



American Hospital  
Association

# Quality Advisory

*(Call 202-626-4629 if you have trouble receiving this five-page update)*

## -- UPDATE --

### **AHA Requests Government Guidance on JCAHO's Plans to Mine Patient Data**

November 3, 2005

The AHA today asked the federal government for guidance on patient privacy concerns raised by the Joint Commission on Accreditation of Healthcare Organizations' (JCAHO) plans to become a "purveyor of performance data analysis for a variety of purposes."

Meeting in Washington with the Department of Health and Human Services (HHS) Office for Civil Rights (OCR), the AHA said hospitals need expeditious guidance before the end of the year to help them deal with how JCAHO's plans impact Health Insurance Portability and Accountability Act (HIPAA) compliance requirements. OCR is specifically responsible for enforcement of HIPAA's patient privacy requirements. Its guidance is critical, the AHA said, because JCAHO's planned expansion into the data mining business appears to have made patient privacy an "afterthought."

The AHA described its concerns to OCR over JCAHO's plans to seek patient-level data from accredited hospitals and use it for purposes unrelated to accreditation. We explained the serious patient privacy concerns these plans create for hospitals and requested that OCR issue specific guidance. Under federal law and the Department of Justice's recent interpretations of criminal prosecutions for HIPAA violations, generally it is the hospital – and not its business associate – that is at risk for civil and criminal penalties if JCAHO's uses of hospitals' patient information are found to be out of compliance with HIPAA requirements. The precise requests we made are detailed in the attached legal analysis prepared by the AHA's outside HIPAA legal counsel, Hogan & Hartson LLP.

In an Oct. 31 letter to accredited hospitals, the JCAHO admitted that HIPAA requirements "may eventually require adjudication by (HHS)."

Because this guidance is so critical to hospitals' ability to protect patient privacy, the AHA will:

- **Disseminate promptly to all hospitals any guidance that OCR issues, and**
- **Help hospitals seek appropriate amendments to the 2006 JCAHO Accreditation Survey Contract that may be necessitated by such guidance.**

Questions on this Update and AHA's activities can be directed to Don Nielsen, M.D., senior vice president for quality leadership (312-422-2708, e-mail [dnielsen@aha.org](mailto:dnielsen@aha.org)) or Lawrence Hughes, regulatory counsel and director, member relations (202-626-2346, e-mail [lhughes@aha.org](mailto:lhughes@aha.org)).

## **HIPAA IMPLICATIONS FOR HOSPITALS OF JCAHO DATA PROPOSALS**

November 1, 2005

This is in response to your request for a brief summary of the legal issues for hospitals raised by certain business activities that the Joint Commission for Accreditation of Health Care Organizations (JCAHO) proposes to undertake within the scope of the Health Insurance Portability and Accountability Act (HIPAA) business associate agreement required to obtain accreditation services from JCAHO. For the reasons summarized below, we believe it is likely that the contractual arrangements with hospitals under which JCAHO proposes to develop its data business will create new compliance issues for hospitals under the HIPAA Privacy Rule. Depending on the applicable state laws, hospitals also may be subject to added risk under state law.

### **JCAHO Business Plans**

Based on actions taken by JCAHO this year, and statements by Dr. Dennis O’Leary in letters to both the American Hospital Association (AHA) and others, we understand that JCAHO is interested in developing a “data business” in which it would use patient-identifiable data obtained from hospitals that it accredits to prepare customized reports for third parties, including but not limited to insurance companies and other payers. These reports could relate to a third party’s commercial interests, such as modifying payments to hospitals and physicians, research on health outcomes, quality of care, or other projects of interest to the third party. Based upon what JCAHO employees have told us, it also wishes to permit JCAHO employees to use patient information obtained in the course of accrediting hospitals to publish studies relating to topics in some or all of these areas.

Unlike other entities that facilitate research and analyses by academic researchers, pharmaceutical and device manufacturers, and payers, JCAHO does not propose to enter into data use agreements with the hospitals it accredits or to use privacy board or institutional review board (IRB) waivers as required by the HIPAA privacy rule for the use of protected health information (PHI) in these activities. Rather, it proposes to ensure that the terms of the contract for accreditation services and the Business Associate agreement required under HIPAA for such accreditation, include general language that arguably authorizes JCAHO to use patient information to which it has access for accrediting a hospital in developing new accreditation products, marketing its data resources to third parties, and conducting the research that it proposes to publish. These activities create concerns for hospitals specifically because under the terms of the federal law and interpretations by the Department of Justice, generally it is the hospital and not its business associate that is at risk for civil and criminal penalties if these activities are found to be out of compliance with the regulation.

### **Issue 1: Minimum Necessary Amount**

*JCAHO Proposed Activity.* Currently, hospitals aggregate their patients’ data in responding to the quality indicators that JCAHO uses in planning a hospital’s survey and preparing reports for the public. JCAHO is interested in obtaining actual patient level data from hospitals that it accredits instead of these aggregates. Such access to patient-data would allow

November 1, 2005

Page 2

JCAHO to prepare the aggregate analyses now furnished by the hospital, but also is more valuable for JCAHO to use in its research and data business.

*HIPAA Implications.* One of the key “general rules” established by the HIPAA Privacy Rule is that a hospital must take steps to limit the information disclosed, even to a business associate, to the minimum necessary information for the purpose – in this case, accreditation of the hospital. 42 C.F.R. 164.502(b)(1). JCAHO has provided no evidence that the aggregate reports on quality indicators that a hospital currently furnishes are inadequate to accredit the hospital. Conversely, there is no evidence that in order to perform accreditation, routine JCAHO access to or possession of copies of a hospital’s patient-level information is necessary, other than during site visits by surveyors, and when the hospital submits evidence of standards compliance, and (in rare situations) sentinel event information reported by a hospital.

*Request for OCR Guidance.* Because JCAHO’s differing interpretation is causing confusion in the hospital community, the HHS Office of Civil Rights (OCR) guidance is needed indicating whether making patient level information or copies available to JCAHO as a requirement of the performance measurement system exceeds the minimum necessary for accreditation of the hospital, in light of the fact that aggregate data previously have been sufficient.

## **Issue 2: Permissible Use of PHI By A Business Associate**

*JCAHO Proposed Activity.* JCAHO says that it would like all hospitals accredited by JCAHO to let it maintain their patient level data in its own databases “to improve JCAHO’s accreditation process.” JCAHO believes that it can use the data reported by hospitals, and other information in its possession, for its *own* purposes, such as “improving the survey and accreditation process,” for research and publications to improve patient safety, and to develop new accreditation standards, as well as for preparing reports and other analyses that it sells to third parties. It proposes that hospitals construe the general category of “accreditation services” authorized by the accreditation agreement and business associate agreement as authorizing these JCAHO uses of patient information disclosed by the hospital for the survey and accreditation process. JCAHO maintains that its own activities should be considered the “health care operations” of the hospital that is seeking accreditation.

*HIPAA Implications.* One of the general rules of the HIPAA Privacy Rule is that in the absence of patient authorization, a hospital (and its business associates) are prohibited from using patient information for any purpose except as specified by the privacy rule. 42 C.F.R. 164.501(a). If a hospital has engaged JCAHO *only* for providing the survey and accreditation, the regulation prohibits the business associate from using the PHI made available for this purpose for other activities. These proposed uses of the hospital’s patient information do not appear to be for the accreditation of the disclosing hospital, but rather for JCAHO’s own research and product development activities.

It seems clear that, in discussing the HIPAA Privacy Rule requirements promulgated in 2000, in 2002, and in a more recent “FAQ,” the Department of Health & Human

November 1, 2005

Page 3

Services (HHS) has concluded that a data use agreement is the appropriate mechanism for hospitals to permit JCAHO access to patient level data for JCAHO's own purposes of improving its accreditation process or the accuracy of its quality reports to the public. Any hospital that also wishes to engage JCAHO as a business associate for other purposes such as analyzing its data for improving the quality of care at its own hospital can make appropriate arrangements for HIPAA Privacy Rule compliance with respect to these activities, rather than entering into a general template agreement for an extensive, unspecified package of "accreditation services" that may or may not match the activities authorized by the disclosing hospital.

The HIPAA Privacy Rule is clear that PHI of one hospital cannot be used for the purposes of another hospital, except in limited circumstances and with very specific controls. We have found nothing in the regulation that would support JCAHO's argument that JCAHO's own research publications and the development of its accreditation products can be considered an authorized activity of a hospital that is undergoing survey and accreditation simply because they are designed to improve quality of care. This reasoning would permit a hospital to disclose PHI for virtually any academic, public health, drug or device company research, as it also is intended to improve the quality of care. It appears that the HIPAA Privacy Rule already addresses this very set of issues when it specifically provides that where a third party wishes to have access to a hospital's PHI for research and/or product development, it should enter into a data use agreement with the hospital permitting use of a limited data set for its research, or obtain a waiver of patient authorization from a privacy board or IRB for the specific research project, or obtain the authorization of patients for the specific project. Nothing in the HIPAA Privacy Rule would exempt JCAHO research and product development from these requirements.

*Request for OCR Guidance.* HHS Office of Civil Rights guidance is needed to confirm that as a business associate, an accrediting body cannot use patient information obtained to perform its duties as a business associate for its own research and product development activities. With respect to the multiple private entities that provide accreditation, OCR guidance is needed to clarify that the research and accreditation products developed by these entities are no different than the research and data services products developed by various health care product and services vendors, and that the HIPAA Privacy Rule's provisions for research govern HIPAA compliance where a business associate wishes to engage in research.

### **Issue 3: Commercialization of Accreditation Data**

*JCAHO Proposed Activity.* JCAHO believes that because it has not and will not promise to keep the hospital's performance on quality measures confidential, it has wide discretion to use the reported information for a broad range of general purposes. As noted above, the performance data in JCAHO's possession generally are aggregates prepared by the hospital using its own patient information to comply with JCAHO requests as part of the accreditation. JCAHO maintains that because these data are "aggregates" when JCAHO receives them, HIPAA does not apply, and it can use the data for such purposes as preparing customized cuts and analyses for third parties such as insurance companies or other payers. It asserts that this is a policy and business issue and not a HIPAA compliance issue, and that its general interest in promoting quality of care trumps hospitals' interests in protecting their patients' data.

November 1, 2005

Page 4

*HIPAA Implications.* The provision of the HIPAA Privacy Rule that governs here is the general rule that prohibits a hospital from using its own patients' data for activities other than as specifically permitted by the privacy rule. 42 C.F.R. 164.502(a). Thus, the issue is whether the hospital -- in preparing the aggregates required by JCAHO in order for the hospital to be accredited -- is using its patients' PHI for purposes of its own accreditation, or whether the performance reports being requested by JCAHO are instead related to JCAHO's own research and commercial activities. For example, the HIPAA Privacy Rule would prohibit the hospital from complying with any other researcher's request for an analysis of patient data for the third party researcher's purposes, unless it complied with the HIPAA Privacy Rule provisions governing research. The question is whether, as a condition of obtaining accreditation -- which is a precondition for reimbursement by many payers -- JCAHO is compelling the hospital unwittingly to use its PHI for JCAHO's commercial and/or research purposes.

This question has become more salient as JCAHO has expanded its data business interests and simultaneously proposes increasing the number and type of "quality indicator" reports that it may require of the hospitals that it accredits. JCAHO's appearance of a conflict of interest here is what creates concern for hospitals. If JCAHO uses performance data (reported in aggregate form) for its own commercial activities, hospitals cannot be confident that as JCAHO proposes to add new performance measures and reports, the hospital is using its patient data to prepare analyses for its own accreditation rather than for JCAHO's data business.

It is clear that the hospitals could not use or disclose their PHI for the purposes of the third parties that might request the reports -- unless they comply with the HIPAA provisions relating to research uses of PHI by the hospital. To the extent that JCAHO personnel have suggested that adding new performance measures will help it to improve the accreditation process in general by identifying new standards and the like, the line between the hospital's health care operations and JCAHO research and product development activities is murky. But when JCAHO commercialization of these analyses is added to the mix, the line appears to have been crossed. In this context, JCAHO requiring a hospital to perform such analyses as a condition of accreditation, or a hospital unwittingly authorizing JCAHO to do so through a business associate agreement that permits expansive use of PHI for "accreditation services," arguably heightens compliance risk.

*Request for OCR Guidance.* OCR guidance is needed to clarify for hospitals that the HIPAA business associate agreement required for survey and accreditation does not require them to give JCAHO copies of patient records, to perform analyses or grant data rights for JCAHO's commercial and product development purposes, pursuant to such business associate agreement. OCR guidance is needed to clarify that like any other entity in the United States that wishes to use patient information maintained by a hospital, JCAHO must ensure that its research and product development activities comport with the HIPAA Privacy Rule provisions governing research by third parties.