HIPAA and Forensic Practice

Does the Health Insurance Portability and Accountability Act (HIPAA) apply to forensic practice? In particular, do forensic practitioners incur the obligations of "covered entities," as defined in the Privacy Rules (§160.103), a subset of HIPAA? Do our files and the information we compile constitute Protected Health Information (PHI)? If so, what steps must we take to be compliant? Do HIPAA obligations attach to some areas of forensic practice, but not others? Even if forensic practice does not fall under HIPAA regulation, must we still attend to some issues raised by HIPAA?

Mary Connell is a forensic psychologist in private practice in Fort Worth, Texas. Areas of primary interest are child custody and access, pre-employment screening, and capital sentence mitigation. She also engages in some focused assessment of standard of care and related issues in tort litigation.

Gerald P. Koocher trained as a pediatric psychologist and is Professor and Dean of the School for Health Studies at Simmons College in Boston. His forensic interests include child custody, professional liability in mental health practice, substituted judgment in medical situations, and tort litigation involving damages to children.

Introduction

By definition, competent forensic psychologists pay close attention to rules and procedures. As of April 14, 2003 most of us had wrestled, at least superficially, with the HIPAA (45 CFR 160) notification issue and had attempted to determine whether we fell under the rubric of "covered entities," who must to comply in full with the regulations. Most of us probably at least filed for an extension to protract the painful process of trying to become compliant, hoping for divine guidance or at least word from some authoritative source that HIPAA does not apply to forensic practice.

Although the following attempt to explore the issue does not represent an official position of any forensic governing authority, we offer the product of our study in the hope that it will illuminate some relevant aspects of the question. Our disclaimer: do not rely upon our advice as the final word on the matter. Each practitioner must engage in a careful analysis of practice activities that might qualify as "health care" services.

Are you a Covered Health Care Provider?

First, we must determine whether we are "covered entities" based upon whether we provide health care as defined by HIPAA. The Act defines health care as "Care, services, or supplies related to the health of an individual. It includes, but is not limited to…Preventive, *diagnostic*, rehabilitative, maintenance, or palliative care, and counseling, service, *assessment*, or procedure *with respect to the* physical *or mental condition, or functional status, of an individual* or that affects the structure or function of the body…"(See: 45 C.F.R.160.103; italics added for emphasis) along with some other non-psychological activities.

Forensic services do not constitute health services, we argue, as they are intended to serve a legal purpose, often in response to court order or mandate, and are not recognized for payment purposes by third party health insurers. While forensic service may include formulation of a diagnosis, the purpose is not to provide health care or treatment, but rather, to address a question before the court. Thus, unless we change roles and agree to take on a treatment function, our forensic activity does not bring us under HIPAA penumbra.

However, if one does engage in treatment, even if court-mandated, HIPAA regulations become relevant. Under circumstances of court-mandated treatment, the Privacy Rules exclude certain materials from the "Access" rights enjoyed by health care service recipients. That is, information compiled in anticipation of use in *civil, criminal, and administrative* proceedings is not subject to the same right of review and amendment as is health care information in general (§164.524(a)(1)(ii)). Further, inmates do not enjoy the right to gain access and propose amendment to their treatment files (§164.524(a)(2)(ii)), if obtaining a copy would jeopardize the health, safety, security, custody, or rehabilitation of the inmate or of other inmates, or the safety of any officer, employee, or other person at the correctional institution.

The Final Rule does declare information regarding an inmate's treatment to be PHI, but there is also recognition of the need of institutional staff to exchange such information without the inmate's consent. A provision (§ 164.512(k)(5)) was added to permit this disclosure, without inmate authorization, for specified health care and other custodial purposes. Former inmates, parolees, probationers, and supervised releasees are treated as non-inmate individuals with all rights owed to them.

Finally, the practitioner who engages in both clinical and forensic activities must comply with HIPAA in non-forensic areas of practice, but may think it appropriate to continue handling forensic matters as he/she has done historically. In fact, it may mislead recipients of forensic services to offer a privacy notice using HIPAA language, or to otherwise imply that information gathered for forensic purposes qualifies as "protected health information." HIPAA does not establish a *new* right, beyond that heretofore enjoyed by litigants through discovery and cross-examination, to access and amend (challenge) file information. Although some forensic practitioners customarily give litigants the opportunity to review reports for factual correctness, and then provide addenda to reports if factual errors are brought to their attention, the breadth of health record alteration rights afforded patients under HIPAA simply does not apply. By our reading, even if it were to be determined that forensic services are "health care," the access language in the privacy rules (§164.524(a)) specifically shelters forensic data from that right of access, and offering such access remains discretionary.

Forensic requirements have historically exceeded what the Privacy Rule requires

Forensic practitioners who practice thoughtfully and ethically have long exceeded requirements set forth in the HIPAA privacy rules, particularly with regard to informed consent for disclosure of information. Since at least 1992, the APA ethics code has specifically required us to notify clients about limits on confidentiality at the outset of the professional relationship. Competent forensic practitioners carefully explain limits on confidentiality, potential uses and likely disclosures of findings and data, and the purpose of the services and alternatives (e.g., right to remain silent) and document this notification. No competent forensic clinician releases confidential data without a signed consent or court order, and forensic clinicians keep records of what was released to whom and when. While HIPAA privacy rules exempt from consideration the exchange of information for treatment purposes, psychologists, by contrast, have long respected service recipients' right to control the release of treatment information.

Useful Tools

The Privacy Rules and the Security Standards (45 CFR §160, 162, and 164), another part of HIPAA, offer information useful to forensic practitioners, whether or not we are considered to be covered entities. The Security Standards were intended for anyone "who maintains or transmits health information" (§ 142.302) so that even if we are not defined as covered entities, we are responsible to effect reasonable and appropriate safeguards against unnecessary disclosure of the information we maintain, which of course includes PHI we obtain from covered entities. These Privacy Rules and Security Standards assist the practitioner in scrutinizing office practices to: assure that PHI is handled in a way designed to protect the privacy of recipients; define proper deidentification of case information for research or other purposes when deidentification is in order; and clearly define the elements required in an authorization to release information.

Security Standards: The Standards may assist us to identify and correct practices that inadvertently jeopardize privacy. For example, a walk-through may uncover such inappropriate practices as having data on computer monitors visible to examinees; office staff making case-related telephone calls audible to examinees; mailing information or billing statements to litigants, or leaving scheduling messages, at places in which privacy is compromised; and transporting files, with case names visible, between home and office. We recommend that everyone review the Security Standards to avoid inadvertently jeopardizing litigants' privacy and to prevent the inadvertent disclosure of PHI.

Deidentification: Another gem in the Privacy Rules includes a clear definition of proper deidentification of PHI (§164.514(a)(b)), potentially useful when submitting case material for research or publication. Data are deidentified when stripped of identifiers for the individual and the individual's relatives, employers or household members, including the obvious identifiers and others that might not be so apparent. Specific examples include, removing reference to geographic subdivisions smaller than a state (street address, city, county, precinct), including zip code or equivalents except for the first 3 digits of the geographic unit to which the zip code applies if the zip code area contains more than 20,000 people; removal of dates directly related to the individual, all elements of dates, except year (date of birth, admission date, discharge date, date of death); deletion of social security numbers; medical record numbers; health plan numbers; vehicle identification/serial numbers, including license plate numbers; and any other unique identifying number, characteristic or code. The reader is referred to the text for the full listing of information to be removed in accomplishing thorough deidentification.

Authorization: Finally, the "authorization to release information" requirements in HIPAA are quite explicit, and since forensic practitioners rely heavily on information from third party sources of information, we remain aware of what such covered entities require by way of authorization. A proper authorization must include (§ 164.508(c)):

1. A description of the information to be used or disclosed

2. The identification of the persons or class of persons authorized to make use or disclosure of the PHI (we understand this to mean that if you are asking the litigant to complete an Authorization form, the form must state who is being authorized to disclose material to you. It might be an individual or a class of individuals such as “all physicians who have provided treatment)

3. The identification of the persons or class of persons to whom the covered entity is authorized to make the use or disclosure

4. A description of each purpose of the use or disclosure

5. An expiration date or event

6. The individual’s signature and date

7. If signed by a personal representative, a description of his or her authority to act for the individual.

The authorization should be in plain language, intended to provide the individual with a clear understanding of what information is to be released, any potential for re-disclosure to another party or agency, and the purposes for disclosure. A covered entity generally may not combine an authorization with any other type of document, such as a notice of privacy practices or a written voluntary consent.

Further, psychotherapy notes are treated distinctly from all other PHI under the HIPAA privacy rules, and as such, need to be treated uniquely within the authorization. Specifically, authorizations for use or disclosure of psychotherapy notes may not be combined with another authorization for the use or disclosure of other kinds of protected health information (§164.508(b)(3)).

Given these requirements placed upon the covered entities from whom we often seek information, it would behoove us to develop an authorization form that includes the required elements, is specific, and is written in plain language.

Employment Evaluations

Employment evaluations, such as pre-employment evaluations, fitness for duty evaluations, and Worker’s Compensation evaluations, deserve special consideration and are fraught with complications.

Pre-employment evaluation: Given that the sole purpose of such assessment is to formulate an opinion to be used by the employer in a non-treatment capacity, a sound argument can be made that pre-employment assessment does not constitute provision of health care and the information garnered, while potentially relevant to the examinee for treatment purposes, will not be released for such purposes, and is not PHI.

Fitness for Duty Evaluation: According to HIPAA, the results of a fitness for duty exam may be considered to be PHI when the provider administers the test, but will not constitute PHI when the results of the fitness for duty exam are turned over to the employer pursuant to the employee's authorization (§164.501). Further, there is no right of access and amendment except that provided by jurisdictional law. Since our only purpose in doing such evaluation is to respond to a question posed by the employer, and we seek authorization to release the information to the employer prior to undertaking the evaluation, and would not do the evaluation without such release (allowable conditionality under §164.508(b)), it seems clear that the information we gather is not PHI. The person under evaluation understands from the outset that our purpose is not to treat, but rather to assist the employer in a determining fitness. However, HIPAA does not specifically exclude providers of such service and does identify the results of such assessment as PHI, so it is possible that the provider may be considered a covered entity that must comply with HIPAA requirements. HIPAA declares that although fitness for duty statements may not reveal a diagnosis, they do relate to a present physical or mental condition of an individual, because they describe a capacity to perform the physical or mental requirement of a particular job. Further, if these statements were created or received by a "covered entity," they are individually identifiable health information deserving of the privacy protections afforded by the Act. Thus, by HIPAA reasoning, if we are covered entities, the product of our work is PHI, and if we create PHI, through, among other activities, diagnosis or assessment, then we are covered entities.

Worker's Compensation Evaluation: Evaluation for Worker's Compensation and similar programs do not fall under HIPAA (§164.512) regulations. Covered entities, however, must comply with the "minimum necessary" rule regarding PHI unless the law requires disclosure of the full record. This rule states that one should limit disclosure of PHI to only that information minimally necessary to facilitate the acceptable purpose for the disclosure.

Summary

The assessments undertaken by forensic practitioners in response to a question before a court of law are not intended to inform, guide, or provide treatment. Such assessments do not qualify for most third party health insurance coverage, and thus do not qualify as health care services. Thus, HIPAA and the privacy rules included therein do not apply, in our opinion, to forensic assessment. Court-mandated treatment adds complications, but generally occurs under fairly clear guidelines within the statutory law of the relevant jurisdiction. HIPAA language repeatedly indicates that the intent of the act does not include replacing or negating existing law or interfering with the smooth functioning of existing programs, such as the Worker's Compensation program, and that individual jurisdictions may have more stringent requirements for handling information that those of the privacy rules, and that in such case, the jurisdictional law prevails. When the jurisdictional law remains silent on a point, the relevant HIPAA statute applies.

It appears, then, that practitioners working solely in forensics can reasonably argue that their forensic assessments in private practice do not fall within the ambit of HIPAA for the following reasons. First, the services provided via forensic practice are provided not for therapeutic purpose, but rather to respond to a psycholegal question or need. Second, the services are provided not at the request of the person being evaluated, but instead at the request of another party or entity outside the health care system. Third, forensic services fall outside health insurance coverage, because they do not constitute health care. Fourth, forensic psychologists do not ordinarily transmit data electronically except in the specific ways for which consent has historically been obtained from the litigant. Fifth, no new protections or rights accrue to examinees by way of HIPAA compliance, that fail to flow if we do not achieve compliance (i.e., no new right of access and amendment of information gathered in anticipation of litigation, no additional opportunities beyond those presently extant to control the flow of information). Finally, it can be noted that forensic practitioners have historically handled information amassed in forensic work with at least as much regard for the individual's privacy as the laws governing such transactions permit.

On the other hand, the argument that forensic practitioners do need to be HIPAA compliant might include the following considerations. First, diagnosis and assessment with respect to the mental condition or functional status of the individual may indeed constitute health care, and therefore, those who provide health care may be considered by HIPAA to be covered entities. Second, by receiving health care information about a litigant, we assume the burden of handling PHI, and the need to provide assurance that we handle it in a secure way. Third, the ultimate legal question of whether as to covered entity status will likely fall to case law for settlement, so that it may prove less expensive and burdensome to become compliant than to become the case that decides the issue.

What is involved in becoming compliant?

A number of compliance packages currently available on the market focus on psychological practice and may be helpful. Alternatively, the highly energetic and resourceful practitioner could achieve compliance independently of such products, by reading the Act, the Privacy Rules, and the Security Standards and adopting the necessary changes. The steps to follow include developing a series of forms, making some changes in the way your office runs, and keeping records of the compliance efforts you make. Necessary forms address, but are not limited to, the following: 1) a privacy policy that is disseminated one time to all service recipients and that details how PHI is handled in your office, 2) rights of the examinee to control and access PHI, how to register complaints, and a number of other necessary ingredients; 3) acknowledgement of receiving the privacy policy; 4) authorization to release information that specifies each of certain kinds of PHI; 5) request for limitations in contact such as telephone numbers, addresses, or email addresses to which the examinee would not want communications sent; 6) request for accounting of PHI release events; 7) request to access and amend PHI; and 8) response to request to access and amend PHI.

Some additional steps to ensure that adequate security exists to prevent unauthorized or unintended disclosure of PHI include, but are not limited to, the following: 1) identifying a Privacy Officer; 2) training staff on handling of PHI; 3) developing a record for accounting of release of PHI; 4) developing a method to notify the examinee of unintended disclosure; and 5) establishing business agreements with such entities as you exchange identifiable PHI, possibly including test scoring services, agencies that receive your reports and store them, and records storage facilities.

This is not a complete list of the steps one would take to become compliant, but may provide a sampling of the kinds of activities that are required, and the reader is urged to utilize a package or a consultant, or to research the law thoroughly, in order to achieve compliance. Most of the packages we examined included checklists and forms to document compliance actions taken. Compliance will not come effortlessly, but the costs will likely assure that you minimize risk of running afoul of the latest intrusion of federal regulation into professional practice.

Additional Resources:

HHS HIPAA web site = http://www.hhs.gov/ocr/hipaa/
Code of Federal Regulations lookup site: http://www.access.gpo.gov/nara/cfr/