take the risk of disclosing the medical records of his patient or testifying in court.

Finding a solution to this dilemma is not an easy task. It is obvious that attorneys cannot continue in their practices with a "business as usual" attitude. With such severe criminal sanctions staring them in the face, attorneys and physicians could not, and would not, risk violating the privacy provisions of HIPAA and its regulations. A long-term solution would be to change the law. That is, work with legislators to amend HIPAA and its regulations, carving out an exception for the casual disclosure of protected health information by physicians to attorneys in cases requiring proof of incapacity – essentially codifying the informal practice of disclosure of medical information that existed pre-HIPAA. Realistically, however, a return to the "good old days" seems unlikely given the time and effort expended by Congress and the Department of Health and Human Services in developing the current law and regulations. Moreover, given the obsession of the American people with their right to privacy, it may be difficult at best to establish a compelling state interest in any encroachment of this right.

In the short term and perhaps a more practical approach would be to change the way estate plan attorneys practice law.

Modify Estate Plan Documents

The language used in tried and true form documents is not necessarily cast in concrete. Pre-HIPAA forms (trusts, Wills, durable powers of attorney, advance health care directives) all contain substantially similar provisions establishing incapacity by means of a certificate issued by one or more physicians licensed in the state of residence of the principal. With the advent of HIPAA, leading attorneys in California [3] are now recommending that:

3) California Continuing Education of the Bar, "Capacity and Undue Influence: Assessing, Challenging, and Defending", Cal CEB Action Guide, Fall 2003

1. The term "physician" be substituted with the terms, "family member" or "trusted friend" or "a committee of family and friends." Rather than having a physician make a determination of incapacity that requires consent of the principal, assign the task to a family member or friend.

2. Instead of the term "incapacity" or "incompetent" substitute the language, "is no longer able to substantially manage the affairs of the trust". Rather than introduce terms such as incapacity or incompetent that require a medical opinion, use lay terms that a family member or friend could apply.

3. Instead of a springing power of attorney, use a currently effective power of attorney containing precatory language that the agent not act until the principal is no longer able to substantially manage his/her financial affairs. Rather than waiting for the principal to become incompetent, allow the agent to act presently without any determination being made as to capacity.

4. Agents under advance health care directives be given express authority to act immediately, even though the principal is still capable of making health care decisions for himself/herself.

Use of Advance Health Care Directives

Estate planning attorneys routinely prepare advance health care directives for clients in a typical estate plan package of documents. The advance health care directive (AHCD) is an instrument authorized under California Probate Code §4670-4701 that allows a principal to appoint an agent to make health care decisions for the principal when the principal's primary physician determines that the principal is unable to make health care decisions on his/her own. The statutory form AHCD found at California Probate Code Section 4701 states:

> "My agent's authority becomes effective when my primary physician determines that I am unable to make my own health care decisions..."

In the pre-HIPAA days, if the principal became incapacitated, the agent would so advise the principal's physician and the physician would issue a letter certifying that the principal is not competent to handle his/her own affairs and the agent would then proceed to make health care decisions (and other decisions if the agent were also attorney in fact for the principal's financial power of attorney) for the principal.

Under HIPAA, attorneys have now encountered a major roadblock. Physicians are reluctant to issue such letters without the consent of their patients. But, if the patient were indeed incompetent, how could the patient give his/her informed consent? Without the patient's consent, physicians refuse to issue certificates of incapacity. Without the certificates, agents cannot make health care decisions (and other decisions) for their principals. We have a classic "Catch-22" [4] situation.

The statutory form AHCD goes on to provide:

> "If I mark this box [ ] and enter my signature, my agent's authority to make health care decisions for me takes effect immediately _____."

While this provision in the AHCD may at first blush appear to resolve the Catch-22, it comes up short for three reasons:

1. Clients are reluctant to give an agent the right to make health care decisions for them when the client is still in good health. In the humble experience of this writer, I cannot recall one instance where a client signed the clause granting the agent authority to make health care decisions immediately.

2. Even if the client authorized the AHCD to become effective immediately, the term "health care decisions" is not defined in the AHCD. Thus, the client's signature authorizing the AHCD to become effective immediately may not necessarily authorize release of medical information.

   California Probate Code Section 4690 provides that if there is a question concerning the capacity of the principal, the agent may consult with and obtain information needed from the principal's physician. [5] Again, while Probate Code Section 4690 appears to solve the

---

4) *Catch-22* a novel by Joseph Heller, refers to a military term for a regulation that is based on a circular argument. In the book, the protagonist, Yassarian wants to get out of the military for concern of his own life. In order to get out of the military, he must prove that he is crazy. The military brass says that if he is concerned for his own life, he cannot be crazy. Thus, the military refused to release Yassarian from service, a victim of Catch-22.

5) California Probate Code §4690. Incapacity of Principal. If the principal becomes wholly or partially incapacitated, or if there is a question concerning the capacity of the principal, the agent may consult with a person previously designated by the principal for this purpose, and may also consult with and obtain information needed to carry our the agent's duties form the principal's spouse, physician, attorney, a member of the principal's family, or other person, including a business entity of government agency, with respect to matter covered by the power of attorney for health care. A person from whom information is requested shall disclose relevant information to the agent. Disclosure under this section is not a waiver of any privilege that may apply to the information disclosed. Leg.H. 1999 ch. 658 §39, operative July 1, 2000.

problem for the attorney, HIPAA, being a federal statute, preempts state law. Accordingly, Section 4690 could not be used to circumvent the HIPAA requirements.

3. Thirdly, and most important, is that the authorization in the statutory form advance health care directive does not begin to rise to the level of a "valid authorization" as defined in the HIPAA regulations, 45 CFR §164.508(a).

   45 CFR §164.508(c)(1) states the requirements for a valid federal disclosure authorization as follows:

   (1) Core elements. A valid authorization under this section must contain at least the following:
   (i) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;
   (ii) The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;
   (iii) The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure;
   (iv) A description of each purpose of the requested use or disclosure…;
   (v) An expiration date or an expiration event that relates to the individual of the purpose of the use or disclosure…;
   (vi) Signature of the individual and date. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be produced.

The patient's consent contained in the statutory form AHCD is woefully inadequate, lacking in all six of the core elements required for a valid authorization under 45 CFR §164.508(c)(1). The only possible inkling of compliance is the principal's signature, but even so, the form does not provide for a date as required in subparagraph (vi). [Ironically, under California law, if one were relying on the statutory form AHCD as authorization to release and disclose medical information, the form does not even comply with California's own Confidentiality of Medical Information Act (Civil Code §56-56.37)]. [6)]

Until the California State Legislature elects to amend Probate code §4701 to incorporate the core elements of a valid authorization under federal law [45 CFR Sec 164.508(c)(1)], it is recommended that the statutory form AHCD not be used as printed. Rather, the practitioner is advised to modify

the form or create his/her own form, adding language that satisfies both state and federal requirements for a valid authorization for the release and disclosure of protected health information, which authorization shall take effect immediately.

Conclusion

With the passage of HIPAA in 1996 and promulgation of the Health and Human Services regulations in April 2003, many, if not all, trust and power of attorney instruments providing for the substitution of principals by successors upon certification of the principal's incapacity by a licensed physician may have been rendered useless, in part, as it is becoming increasingly clear that such certification may be unobtainable. One of the primary purposes of HIPAA was to ensure the privacy of protected health information of patients in the health care system. What was not intended was the adverse impact the privacy regulations would have on the practice of law in the area of estate

---

6) California Civil Code §56.11 lists the following requirements for a valid authorization:
An authorization for the release of medical information by a provider of health care, health care service plan, pharmaceutical company, or contractor shall be valid if it:
   (a) If handwritten by the person who signs it or is in typeface no smaller than 8-point type.
   (b) Is clearly separate from any other language present on the same page and is executed by a signature which serves no other purpose than to execute the authorization.
   (c) Is signed and dated by one of the following:
      (1) The patient. A patient who is a minor may only sign an authorization for the release of medical information obtained by a provider of health care, health care service plan, pharmaceutical company, or contractor in the course of furnishing services to which the minor could lawfully have consented under [former CC §25-43 (see Fam C §§6900-6925) relating to medical treatment] or [former CC §60-70 (see Fam C §§7000-7143) relating to emancipated minors].
      (2) The legal representative of the patient, if the patient is a minor or an incompetent. However, authorization may not be given under this subdivision for the disclosure of medical information obtained by the provider of health care, health care service plan, pharmaceutical company, or contractor in the course of furnishing services to which a minor patient could lawfully have consented under [former CC §25-43 (see Fam C §§6900-6925) relating to medical treatment] or [former CC §§60-70 (see Fam C §§7000-7143) relating to emancipated minors].
      (3) The spouse of the patient of the person financially responsible for the patient, where the medical information is being sought for the sole purpose of processing an application for health insurance or for enrollment in a nonprofit hospital plan, a health care service plan, or an employee benefit plan, and where the patient is to be an enrolled spouse or dependent under the policy or plan.
      (4) The beneficiary or personal representative of a deceased patient.
   (d) States the specific used and limitations on the types of medical information to be disclosed.
   (e) States the name or functions of the provider of health care, health care service plan, pharmaceutical company, or contractor that may disclose the medical information.
   (f) States the name or functions of the persons or entities authorized to receive the medical information.
   (g) States the specific uses and limitations on the use of the medical information by the persons or entities authorized to receive the medical information.
   (h) States a specific date after which the provider of health care, health care service plan, pharmaceutical company, or contractor is no longer authorized to disclose the medical information.
   (i) Advises the person signing the authorization of the right to receive a copy of the authorization.

planning and the drafting of estate plan documents. Estate planning attorneys would be well advised to revisit provisions contained in their form instruments and modify them as necessary. Until (and unless) Congress decides to amend HIPAA to make it more estate plan friendly, practitioners may wish to include in their advance health care directives language that make the directives operative immediately or authorize the agent's access to and disclosure of protected health information immediately through the use of a valid authorization.