

Coming Soon: Second Data Bank on Fraud and Abuse

BY MARK A. KADZIELSKI, JD

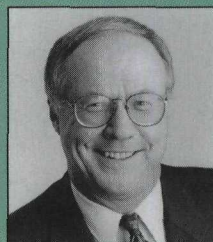
As a key part of the overall government crackdown on healthcare fraud and abuse, the Healthcare Integrity and Protection Data Bank (HIPDB) is scheduled to open in the fall of 1999 (although its opening has been delayed once and may be delayed again). The HIPDB is, in many respects, a more refined version of the National Practitioner Data Bank (NPDB), which was established by the Health Care Quality Improvement Act of 1986. NPDB has been open since September 1, 1990, collecting information on healthcare professionals, primarily physicians and dentists, in connection with adverse licensure, clinical privileging, and malpractice actions.¹ The HIPDB will contain information about adverse actions against all healthcare providers, suppliers, and practitioners. Although the new database represents a step forward, its broad definitions and exclusion of hospitals from access to its information present some serious problems.

WHY A SECOND DATA BANK?

The HIPDB was enacted as part of the Health Insurance Portability and Accountability Act (HIPAA) of 1996, which focused on the need to combat healthcare fraud and abuse. Among other actions, it established a national data bank to receive and disclose certain final adverse actions against healthcare providers, suppliers, or practitioners. The secretary of Health and Human Services (HHS) is required to maintain this data bank, which will be operated in the same fashion as the NPDB, under the auspices of the same HHS department, the Health Resources and Services Administration, Bureau of Health Professions.

WHAT WILL BE INCLUDED IN THE HIPDB?

The HIPDB requires reporting by federal and state agencies that license and certify healthcare providers, suppliers, or practitioners, and by health plans that exclude healthcare providers, suppliers, or practitioners. These entities must report to the HIPDB five types of final adverse



Mr. Kadzielski is the partner in charge of the West Coast Health Practice at Akin, Gump, Strauss, Hauer & Feld, LLP, Los Angeles.

actions against a healthcare provider, supplier, or practitioner:

- Civil judgments in federal or state court related to the delivery of a healthcare item or service
- Federal or state criminal conviction related to the delivery of a healthcare item or service
- Actions by federal or state agencies responsible for licensing and certification
- Exclusion from participation in a federal or state healthcare program
- Any other adjudicated action or decision that the secretary of HHS establishes by regulations

Final adverse actions against providers, suppliers, or practitioners must be reported, regardless of whether the subject of the report is appealing the action. Significantly, federal and state agencies and health plans, but not hospitals, will be permitted to query the HIPDB.

FRAUD AND ABUSE DEFINED BROADLY

In its proposed regulations, the HHS Office of the Inspector General (OIG) has construed the term "healthcare fraud and abuse" broadly. The OIG has specifically indicated that reportable actions are those related to provider, supplier, and practitioner practices that are inconsistent with accepted sound fiscal, business, or medical practices, and directly or indirectly result in:

- Unnecessary cost to the program
- Improper payment
- Services that fail to meet professionally recognized standards of care or that are medically unnecessary
- Adverse patient outcomes, failure to provide covered or needed care in violation of contractual arrangements, or delays in diagnosis or treatment²

The OIG has thus cast a wide net to collect information about conduct that falls within these broad parameters.

Moreover, the OIG has chosen, at this time, not to define the term "healthcare abuse" and will proceed on the assumption that Congress

Continued on page 15

LAW

Continued from page 12

intended a broad interpretation of that term. In the proposed regulations the OIG indicates its belief that healthcare abuse would include "verbal, sexual, physical or mental abuse, corporal punishment, involuntary seclusion or patient neglect or misappropriation of patient property or funds." The OIG seeks comments on whether such a broad definition, or any definition that would capture the range of the adverse actions specified by Congress, should be included in the regulations.

The definition of "health plan," the only private entity that must report and which may query the HIPDB, is also rather broad. Health plans are defined as including those plans, programs, or organizations that "provide health benefits, whether directly or through insurance, reimbursement or otherwise." The proposed regulations specifically acknowledge that credentials reviews and fraud investigations are often conducted at the corporate level by organizations offering and managing managed care plans or other health-benefit plans or services, and therefore the broad construction of the term "health plan" is justified.

SOME KEY PROBLEMS

In addition to its ambiguities and its broad definitions, the HIPDB expressly excludes acute care hospitals from accessing its information. Since the NPDB, acute care hospitals have been in the forefront of reporting information on corrective actions against practitioners and using such information from the NPDB in the peer review and credentialing process. The HIPDB reverses this traditional flow of credentialing information.

In the past, managed care organizations often contracted with physicians and other healthcare professionals if they already had met acute care hospitals' credentialing standards. Moreover, in the explosion of managed care contracting that has occurred, much of the managed care credentialing process, including NPDB checks, has been conducted by medical groups, independent

physician associations, and others that have been "delegated" or "subdelegated" by a managed care organization to obtain this information. Through HIPAA and the HIPDB, Congress, and now the OIG, is clearly holding health plans responsible for obtaining such information from the HIPDB themselves. This new accountability for managed care organizations will create more liability exposure for them whether they retain or terminate practitioners with adverse HIPDB reports.

Managed care organizations will now receive more requests for information on physicians and healthcare professionals from acute care hospitals, and will need to have legally correct information-sharing agreements with hospitals. They will also need to make tough decisions regarding provider contracting and credentialing.

The inability to access the HIPDB will be frustrating for hospitals and healthcare delivery systems that have instituted corporate compliance programs. Healthcare compliance programs must deal with practitioner credentialing issues, particularly questions relating to practitioners who do not participate in Medicare, or who have civil judgments or sanctions against them. If hospitals cannot access HIPDB information promptly and directly, but are held to a high corporate credentialing standard, their hands will be tied. Whether or not Congress will recognize this and amend HIPAA to permit hospitals to access the HIPDB remains an open question. Nevertheless, making tough credentialing decisions regarding practitioners is an essential process, one that will not be made any easier by the HIPDB. □

NOTES

1. Mark A. Kadzielski, "Practitioner Data Bank to Open Soon," *Health Progress*, March 1990, p. 87; "Does the Data Bank Inhibit Peer Review?" *Health Progress*, December 1990, p. 58.
2. 63 Fed. Reg. 58341 (October 30, 1998).

NET GAINS

Continued from page 13

"Although there should be active involvement by the IS [information services] division, the planning and development should be driven by someone who is clearly focused on the organization's business and operational goals."

Think Big But Start Small Although you need an overarching vision of the ways an intranet can benefit your organization, you should begin by implementing services that add immediate value. CHI began by developing an online telephone directory, because it was easy to use and benefited a large number of users.


Avoid Scattershot Development If you allow different groups to create their own intranet sites or pages without coordination or oversight, you may soon find your organization mired in information chaos.

If You Build It, They May Not Come The toughest part of getting your money's worth from an intranet is in motivating employees to actually use it. "To be successful, an organization must actively work at changing expectations and culture," says Paulson.

Create a Realistic Budget Much of an intranet's appeal lies in its low cost of implementation. Even so, you should not implement one without first establishing a realistic budget that includes the costs of staffing it and creating and maintaining its content.

Go See an Intranet in Action "Healthcare systems often create their own intranets without ever having seen one," says Paulson. "It's better to visit a system or hospital that already has an intranet and watch it in action."

When they are successfully implemented, healthcare intranets make better information available to more people at a lower cost. An intranet's value does not come from its technology. It comes from leaders' readiness to provide employees with a new tool and encourage them to improve the way work is done. □

 Contact Tom Lawry at tclawry@verus-tech.com, or at 4628 175 Ave., SE, Bellevue, WA 98006; phone: 425-643-7117; fax: 206-643-0302.