Misinterpreted Facility Directory Rules Confuse Patients, Thwart Clergy Members

In the first six months of HIPAA privacy implementation, one of the most confusing and problematic sets of provisions in the new privacy rule has evidently involved facility directories.

Some patients who’ve exercised their right to not be included in the facility directory have been surprised and disappointed their friends and loved ones had no way to find them.

Many members of the clergy — accustomed to easy access to hospitals for visiting sick parishioners — have had roadblocks thrown in their way due to misinterpretations of what the new privacy law requires.

continued
For example, misleading information has spread through many communities that, under HIPAA, clergy could no longer visit their sick parishioners in the hospital, or print their names in church newsletters. Some church bulletins carried requests for parishioners to call the church if they knew of parishioners who were hospitalized, since hospitals were no longer allowed under HIPAA to tell clergy about patients.

Rather than barring the clergy from hospitals, the drafters of HIPAA rules and regulations took great pains to add language that would preserve the clergy’s right to comfort sick parishioners in health care facilities. The rights of the clergy to continue their work in health care facilities are embodied in two exceptions to HIPAA rules. But first, what are the general rules governing patient information in facility directories?

Consenting or Opting Out

The final privacy regulations (Sec. 164.510) permit covered entities to include four elements of protected health information in facility directories if patients do not object or wish to place restrictions on disclosures: (1) the patient’s name, (2) his or her location in the facility, (3) the patient’s general condition (in terms that don’t reveal specific medical information, using terms such as “fair,” “critical” and “stable”), and (4) religious affiliation.

Covered entities must get a patient’s verbal consent to list this information in the directory. And patients can decide to be excluded from the directory altogether, to merely having their names listed (which would permit phone calls), to omit their location (which would inhibit visitors), and so forth. They may withhold their religious affiliation if they don’t want to be visited by the clergy, who are the only ones permitted to learn a patient’s religion.

If patients decline to be listed in the facility directory, their family and friends (and the clergy and others) won’t be able to find them when they stop at the reception desk or try to telephone them. It’s easy for a hospital patient, who may be in pain and/or uneasy about his or her physical appearance, to reply: “I don’t want to see or hear from anyone.” But it’s essential that you help patients understand that “opting out means you won’t have any visitors or get any phone calls, flowers or other deliveries. No one will know you are here.”

If patients opt out of the directory, a computer entry can be made indicating that the patient wishes to be anonymous. In some cases involving domestic disputes, patients may be admitted to a hospital under a pseudonym.

Who Can Access Directory Info?

HIPAA privacy regs also require you to inform patients of the persons to whom you may disclose directory information, and permit patients to object to all or certain specified disclosures (e.g., to an abusive spouse, the clergy, the press). Unless modified by patient preferences, covered entities are expected to release directory information to any person who asks for a patient by name, except for members of the clergy, who can access patients of their denomination without knowing their names.

These disclosures to the clergy alone represent a slight change from the original privacy Notice of Proposed Rulemaking, “which did not require members of the general public to ask for a patient by name in order to obtain directory information and which, in fact, would have allowed covered entities to disclose the individual’s name as part of the directory information,” according to the final rule preamble. In the final rule, population-wide data of this nature are now reserved for religious purposes only.

Despite popular misconceptions to the contrary, HIPAA architects included separate language that guarantees continued free access to sick parishioners by the clergy. In fact, covered entities would not be permitted to
include religious affiliation in their directories at all if the intent was not to have members of the clergy access this information. No one else is permitted to access religious affiliation.

Members of the clergy can ask facilities for lists of patients in their denomination without having their names. In a Q&A devoted to this subject, HHS indicates that: “…a hospital may disclose the names of Methodist patients to a Methodist minister unless a patient has restricted such disclosure.”

The term “clergy” is not defined in the HIPAA rule, but will most certainly include priests, rabbis and ministers of all denominations who work in the community.

The preamble to the Dec. 28, 2000, final rule (FR 82522) clarifies that “…the rule in no way requires a covered health care provider to inquire about the religious affiliation of an individual, nor must individuals supply that information to the facility. Individuals are free to determine whether they want their religious affiliation disclosed to clergy through facility directories.”

The preamble goes on to explain, “Although this section provides a special rule for members of the clergy, it does so as an accommodation to patients who seek to engage in religious conduct. For example, restricting the disclosure of an individual’s religious affiliation, room number, and health status to a priest would cause significant delay that would inhibit the ability of a Catholic patient to obtain sacraments provided during the last rites.”

**Protects for Victims of Abuse**

In its preamble to the Aug. 14, 2002, final regulation (FR 53213), HHS responded in this manner to a commenter who suggested that the now-abandoned consent requirements be retained to protect victims of domestic violence: “…the provisions that provide real protections to victims of domestic violence in how information is used or disclosed … are provisions that allow an individual to object to disclosure of directory information … that provide an individual the right to request

---

**Rules on Facility Directories and Incapacitated Patients**

When, due to emergency circumstances or incapacity of the patient, the patient has not had a chance to decide whether he or she wants to be listed in the facility directory, these disclosures may continue to occur, if such disclosure is (a) consistent with any known prior expressed preference of the individual and (b) in the individual’s best interest as determined in the professional judgment of the provider. In the preamble to the Dec. 28, 2000, final privacy regulation (FR 82521), HHS listed several factors that the government “encourages covered entities to take into account when making decisions about whether to include an incapacitated patient’s information in the directory:

(1) Whether disclosing that an individual is in the facility could reasonably cause harm or danger to the individual (e.g., if it appeared that an unconscious patient had been abused and disclosing the information could give the attacker sufficient information to seek out the person and repeat the abuse);

(2) Whether disclosing a patient’s location within a facility implicitly would give information about the patient’s condition (e.g., whether a patient’s room number revealed that he or she was in a psychiatric ward);

(3) Whether it was necessary or appropriate to give information about patient status to family or friends (e.g., if giving information to a family member about an unconscious patient could help a physician administer appropriate medications); and

(4) Whether an individual had, prior to becoming incapacitated, expressed a preference not to be included in the directory. The preamble stated that if a covered entity learned of such a preference, it would be required to act in accordance with the preference.”

The privacy rule preamble indicates that when incapacitated individuals “subsequently gain the ability to make their own decisions, health facilities should ask them within a reasonable time period for permission to include their information in the facility directory.”

The final rule on Dec. 28, 2000, expanded the circumstances under which covered entities can disclose directory information without a patient’s agreement. Whereas the proposed privacy rule allowed such exposures only for patients who are incapacitated, the final rule also permits such disclosures in emergency treatment circumstances. The preamble to the final rule (FR 82522) indicates that disclosures are also permitted “when a patient is conscious and capable of making a decision, but is so seriously injured that asking permission … would delay treatment such that a patient’s health would be jeopardized....”

Go to www.AISHealth.com to sign up for 4 different FREE e-mail newsletters — Business News of the Week, Government News of the Week, Today in E-Health Business and MD Practice Alert.
restrictions and that grant an individual the right to request confidential communications."

Important caution: When it comes to protecting the rights of all patients — and especially victims of abuse — it’s important to be sensitive to whether disclosing a patient’s location is tantamount to disclosing his or her medical condition (e.g., if he or she is in the psych ward).

What should your organization do if/when a gunshot victim requests exclusion from the facility directory, and the police are asking you about him? Disclosures to law enforcement, which have spawned equally confusing scenarios for some covered entities, will be addressed in the November 2003 Report on Patient Privacy.

### Verbal Agreements Are Trouble

Section 164.510 of the final privacy regs permits a covered entity to ask verbally, and obtain verbal direction from patients regarding, whether they agree to being listed in the facility directory (or object to being listed or wish to restrict disclosures). While you are permitted to inform a patient of your directory policies verbally, and you can “hear” a patient’s verbal consent for (or restrictions on) disclosures, covered entities would be well advised to:

1. Provide patients — in their Notice of Privacy Practices, or in another buck slip provided at registration — with a very brief, monosyllabic written summary of what it means to be excluded from the directory (e.g., a piece of paper nurses can refer to if patients insist on opting out), and
2. Document, and maintain records of, their patients’ consent, objection or restrictions re the directory — not by having patients sign anything, but by having a presiding employee initial and date some record of their witnessing of consent.

Absent this type of recordkeeping — which is certainly not required by HIPAA and which some may find excessive — formal proceedings later on could boil down to little more than playground-style “he said, she said.”

Is this worth the effort? If covered entities wind up defending themselves against HIPAA allegations, the charges may well include violations of patients’ rights. There are only a few places in HIPAA regulation where covered entities can violate a patient’s rights in a blatant (and potentially harmful) way, and this is one of them.

### Hospitals Agonize Over Students’ Career Shadowing Under HIPAA

As people who are passionate about health care, privacy officers dread the thought of shutting down observation programs for high school students interested in a career in medicine because these programs are an effective recruitment tool. But with HIPAA implementation, some privacy officers are worried whether these programs — which generally involve high school students shadowing clinicians — can continue.

“This might prove to be one of the stickiest wickets for HIPAA,” says Candace Foster, HIPAA project leader at Deaconess Hospital in Evansville, Ind. “We are struggling to keep these programs going without compromising privacy.”

There are two sides to this coin. On the one hand, Foster says, these are not medical or nursing schools, so the students aren’t typical work-force members. On the other hand, “they are members of specific, health care-oriented high school classes — and HIPAA allows us to use PHI for educational purposes.”

Foster informally surveyed hospitals about their shadowing programs and found mixed responses to the viability of shadowing under HIPAA. Some hospitals abandoned their shadowing programs on the grounds that patient authorizations are necessary under HIPAA and too cumbersome to obtain. Other hospitals are working on ways to maintain shadowing, such as certifying students as members of the work force.

**Lourdes Hospital** in Binghamton, N.Y., will continue its “New Visions” program, in which 25 high school students spend one to two hours every day at the hospital during the entire school year learning about all aspects of the hospital, says Anne Wolanski, assistant vice president of risk management and corporate responsibility. These future physicians, nurses, etc. “are well-oriented to policies and procedures, and confidentiality is very drilled in.” To minimize the risk of breaches, New Visions participants receive the same orientation as new employees.

**Riverside Healthcare** in Kankakee, Ill., doesn’t allow high schoolers to shadow clinicians in the hospital. Instead, it takes the health care show out on the road, visiting high schools to educate about the profession and interested kids in health care careers, says Chief Privacy Officer Karen Block.

**O’Bleness Hospital** in Athens, Ohio, has tightened its procedures for student shadowing. “We have informed all staff, including physicians, that if they want to sponsor a shadower, they must first report their intent to our volunteer resources department. The shadower gets a brief orientation about confidentiality, HIPAA,
safety, etc., and signs a confidentiality form. They are then allowed to shadow,” says Privacy Officer Tammy Johnson. “If they are coming into direct contact with the patient, we always get the patient’s authorization first.”

Contact Johnson at tjohnson@obleness.org, Foster at Candace_foster@deaconess.com, Wolanski at awolanski@lourdes.com, or Block at Karen_M_Block@rsh.net

**Wireless Networks Can Create Major HIPAA Vulnerabilities**

A hospital or medical group with its electronic medical records available on a wireless computer network is at far greater risk for unauthorized entry (and ultimately, HIPAA breaches) than are facilities with LAN lines.

Within a certain range of a hospital’s unsecured wireless network, all a hacker needs to gain access to confidential patient information is a personal computer and a wireless card, which can be purchased at a computer store or on the Internet for under $100. This practice is called “wardriving,” by which hackers essentially drive around searching for wireless access points (WAPs).

Just last month, the vulnerabilities of a medical group’s wireless network were exposed when a hacker mailed copies of checks and insurance forms containing patients’ names and procedures to a local television station. WRAL, a television station in the Raleigh-Durham area, reported that an information security consultant was arrested for allegedly accessing patients’ confidential information through the unsecured wireless network of Wake Internal Medicine Consultants Inc. in North Carolina. According to WRAL, he wanted to expose the company’s “lax” computer security.

*How does this affect HIPAA compliance?* Since HIPAA privacy standards require the protection of individually identifiable health information, anything that is transmitted electronically through a wireless network and contains PHI is vulnerable. But HIPAA doesn’t set any specific guidelines on how to secure wireless, says Marne Gordan, director of regulatory affairs for TruSecure Corporation, a Herndon, Va.-based company that provides information security intelligence and services. “Any organization that uses wireless technology has a potential to open up vulnerable areas in their environment. HIPAA is a measure of how well you manage whatever you have in your environment,” she says.

Gary Miliefsky, president and CEO of PredatorWatch, Inc., in North Chelmsford, Mass., which supplies network vulnerability management tools, explains that many wireless networks are enabled as “ad hoc” without the proper level of management. “Security has been an afterthought in the wireless network space,” he says.

But wireless networks for some applications are very compelling, and in most cases covered entities can implement relatively simple methodologies to reduce risk to an acceptable level, says Tom Hanks of the health care sector of IBM Business Consulting Services. Hanks explains that for many environments, securing a wireless network can be achieved through WEP (wireless encryption protocol) encryption that is integrated with the wireless equipment. Newer wireless cards and routers come with an option to enable encryption between the PC and the router; but the encryption feature is usually defaulted to “off” when purchased, he says. Some systems may also have older equipment that does not feature encryption, but a simple system upgrade can usually do the trick.

Contact Gordan at info@trusecure.com, Hanks at tomhanks@us.ibm.com or PredatorWatch’s Debra Angeloni at dangeloni@predatorwatch.com.

**More Compliance Resources From AIS**

- **NEW!** A Guide to Auditing and Monitoring HIPAA Privacy Compliance, how-to-it guidance on installing effective HIPAA auditing and monitoring systems. Includes practical templates, tools and documents on a companion CD.

- **NEW!** Sarbanes-Oxley: Best Practices for Private & Nonprofit Health Care Entities, an easy-to-understand, highly practical book detailing specific actions and strategies compliance officers can put in place to achieve organization-wide adherence to these new best practices.

- **✓ Report on Medicare Compliance**, the industry’s leading source of weekly news and analysis on what you can do about billing problems, cost report errors, bad documentation, HIPAA, DRG upcoding and other complex compliance issues.

- **✓ A Guide to Auditing Health Care Billing Practices**, step-by-step guidance on one of the most challenging problems in Medicare compliance.

- **✓ HIPAA Patient Privacy Compliance Guide**, 1,000 pages of practical guidance and “how-to” tools from the nation’s top HIPAA experts.

- **✓ HIPAA Security Compliance Guide**, easy-to-understand summaries of the complex new security regulations, along with sample policies, procedures and other practical compliance tools from top health care security experts.

Visit the AIS MarketPlace at www.AISHealth.com

Copyright © 2003 by Atlantic Information Services, Inc. All rights reserved. Reproduction by any means — including photocopy, FAX or electronic delivery — is a violation of federal copyright law punishable by fines of up to $100,000 per violation.
‘Minimum Necessary’ Creates Maximum Complexity

One of HIPAA’s most challenging requirements is the “minimum necessary” standard, which mandates that the PHI that is used or disclosed be limited to the minimum PHI necessary to accomplish the intended purpose. While this principle sounds relatively simple, implementing “minimum necessary” over a large, complex organization has been a trying task for even the most experienced privacy officers (RPP 7/03, p. 3).

At Casa Grande Regional Medical Center (CGRMC) in Arizona, employees are assigned to one of three levels of PHI access, depending on what they need to get their work done, says Privacy Officer Becky Buegel. These three levels, which are defined in Procedure 4 below, are: (1) full health information access, (2) selective access, and (3) incidental access. For example, many physicians, nurses and other clinicians will have “full access”; people in the billing office and materials management probably need “selective access” because they may need the patient’s name and diagnosis; and the custodial staff will have “incidental access.”

At CGRMC, the challenge of deciding which level of access is appropriate for each job code/position number falls to the department managers as it pertains to their supervisees. Access levels may vary widely from one department to another, even if job titles are the same. For example, the receptionist in the medical imaging department has needs that are somewhat different from those of the receptionist in admitting, Buegel says.

Contact Buegel at rbuegel@casagrande.com.

CGRMC’s Policies and Procedures for Minimum Necessary

I OBJECTIVE:
Casa Grande Regional Medical Center (CGRMC) is required by the HIPAA Privacy Rule to make a “reasonable effort” to limit requests for uses and disclosures of protected health information (PHI) to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. While CGRMC is committed to ensuring privacy and security of PHI, it is important to recognize that there must be a balance between avoiding disclosure of more patient information than is necessary against having sufficient patient information in order to assure proper care. To support its commitment to patient privacy and confidentiality, CGRMC will ensure that appropriate steps are taken to disclose only the minimum amount of PHI needed to accomplish the particular use or disclosure, as required under CFR §164.502(b), as well as other pertinent local, state, and/or federal laws and regulations.

II POLICY:
(1) The CGRMC workforce will follow proper procedures to ensure that only the minimum amount of PHI necessary to accomplish the specific purpose of a use or disclosure is actually used or disclosed.
(2) The CGRMC workforce will request only the minimum amount of PHI necessary to accomplish the specific purpose of the request.
(3) This policy does not apply to the following uses or disclosures:
   (a) Disclosures to or requests by a provider for treatment;
   (b) Uses or disclosures made to the individual who is the subject of the information;
   (c) Uses or disclosures pursuant to an authorization;
   (d) Uses or disclosures required for compliance with HIPAA standardized transactions;
   (e) Disclosures made to the Department of Health and Human Services when disclosure of information is required under the rule for enforcement purposes;
   (f) Uses or disclosures required by law; and
   (g) Uses or disclosures required for compliance with applicable laws and regulations.

III DEFINITIONS:
Protected Health Information – means individually identifiable health information that is transmitted by electronic media; maintained in any medium described in the definition of electronic media; or transmitted or maintained in any other form or medium.

IV PROCEDURE:
(1) All proposed uses or disclosures of PHI will be reviewed by persons having an understanding of CGRMC’s privacy policies and practices, and sufficient expertise to understand and weigh the necessary factors.
(2) The entire medical record will only be used, disclosed, or requested when the entire record is specifically justified as being reasonably necessary to accomplish the purpose of the use, disclosure, or request.
(3) The following categories have been assigned to the CGRMC workforce:
Limiting PHI Access to Outsiders
continued from p. 1

Sometimes outsiders are lumped in with other members of the work force (e.g., volunteers) or designated as business associates (e.g., vendors); sometimes they stand alone. “For any of those people, they have to have a good reason to be there,” says Tammy Johnson, privacy officer at O’Bleness Hospital in Athens, Ohio. “And they must sign a confidentiality agreement. If not, they shouldn’t be there” — a decision generally made by the department manager or nurse supervisor.

How do hospitals approach the application of the privacy rule to these outsiders? The first step for Lourdes Hospital in Binghamton, N.Y., was to categorize outsiders, says Anne Wolanski, assistant vice president of risk management and corporate responsibility. “Outsiders can be categorized first based on the notice of privacy practices, which indicates who is part of your organized health care arrangement,” she says. This includes physicians on the medical staff, providers allowed to write in the patient’s medical record and volunteers who are permitted to help patients while they are in the hospital or receiving care at a Lourdes site.

The next layer is the patients’ visitors and clergy. Access is essentially determined by expressed patient preferences (e.g., opting out from the directory). The third layer is everyone else — notably these outsiders. They prompt a variety of responses, from vendors who are closely tracked (e.g., register, wear a badge) to volunteers subject to extensive privacy-rule training and written confidentiality statements.

To help her think through the management of various classes of outsiders, Johnson does an informal risk

(a) Healthcare Provider – A licensed healthcare professional who provides direct or indirect patient care or consulting service. This includes, but is not limited to: physicians, nurses, respiratory therapists, social workers, etc.

(b) Patient Care – Staff who provide direct or indirect patient care at the request of or referral from a Healthcare Provider. This includes, but is not limited to: admissions, dietary aides, unit clerks, housekeeping, etc.

(c) Healthcare Operations – Staff who work within the organization providing a variety of services that support the delivery of patient care or healthcare operations. This includes, but is not limited to: risk management, finance, business office, health information management, etc.

(d) Administrative – Staff who work within the organization providing administrative support. This includes, but is not limited to: HR, community relations, etc.

(4) The following levels and conditions of access will be assigned to the categories of workforce noted in number (3), above:

(a) Full Health Information Access shall be given to members of the workforce who, based on their duties, need ongoing, regular access to PHI in all forms, while the individual is on duty and performing within the scope of his or her job; such access must be for cause, consistent with job responsibilities, and related to a patient, claim, audit, review, or other legitimate business purposes.

(b) Selective Access shall be given to members of the workforce who need access to certain automated or hard copy PHI on a regular basis for purposes such as directing a call or letter, sorting mail, filing, typing, and similar activities with the scope of his or her job.

(c) Incidental Access shall be given to members of the workforce who do not necessarily need access but may see PHI through incidental use such as fax and copier machines, filing, typing, etc.

(5) Requests for disclosures of PHI will be reviewed on an individual basis in accordance with criteria listed in the policy.

(6) CGRMC may reasonably rely on requests by

(a) Public health and law enforcement agencies in determining the minimum necessary information for certain disclosures;

(b) Other covered entities in determining the minimum necessary information for certain disclosures;

or

(c) By a professional who is a member of its workforce or is a business associate of CGRMC for the purpose of providing professional services to CGRMC, if the professional represents that the information requested is the minimum necessary for the stated purpose.

(7) In the event of disclosures for research purposes, CGRMC will review the documentation of required Institutional Review Board or other approval in determining the minimum amount of PHI necessary.

(8) Knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer.
analysis. “I think to myself, what is the worst-case scenario that could happen if we disclosed PHI to this particular person who is not a work-force member?” For example, what is the relative risk of a drug sales rep talking to nurses for 15 minutes and then leaving, versus bringing in lunch for a 90-minute education session with the nurses in the department? “I analyze the risks and talk to my risk manager and tell her what I think, and we hash it over. Then I take it back to the departments involved and ask for their feedback because nursing knows nursing, etc,” she says, before a final decision is made.

How Certain Outsider Categories Are Managed

Here is a sampling of how hospitals are managing various categories of outsiders:

(1) Volunteers: They are treated as members of the work force, but volunteers need extra support enforcing HIPAA’s privacy protections. “They are at the social center of a hospital,” Cornwell says, because of their exposure to non-treatment-related information about patients, their role in comforting patients and their interaction with friends and families through staffing the front/information desk. Volunteers may be weak links in the privacy chain when asked for patient information. “Some of these ladies have been in our auxiliary for 30 years. They know all the patients and nurses and doctors, so there is a huge likelihood for that information to be used socially,” Cornwell says. For example, suppose they run into a friend at the grocery store, and the friend asks about a mutual acquaintance who’s been admitted to the hospital. The volunteer may feel weird and pretentious saying what she has been instructed to say — something along the lines of “I’m sorry, I’m not at liberty to discuss that” — especially to a close friend. Cornwell suggests volunteers cope by answering a question with a question. If the visitor says “How is Mrs. Smith doing? I heard she is in the hospital,” then the volunteer can respond, noncommitally, “Have you spoken with her husband?”

It can get even tougher when volunteers are manning the front desk, which means disclosing either only directory information or, if the patient opted out, nothing. It’s awkward for a volunteer to say “I’m sorry; we don’t have a patient by that name” when the volunteer knows it isn’t true — especially if the visitor is sure the patient is there. Visitors who are told that black is white may become belligerent. And volunteers are miserable having to lie or be rude. As an alternative, Cornwell says, volunteers at her hospital now say “We don’t have a patient by that name in our public directory.” And they can always call Cornwell for help.

To enhance volunteer safeguards, “we are careful not to put volunteers in certain sensitive areas,” such as risk management and quality assurance, where they could access highly confidential information associated with, for example, case reviews, Wolanski says. “The types of tasks that a volunteer is assigned to probably won’t have them directly involved in looking at a patient’s medical records,” Wolanski says, noting the hospital has always taken that precaution, even before HIPAA.

(2) IT and other certain vendors: Hospitals monitor vendors more closely now, and some vendors are business associates. At Lourdes, “vendors are expected to have an appointment to visit a particular department. We have a vendor policy regarding their need to sign in and wear a badge identifying who they are and their destination. If they do not follow this policy, they can be refused further access to our hospital,” Wolanski says.

Riverside HealthCare in Kankakee, Ill., has obtained business associate agreements with its IT vendors because they have access to the computer systems that store patient information, says Chief Privacy Officer Karen Block. It’s been a real challenge, she says, because the health system uses a lot of vendors. When Riverside presented its HIPAA-compliant business associate agreement for signature, some vendors responded by insisting on using their own business associate agreement — especially because they feared any attempt to include an indemnification clause. “No one wants to sign that,” she says. Usually Riverside persuades the vendor to sign the health system’s version of the business associate contract, but if the vendor digs in its heels, it may relent. “We have our HIPAA legal counsel review it to make sure we don’t sign our lives away,” Block says.

Consistent with her risk analysis, Johnson evaluates vendor access depending on their contact with PHI. For example, if IT vendors “will just be in MIS and have no access to patient information, then we don’t worry about it. If they will have any access to our clinical information system, we make sure they sign a confidentiality agreement.”

As for other kinds of vendors (e.g., building contractors, electrical), generally the main goal is to verify their identity and keep track of them, Foster says. They wear a bright orange vendor badge with a unique number but not a picture. Sometimes their work takes them into locations where there are patients and/or medical records, but “my impression is they are way too busy to pay attention to anything except the work and their safety” or there are employees present (e.g., health information management department) to keep an eye on them. “The contracts we sign with vendors contain confidentiality agreements. We hold them accountable for their own employees,” which means the vendor handles the discipline if one of its employees breaches confidentiality, Foster says.
(3) Medical device sales reps: Depending on the nature of the device, medical device reps are treated differently than drug reps because they may need access to PHI or the patients themselves and may even be present at surgery. But they still must check in with the materials management department and wear badges. For example, orthotics and prosthetics suppliers may need to examine medical records and fit patients directly. There are also vendors who attend surgery because their input is needed by the surgeons who are implanting the device (e.g., pacemaker) or using some new technology (e.g., laser) manufactured by the sales rep’s company.

The sales rep may be a part of the treatment team, so PHI disclosure is proper under the treatment, payment and operations exception, according to guidance from the HHS Office for Civil Rights. Therefore, patient authorization isn’t required — though some hospitals seek it anyway or add a line to the surgery consent form stating that the vendor’s sales rep will be present during surgery.

One privacy officer isn’t totally comfortable putting sales reps under the TPO exception. Block says her hospital “doesn’t necessarily consider device reps members of the treatment team.” She says she doesn’t think it’s

PATIENT PRIVACY COURT CASES

This monthly column is written by Rebecca C. Fayed of the Washington, D.C., office of Epstein, Becker & Green, P.C. It is designed to provide RPP readers with a sampling of the types of patient privacy cases that courts are now hearing. It is not intended to be a comprehensive monthly survey of all patient privacy court actions. Contact Rebecca C. Fayed at (202) 861-1383 or rfayed@ebglaw.com.

◆ An Illinois appellate court held that a patient’s mental health records could be used by the Department of Professional Regulation during a disciplinary proceeding against the patient’s psychiatrist without the patient’s consent. The Illinois Department of Professional Regulation appealed a circuit court decision issuing a preliminary injunction barring them from disclosing at any hearing any information related to the patient without first obtaining a confidentiality release from the patient. The department argued that because of Illinois law, the lower court should not have found that the patient had a right to nondisclosure of mental health information. Rather, the department argued, Illinois law authorized the use of redacted mental health information in a disciplinary proceeding against the patient’s psychiatrist, without the patient’s consent. On appeal, the Appellate Court of Illinois reversed the lower court’s opinion finding that when the Illinois “Confidentiality Act is read as a whole it is clear that the legislature contemplated the use of mental health records for which no consent has been secured in certain judicial proceedings.” Explaining that its statutory interpretation promotes the goals of both the Illinois Confidentiality Act and the Illinois Medical Practice Act, the court stated that “[p]atients remain anonymous, thereby preserving a sufficient level of privacy necessary to encourage other people to seek mental health treatment, which is the goal of the Confidentiality Act…. At the same time, it enables the Department to enforce standards of practice for the psychiatric profession and protect the public from those not qualified to practice medicine, which is the goal of the Medical Practice Act.” (John Doe v. Illinois Department of Professional Regulation)

◆ The Appellate Court of Connecticut held that physician expert could disclose medical records during a deposition without a patient’s authorization. While the plaintiff in this case called Dr. William Gerber as her expert witness in an action against her employer, she filed this action alleging that during a deposition in that case, Dr. Gerber “wrongfully… disclosed confidential and private information about her.” The Appellate Court disagreed with the plaintiff, explaining that “the disclosure of the plaintiff’s medical records took place during the deposition of the plaintiff’s expert, Gerber, and that the disclosure was pursuant to applicable rules of court…. Thus, because the disclosure was made pursuant to applicable court rules, it clearly fell within the exception set forth” under Connecticut law. As the court stated, Connecticut law generally prohibits the unauthorized disclosure of medical records. However, one exception to this rule is that a patient’s consent is not required for a disclosure “pursuant to any statute or regulation of any state agency or the rules of court.” Accordingly, the court found that the expert physician did not wrongfully disclose the information during the deposition. (Alexandru v. West Hartford Obstetrics and Gynecology, P.C.)
feasible for the device rep to attend surgery unless there is patient authorization. There’s always a chance the patient will say “no,” and then she says it’s up to the surgeon to convince the patient to green-light the device rep’s presence.

Lourdes Hospital requires device sales reps to fill out various forms before they’re permitted in surgery. For example, the sales rep signs a confidentiality statement and a form attesting to proper immunizations. “The patient is always given the opportunity to refuse having them there,” Wolanski says.

But it’s essential not to let HIPAA anxiety interfere with patient access to life-enhancing devices, says Becky Buegel, privacy officer at Casa Grande Medical Center in Arizona. “You want patients to get new medical devices. You just have to tighten up [privacy safeguards],” she says. “You either consider them part of the treatment team and document accordingly, or get patient authorization.” As for the abuses with salesmen in the operating room, those were not issues of privacy as much as patient safety.

(4) Drug sales reps: The privacy rule prompted hospitals to crack down on drug sales reps. How much their access is curtailed depends on the way they deliver their sales presentations. “We designed a confidentiality agreement for drug reps and then left it up to unit supervisors whether it’s necessary [to get the rep’s signature],” Johnson says. “If they just drop off samples and leave, then it’s not necessary. But if they will be there for a period of time, then a confidentiality agreement may be necessary.” For example, if the drug rep is giving a 90-minute presentation in the nurse education room while nurses change shifts and give reports, it’s wise to get a confidentiality agreement signed.

The privacy officers generally said that stringent privacy protections for drug reps are more important in their physician clinics, where the reps tend to be in closer proximity to PHI.

(5) Medical and nursing students: They are treated as members of the work force, so they receive full-fledged HIPAA education.

(6) Clergy: This has been one of the biggest adjustments under HIPAA because this class of outsiders — external clergy, not hospital chaplains — was accustomed to virtually unfettered access, and now must be monitored (the same as all other outsiders) to make sure they aren’t exposed to PHI unnecessarily.

For example, at Riverside, the hospital identified the 40 or so clergy members who routinely minister to hospital patients, and assigned each a unique log-in number for the computer located in the pastoral care department. The log-in number gives the clergy member access only to the names of patients who attend his or her church/temple/mosque, etc. How do patients make it to the list? At registration, according to a script that Block has given registration clerks, patients are asked their religion and the name of their congregation, and then are told that “By answering the name of your religion and congregation, your name will appear on a list for visiting clergy.” (The staff chaplain is available for patients who can’t see their own minister, etc., such as if they are visiting from out of town.) Obviously patients who opt out will not appear in the computer.

Clergy members who aren’t at the hospital often enough to merit a log-in number can get a printout of their congregation members from the switchboard, assuming they have proper ID.

Riverside HealthCare also wants to make sure clergy is informed when patients ask for them, but safeguards are necessary when passing along information. For example, the hospital doesn’t want to leave a message for the clergy member that parishioner Clark Kent is in the hospital if the answering machine is located in the clergy member’s family room. So the hospital sent a form to about 120 clergy members asking them who the hospital can leave a message with (e.g., spouse, secretary, on a secure answering machine) when a parishioner requests the clergy member’s presence but the clergy member can’t be located.

Local clergy isn’t thrilled with the new procedures, Block says. Some clergy members have complained that the nearby competing hospital isn’t subjecting clergy to the privacy restraints. But the hospital is sticking to its HIPAA guns.

Deaconess Hospital also treats outside clergy the same as any other visitors, Foster says. When clergy members show up, they generally check in at the religious life office and collect a list of their hospitalized parishioners (if those persons request a clergy visit). If the religious life office is closed, they ask for the patient by name at the front desk. If it is after hours and the patient has an emergency, clergy members identify themselves to security and explain who they are there to visit. Trust is essential; “our religious affairs director said it would be a big task to keep clergy identification badges up to date with photos,” she says.

(7) Employee friends/family: The privacy officers say employees generally know that when spouses, friends or family plan to take them to lunch, they should be met in the lobby or cafeteria and not enter patient areas. There’s an occasional transgression. For example, Johnson entered the transcription area one day to find a strange woman sitting at an employee’s desk, leafing through names on the transcription sheets, “She was waiting for her cousin,” an employee, Johnson says. After that, Johnson told employees to meet friends and family in
more public areas. Since HIPAA took effect, that also became a more official stance at Casa Grande Regional Medical Center. “We now ask them to wait in the cafeteria,” Buegel says. “We want employees to start thinking in terms of whether this person needs to be here or whether they can go to the cafeteria with them and get out of a patient area.”

(8) Law enforcement: This is a complex area and hospitals are grappling with it (RPP 9/03, p. 1). They are trying to live by the HIPAA constraints on PHI disclosures as law enforcement situations arise and articulate them in policies and procedures, but real life is a lot more ambiguous than the scenarios written into the privacy rule. For example, the rights of law enforcement officers to obtain PHI gets muddled in employees’ minds depending on whether the patient is a victim, witness, suspect or fugitive. And where do state laws fit in? For example, Block says that Illinois state law requires providers to turn over drunk-driving blood test results to the police, so they are acting on the assumption that mandate takes precedence over HIPAA.

Hospitals are developing procedures to put some brakes on police access to PHI. “Law enforcement always comes in and wants to talk to patients if there’s an accident and we don’t want them just to open curtains, randomly looking for the right patient,” Johnson says. “They are now required to stop at the nurse’s station and tell us who they want to see and why. Then the clerk checks with the physician if the police officer doesn’t know the patient by name. Then we ask the patient if it is OK for the police to come and talk to them. Sometimes I tell the police they have to wait until the patient comes out of the hospital unless the police officer has a court order.”

Christine Jensen, HIPAA project manager at Denver Health, says state law also governs a lot of her health system’s interaction with law enforcement. For example, state law requires hospitals to report victims of crimes and accidents to the police. The law doesn’t dictate what details to supply, but over time the Denver police department developed a form eliciting basic information. If a police officer later calls the emergency department for information, the ED staffer refers the officer back to the police department, explaining the information has already been supplied. “If they want more detailed information, we have to get patient authorization,” Jensen says.

Buegel is developing policies and procedures for responding to law enforcement requests, and generally they will require police to obtain patient records from the HIM department during regular business hours — except if there’s urgency, Buegel says. For example, if a person under arrest needs treatment, “then we will hand over information to people accompanying the guy to jail.” HIM is coordinating with the ED “because they will be presented with more circumstances, and then we will put together a grid” that dictates PHI disclosures permitted in response to various law enforcement circumstances.

Contact Johnson at tjohnson@obleness.org, Wolanski at awolanski@lourdes.com, Buegel at rbuegel@cgrmc.org, Foster at Candace_foster@deaconess.com, Cornwell at MECornwell@FloydMed.org, Block at Karen_M_Block@rsh.net and Jensen at Christine.Jensen@dhha.org.

HIPAA Myths Can Be Dangerous

When O’Bleness Hospital in Athens, Ohio, was preparing a patient for transfer to another hospital for a pacemaker implant, the nurse asked the recipient hospital for the name of the physician there who would be managing the case. The reason: The O’Bleness nurse wanted instructions for transporting the vulnerable patient. But the recipient hospital refused to divulge the name of the physician without a patient authorization, citing HIPAA privacy rule restrictions.

The recipient hospital was incorrect in its interpretation of HIPAA, and was letting its misguided interpretation of the privacy rule potentially interfere with patient care. “The patient was having a cardiac crisis, and we just wanted to ask the doctor what to do during the transfer,” says Privacy Officer Tammy Johnson. And in terms of the disclosure, the only information at issue was the name of the physician attached to the case. Johnson felt she had no choice and obtained the authorization from the patient, so the nurse could get the doctor’s name and call him for transfer instructions.

But it was a close call in terms of the patient’s well-being. This was another case of HIPAA overkill, with a provider insisting on patient authorization even though the disclosure was treatment related. To prevent future recurrences of superfluous authorization demands from this hospital, Johnson contacted the other hospital’s privacy officer, and told her about the HIPAA myth and the risks it poses to patient care. And “I told my whole hospital this was a big thing. If it involves patient care, don’t be afraid to do it.”

Contact Johnson at tjohnson@obleness.org.
CMS said on Sept. 23 that it would deploy its previously disclosed Medicare fee-for-service contingency plan to accept electronic transactions in legacy formats after the Oct. 16 HIPAA transaction and code sets (TCS) deadline. The decision generally pleased providers, but both they and CMS noted that it does not require private payers to take similar actions. Language CMS released to its Medicare contractors stressed that its contingency plan would last for only a “limited time.” The decision on when to halt it, CMS added, would be made based on its monitoring of progress in HIPAA-compliant claims as well as the number of submitters that are testing compliant formats.

The state of Illinois suspended the licenses of eight physicians who owned a Chicago-area medical group after they failed to adhere to a bankruptcy court agreement to safeguard the records of former patients, according to the Illinois Department of Professional Regulation. The department imposed the suspensions after discovering more than 100,000 records, X-rays, mammograms and ultrasounds in the basement of the former Meyer Medical Physicians’ Group office in Merrionette Park and in a former auto repair garage next door, says department spokesman Tony Sanders. The medical group had promised as part of the bankruptcy agreement to pay $120,000 to safeguard and copy patients’ records. Contact Sanders at (217) 524-8195.

Concerned about the potential for financial institutions to obtain protected health information for marketing purposes, the Health Privacy Project (HPP) in Washington, D.C., is urging HHS to provide public guidance that affirms restrictions on unauthorized disclosure of PHI. When banks process payments through an automated clearinghouse (ACH) network on behalf of health care clients, these transactions contain PHI when they include transmissions of the electronic remittance advice, HPP explains in a letter to HHS. According to HPP, the privacy rule requires that PHI transmitted through the ACH network be encrypted in a way that makes it accessible only to the intended recipient provider or health plan. HPP says it is concerned that PHI that is not encrypted or restricted could be used by financial institutions to obtain information about individuals for marketing purposes, which would clearly violate HIPAA. To view the letter, visit www.healthprivacy.org.

National Imaging Associates, Inc., a radiology benefit management company that serves more than 11 million health plan enrollees, says it is the first radiology organization to receive HIPAA privacy accreditation from URAC. The accreditation program, launched in April, is the nation’s first independent HIPAA privacy accreditation program for covered entities and business associates. In July, URAC awarded the first round of privacy accreditations to 21 organizations (RPP 8/03, p. 12). Contact Nicole Mudloff of National Imaging Associates at (212) 941-8499.

A Wal-Mart pharmacy in Lubbock, Texas, allegedly violated its own privacy practices by accidentally stapling a one-page list of confidential customer information to a prescription, according to The Lubbock-Avalanche Journal. The problem was identified by a Journal reporter, whose prescription was attached to a document that listed 22 customers, their telephone numbers and 31 drugs prescribed to them, says the newspaper. The prescriptions included antipsychotics, antidepressants and birth control pills, according to the report.

The Harris County District Attorney’s Office in Texas seized documents from a Ben Taub Hospital employee’s desk as part of an investigation into a company that allegedly sold stolen hospital records to personal injury lawyers, according to The Houston Chronicle. The hospital employee was not arrested or charged, but was suspended without pay pending the outcome of the investigation, says the Chronicle. The operators of Industrial Safety Consultants are being investigated for allegedly paying hospital employees to steal patient records and selling them to personal injury lawyers in Houston, San Antonio, McAllen and Corpus Christi, says the Chronicle. Based on an undercover surveillance operation commissioned by the government, law enforcement officers speculate that a transaction to exchange stolen records took place, according to Joel Androphy, a lawyer representing the company and its operators. Androphy says it was not his client who made the purchase and that investigators do not have sufficient evidence to prove that any money was exchanged.
If You Don’t Already Subscribe to the Newsletter, Here Are Three Easy Ways to Sign Up:

(1) Call us at **800-521-4323**

(2) Fax the order form on page 2 to **202-331-9542**

(3) Visit **www.AISHealth.com** and click on “Shop at the AIS MarketPlace”

If You Are a Subscriber And Want to Routinely Forward this E-mail Edition to Others in Your Organization:

Call Brenda at **800-521-4323** to discuss AIS’s very reasonable rates for your on-site distribution of each issue. (Please don’t forward these e-mail editions without prior authorization from AIS, since strict copyright restrictions apply.)