Privacy Implications of Disease Management Programs

In an effort to keep costs down and improve the quality of care, many health organizations, health plans and providers have begun adopting and implementing disease and/or care management programs, typically using special disease management software. These software programs greatly ease the sharing of information among a patient’s treatment team — but also expose users to the risk of improperly disclosing patient information. Health plans and providers should keep privacy requirements in mind when licensing and using disease management programs.

What’s Disease Management?

The Disease Management Association of America (DMAA) has defined disease management as “a system of coordinated health care interventions and communications for populations with conditions in which patient self-care efforts are significant.”

Electronic medical records allow a patient’s health history and current condition to be instantly available to an entire medical treatment team, helping in delivery of the most appropriate and best care. This information could affect the treating physician’s suggested care plan, help prevent bad outcomes and ultimately improve patient care.

Typically, managed care organizations and other types of health plans license disease management software for use by institutional and group providers to facilitate the sharing of patient information with a beneficiary’s participating physicians and other members of the treatment team. Using a PC and Web-based software, participating physicians can log on to a managed care organization’s Web site and quickly gain access to a patient’s health information. This allows the participating physicians to fully consider the patient’s general health status, as well as other diagnoses and conditions that could potentially affect patient care and treatment. Consequently, physicians and their patients can take a more active role in care planning and clinical decision-making.

However, any electronically-based disease management program can create significant...
risk to an organization through unauthorized use or disclosure of patient information. Any disease management program must comply with applicable federal and state patient confidentiality, privacy and consent requirements.

**Federal Law**

Generally, under federal law, a covered entity – including a health care provider, health plan and health care clearing house – may not use or disclose protected health information (PHI) except as permitted or required under the privacy regulations (Privacy Rule) of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). A “health care provider” includes any physician who transmits any health information in electronic form in connection with a transaction covered by the Privacy Rule.

PHI includes individually identifiable health information, including demographic information collected from an individual and is created or received by a covered entity or employer and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual and that identifies the individual or that reasonably could be used to identify the individual.

The Privacy Rule prohibits a covered entity from using or disclosing PHI without valid authorization unless otherwise permitted by the rule. Since a participating physician would be permitted access to an individual’s PHI through use of the Web-based disease management program, any disclosure of PHI to the physician would have to comply with HIPAA and the Privacy Rule. However, requiring a provider to obtain the patient’s authorization before using or disclosing PHI for disease management purposes is simply not practical. One of the strengths of these programs is the immediate availability of patient information for the care and treatment of the patient. To comply with HIPAA and the Privacy Rule, the parties would have to rely on an exception to the HIPAA authorization requirement. The treatment and health care operations exceptions may be viable alternatives for uses and disclosures of PHI related to disease management.

Disease management was originally mentioned in the proposed draft of the Privacy Rule under the treatment definition. In the final Privacy Rule, however, disease management was removed. The Department of Health and Human Services (HHS) concluded that no consensus industry definition or core set of activities applied to all or most disease management programs. Without a single disease management definition, HHS thought that including it in the definition of treatment would be confusing and ripe for abuse. Instead, HHS references many disease management activities in its definition of health care operations, and recognizes that virtually all activities carried out as part of legitimate disease management programs should be exempt from the consent and authorization requirements under either the treatment or health care operations exceptions.

**Treatment**

Under the Privacy Rule, treatment includes:

- the provision, coordination and management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party
- consultations between health care providers relating to a patient
- the referral of a patient for health care from one health care provider to another.

In the final Privacy Rule, HHS essentially determined that disease management activities that focused on a specific individual would fall within the treatment definition, even though the term has been removed. In order to utilize the treatment exception for disease management purposes, the purpose of the use or disclosure would have to be focused on a specific individual rather than population-based activities.

**Health Care Operations**

The Privacy Rule defines health care operations to include the following activities (provided such activities are related to covered functions of the covered entity):

- quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines (provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities)
- population-based activities relating to improving health or reducing health care costs
- protocol development
- case management and care coordination
- contacting of health care providers and patients with information about treatment alternatives
- related functions that do not include treatment.

Disease management activities that are population-based would fall within the health care operations exception, including activities related to improving health, coordinating care, reducing health care costs, communicating treatment alternatives and outcomes evaluation. A participating physician would be accessing a patient’s PHI in connection with a disease management program for reasons that would presumably fall within the scope of this exception and not require patient consent or authorization.

HIPAA's security regulations (Security Rule) also require covered entities to implement certain administrative, physical and technical safeguards to protect electronic PHI. Since the information that would be accessed by participating physicians under a Web-based
Specialty Hospitals, continued from page 1

While the plan is under development, Congress has required the Centers for Medicare and Medicaid Services (CMS) to continue its suspension on the enrollment of new specialty hospitals in the Medicare program, which was set to expire on February 15, 2006. The suspension began in June 2005 after the expiration of the federal moratorium on payments to certain specialty hospitals for services rendered to Medicare beneficiaries as a result of a referral from a physician who had an investment interest in the hospital. The suspension will remain in effect until HHS’ final report is submitted to Congress or six months after the DRA’s enactment, whichever is earlier. If HHS fails to complete the report within the required six months, the suspension will be extended for an additional two months.

CMS released its Interim Report to Congress on May 9, 2006, and on May 17, CMS Administrator Mark McClellan testified to the Senate Finance Committee regarding specialty hospitals. In addition to addressing the issues outlined by the DRA, CMS discussed steps that it has taken to respond to recommendations and concerns contained in earlier reports on specialty hospitals generated by HHS and the Medicare Payment Advisory Commission (MedPAC), including:

- proposed payment reforms for inpatient hospital reimbursement
- reform payments to Ambulatory Surgical Centers (ASCs)
- Emergency Medical Treatment and Labor Act (EMTALA) obligations
- hospital definitions.

Proposed Payment Reforms for Inpatient Hospital Reimbursement

CMS has taken steps to revise the hospital Inpatient Prospective Payment System (IPPS) for nine cardiovascular diagnosis-related groups (DRGs) to better recognize severity of illness. The fiscal year 2007 IPPS proposed rule includes two additional payment reforms: the proposed payment changes would not only assign weights to DRGs based on estimated hospital costs rather than on reported charges, but also reconfigure DRGs to reflect not only the patient’s diagnosis but also the severity of the illness.

CMS hopes this change will make it less attractive for a physician investor in a specialty hospital to refer less severely ill, but more profitable patients to the specialty hospital and refer the more severely ill and costly patients to community hospitals.

Reform Payments to Ambulatory Surgical Centers (ASCs)

In its 2005 report to Congress, HHS found that many orthopedic and surgical specialty hospitals were more similar to ASCs than to acute care hospitals (i.e. few inpatient beds and a perceived concentration on outpatient care). However, payment rates differed between specialty hospitals and ASCs for what were essentially similar services. As a result, CMS intends to reform payments to ASCs beginning in 2008 to remove some of the incentives for physician investors to form orthopedic and surgical specialty hospitals to take advantage of higher payments under hospital payment systems.

In its Interim Report, CMS describes how it intends to respond not only to the DRA’s mandates concerning the issues of physician investment, but also to charity care and care to Medicaid beneficiaries, and to enforcement.

Emergency Medical Treatment and Labor Act (EMTALA) Obligations

Many specialty hospitals do not have emergency departments and have not been required to follow the screening and stabilization requirements under EMTALA. The fiscal year 2007 IPPS proposed rule includes a provision requiring all hospitals (including specialty hospitals) with specialized capabilities to accept, within the capacity of the hospital, appropriate transfers of unstable patients covered by EMTALA without regard to whether the hospital has an emergency department.

Definition of Hospital

CMS is scrutinizing whether specialty hospitals meet the definition of a hospital. Under current law, a hospital must be “primarily engaged” in furnishing services to inpatients. CMS does not intend to refine that definition, but will continue to interpret “primarily engaged” on a case-by-case basis and explore other options for addressing the issue.

Response to DRA’s Mandated Strategic and Implementing Plan

In its Interim Report, CMS describes how it intends to respond not only to the DRA’s mandates concerning the issues of physician investment, but also to charity care and care to Medicaid beneficiaries, and to enforcement.

Evidence on Financial Arrangements and Care to Low Income and Charity Care Patients

CMS is sending a survey to approximately 130 specialty hospitals and 270 general acute care hospitals to gather information about physician investment interests in specialty hospitals and the provision of care to low-income and charity care patients. The survey asks for information about:
• the identity of physician investors and returns on the investments
• any limitations on liability the physician investors have available to them
• if the physician investors received a loan from the hospital to purchase the investment interest
• whether the physician investors have a compensation arrangement (management contract) with the hospital or an entity related to the hospital.

The survey also asks the hospitals to list their number of Medicaid discharges, revenue derived from Medicaid patients and the amount of charity care provided.

**Enforcement**

CMS wants public comment on how it can best support enforcement actions against inappropriate investment in specialty hospitals. CMS acknowledged that many questions related to whether a physician’s investment is “proportional” or “bona fide” are appropriately addressed under the federal anti-kickback statute. Accordingly, CMS intends to consult with the HHS Office of Inspector General (OIG) for guidance on matters relating to anti-kickback statute enforcement.

Additionally, if CMS uncovers evidence of possible violations of the anti-kickback statute or evidence of potential violations of the physician self-referral law (the Stark Law), it will refer those cases to the OIG for possible enforcement actions.

McClellan explained CMS’ view of the “whole hospital” exception to the Stark Law to the Senate Finance Committee. “CMS recognizes that there are different opinions regarding physician-owned specialty hospitals. Physician-owned specialty hospitals are legal under the existing whole hospital exception to the physician self-referral law and elimination of the exception cannot be done administratively,” he said.

**Conclusion**

CMS appears likely to rely upon the data it receives from the survey process to make any recommendations concerning physician investments in specialty hospitals. As CMS has stated that it will refer matters to the OIG if it uncovers evidence of possible violations of the federal anti-kickback statute or Stark, hospitals receiving such surveys may wish to consult with counsel before completing the CMS survey. Additionally, CMS’ statement that the whole hospital exception cannot be eliminated administratively indicates it’s deferring to Congress on the decision to enact another moratorium regarding specialty hospitals.

**Author:**

Gregory M. Fliszar
215.981.4349
fliszarg@pepperlaw.com

---

**Medicaid Benefits Require Proof of Citizenship Starting July 1**

Staring July 1, 2006, individuals signing up to receive Medicaid benefits or to renew benefits will be required under federal law to show proof of U.S. citizenship — such as a passport or certificate of naturalization, or a birth certificate and some form of identification. The requirement is a provision of the Deficit Reduction Act of 2005. The provision’s intent is to prevent undocumented immigrants from claiming to be citizens to receive benefits only provided to legal residents. Under federal law, undocumented immigrants can receive only emergency care through Medicaid.

In many cases a single document, such as a passport or certificate of naturalization, will satisfy the requirement. A U.S. birth certificate will establish citizenship, but individuals also will need evidence of identity, such as a driver’s license. Other types of documentation also may be used, such as school records for children.

Current Medicaid beneficiaries will not lose benefits while they are making a good-faith effort to provide documentation to the state.

The U.S. Department of Health and Human Services issued guidelines for compliance with the requirements on June 9, 2006, to be followed by regulations published in the Federal Register. The guidelines are online at www.cms.hhs.gov/MedicaidEligibility/05_ProofofCitizenship.asp.
Pennsylvania Senate Bill 712, also known as the Breach of Personal Information Notification Act, went into effect on June 20, 2006. The Act applies to entities doing business in Pennsylvania that maintain, store or manage computerized databases that include personal information of multiple individuals – such as hospitals and other providers, health plans and a wide variety of other health care entities.

Such entities must promptly notify Pennsylvania residents if their unencrypted and unredacted information was or is reasonably believed to have been compromised by a breach of security that would harm a Pennsylvania resident. If residents’ personal information was stolen while encrypted, notice must still be provided if the security breach allowed an unauthorized person to access the data in an unencrypted form. A vendor that manages such data on behalf of a customer is only responsible for notifying that one customer.

What is Personal Information?

The Act defines personal information as an individual’s name linked with her or his Social Security number, driver’s license or state identification card number, or information that would permit access to that individual’s financial account. Personal information does not include information made publicly available from government records.

Required Notice

Notice can be given by mail, e-mail or over the telephone, with some caveats meant to ensure receipt of the notice. “Substitute notice” may be used if the entity needs to notify more than 175,000 people, the cost of notification would exceed $100,000, or the entity lacks sufficient contact information. Substitute notice consists of posting notice on the entity’s Web site, notifying major statewide media, and e-mailing notice upon acquisition of valid e-mail addresses. Any entity notifying more than 1,000 people of a single breach also must promptly notify consumer reporting agencies of the timing, distribution and number of notices.

Exceptions

The Act carves out several exceptions. If a law enforcement agency advises an entity in writing that notification under this Act will impede an investigation, the entity must give notice only after the agency has determined that the notice will not compromise the investigation or security. Financial institutions meet the requirements of the Act by complying with the notification rules under the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice. Similarly, complying with notification rules promulgated by an entity’s primary or functional federal regulator will meet the entity’s duties under the Act. If an entity complies with its own preexisting notification procedures, and those procedures are consistent with the notification requirements of the Act, the entity has met its duty under the Act.

Remedies

Violations of the Act also violate the Unfair Trade Practices and Consumer Protection Law (UTPCPL). No private cause of action is allowed under the Act or the UTPCPL for a violation of the Act; only the Office of Attorney General can bring such an action.

Tips

The best advice is to be proactive to avoid the breach of security. Minimize the use of personal information in your operations by eliminating the use of social security numbers or redact them; at a minimum, always encrypt information before transmission. Also, you should properly dispose of storage media. Create and document best practice standards for privacy and security and train all employees on them. Should a breach occur, you should understand what the regulations require and set into motion an action plan to assess whether and how to report. Be sure to update your compliance plan as this area of the law is rapidly changing.

Author:

Sharon R. Klein
949.567.3506
215.981.4172
kleins@pepperlaw.com
Much has been written in recent years about the rising costs of imaging procedures. Radiology and imaging is estimated to be a $75 billion - $100 billion industry, and hundreds of millions of medical imaging procedures are performed each year. The performance of imaging procedures has become the fastest-growing physician service. Health plans, as the payors for many of these services, have noted this rapid increase; some plans have estimated plan imaging cost increases of between 20 percent and 30 percent annually.

Several factors are often cited as causes for this increase: more demand by consumers for non-invasive imaging tests; the practice of defensive medicine; diagnostic imaging tests ordered by non-radiologists; and ownership in imaging centers by non-radiologist physicians. Various approaches are being examined and implemented to address concerns of over-use, including two provisions in the Deficit Reduction Act of 2005 (DRA) that directly affect the provision of imaging procedures.

The DRA adopted a reimbursement reduction for the second and subsequent imaging procedure on contiguous body parts in the same family in the same session. Effective in January 2007, this reduction will be phased in over two years with a 25 percent reduction in 2006 and a 50 percent reduction in 2007. This reduction applies to 11 families of imaging procedures.

The DRA also imposes new payment caps on the technical component of imaging services performed in physician offices or diagnostic testing facilities. Effective January 1, 2007, payment for the technical component of imaging services performed in physician offices or diagnostic testing facilities cannot exceed payment rates for the same services under the Medicare hospital outpatient prospective payment system fee schedule.

Effective January 1, 2007, payment for the technical component of imaging services performed in physician offices or diagnostic testing facilities cannot exceed payment rates for the same services under the Medicare hospital outpatient prospective payment system fee schedule.

In Pennsylvania, Pittsburgh-based Highmark Blue Shield (Highmark) has been at the forefront in efforts to manage imaging costs. Highmark recently implemented its radiology management program, which includes an imaging provider privileging process as well as a pre-authorization program. Also in Pennsylvania, Independence Blue Cross (IBC) reinstated a pre-authorization program for outpatient imaging procedures effective October 10, 2005.

Highmark Guidelines

Highmark has implemented its Professional Provider Privileging Guidelines and is working with National Imaging Associates, Inc. (NIA), an imaging management firm. Required privileging for imaging procedures became effective January 1, 2006 for magnetic resonance (MR), CT and PET providers; and September 1, 2005, for all other imaging services. Highmark will only reimburse participating members if they are privileged for the provided imaging services. These privileging requirements apply to imaging provider sites in the 21 counties of central Pennsylvania. Additional guidelines and information, along with a privileged provider directory, are available at the Provider Resource Center on the Highmark Web site (www.highmarkblueshield.com).

Highmark’s guidelines include general requirements for all privileged imaging providers as well as guidelines for specific modalities. According to the purpose section of the guidelines, they are “intended to promote reasonable and consistent quality and safety standards for the provision of imaging services.”

General Guidelines

All Highmark credentialed imaging providers must:

• provide a written report within 10 business days (30 days for mammography reports) from date of service to the ordering provider
• have a documented quality control program inclusive of imaging equipment and film processors, and a documented radiation safety program and as low as reasonably achievable (ALARA) Program
• have a current (within 3 years) letter of state inspection, calibration report or physicist’s report if utilizing equipment producing ionizing radiation
• be credentialed by Highmark and Keystone Health Plan West.

The Highmark Medical Policy will apply to the delivery of services detailed in the guidelines. In addition, the Highmark Professional Provider Privileging Guidelines
include guidelines for each of the following imaging providers: plain films, bone densitometry, nuclear cardiology, echocardiography/stress echocardiography, peripheral vascular ultrasound, obstetrical/gynecological ultrasound, urological imaging, mammography, ultrasound, PET, fluoroscopy, CT and MR, women’s health and mobile services.

**Guidelines Specific to PET**

To meet Highmark’s guidelines, PET must be performed by a hospital, partially owned by a hospital as part of a joint venture or other partnership, owned and operated by an oncology practice clinically affiliated with hospital or community based cancer treatment programs, or be in an area with an access need.

Additionally, PET facilities must employ technologists certified in nuclear medicine by one of the listed certifying organizations or licensed by the state in nuclear medicine technology, and only high-performance, full-ring PET systems will be considered.

PET scan providers also must achieve accreditation by ICANL (Intersocietal Commission for the Accreditation of Nuclear Laboratories) or the ACR within two years of provisional acceptance in the privileging program. The facility must submit evidence of application for accreditation to NIA within three months of receipt of the letter indicating provisional acceptance.

**Guidelines Specific to CT and MR**

Practice sites offering CT and MR must:

- provide at least five out of a list of nine modalities
- offer diagnostic imaging services for a minimum of 40 hours per week
- be staffed on-site by a credentialed radiologist who has a current Advanced Cardiac Life Support (ACLS) or Advanced Radiology Life Support (ARLS) certification during the 40 minimum hours of operation and whenever contrast enhanced procedures or diagnostic mammography are performed (including during non-standard hours)
- employ an appropriately licensed or certified technologist
- provide MRA capability, if offering MRI services
- achieve accreditation by the ACR for MRI within one year of provisional acceptance in the privileging program (if offering MRI services). The practice must submit evidence of application for accreditation within three months of receipt of the letter indicating provisional acceptance.

The guidelines do not preclude credentialed cardiologists from performing echocardiography/stress, echocardiography, peripheral vascular ultrasound, arterial angiography, and nuclear medicine/nuclear cardiology diagnostic services at a CT/MR practice site.

In a recent addition to the guidelines, Highmark added an exception to the on-site radiologist staffing requirement when the practice uses teleradiology and satisfies a series of additional requirements, including:

- a Highmark credentialed physician must be: on site during normal business hours (at least 40 per week); a member of the imaging provider group; available for patient, referring physician and teleradiologist consultation (minimum of 40 hours per week); current on ACLS or ARLS certification; and on site when contrast enhanced procedures or diagnostic mammography are performed (including during non-standard hours)
- images must be transmitted in real-time, or near real-time mode, so that the interpreting radiologist can collaborate with the rendering physician and the technicians performing the studies
- clinically significant data must not be lost in the transmission process.

If imaging providers wish to use teleradiology they must submit a teleradiology privileging application in addition to the general privileging application.

**Hospital Guidelines**

Highmark also has adopted radiology privileging guidelines for hospitals. While they are similar to the provider guidelines, there are some key distinctions. All hospital imaging centers located within a 35-mile radius of the hospital’s main campus are treated as part of the hospital. Each hospital-based imaging location is not required to separately satisfy the privileging requirements. Additionally, the hospital guidelines do not require each hospital-based imaging location providing CT or MRI services to provide at least five of the nine imaging modalities. When these guidelines were updated in March 2006, Highmark added the teleradiology exception to the guidelines specific to CT and MRI.

**Prior Authorization**

In addition to requiring privileges, Highmark requires all physicians and clinical practitioners to obtain authorization when ordering select procedures. The Highmark prior authorization program became effective April 1, 2006. In March 2005, to ease the transition, Highmark implemented the prior notification phase for physicians routinely ordering procedures. During this phase, providers were to notify Highmark before ordering select CT, MRI and MRA scans and all PET scans; however, reimbursement was not affected, and authorization numbers were not issued.

Currently, Highmark requires all physicians and clinical practitioners to obtain authorization when ordering select outpatient, non-emergency advanced imaging procedures,
including select CT scans, select MRI and MRA scans and all PET scans covered by Highmark. Authorization numbers will be provided and will be required for reimbursement. Highmark has implemented an online authorization request system called NaviNet. Highmark and NIA have developed guidelines for clinical use of diagnostic imaging examinations to assist providers. Highmark has also implemented a retrospective review and appeal process. The prior authorization reference guide posted on Highmark’s Web site offers additional information for providers.

Other insurers have implemented pre-authorization programs for imaging services, including IBC, which reinstated pre-authorization for outpatient imaging effective October 10, 2005. The IBC program applies to diagnostic imaging in CT, MRI, nuclear cardiology and PET. It does not apply to diagnostic imaging performed in connection with inpatient hospitalizations or emergency room care. The IBC program applies to managed care providers in Pennsylvania, New Jersey and Delaware.

Conclusion

Privileging and pre-authorization, along with caps on reimbursement, are some of the approaches being taken to curtail over-utilization of diagnostic imaging procedures. Insurers say that privileging and pre-authorization are designed to promote quality and patient safety while avoiding unnecessary and/or duplicative expensive services. Whether this growing trend will become standard practice remains to be seen.

disease management program would constitute electronic PHI, the parties involved would also have to ensure that the program, as well as the parties’ using the program, complies with the requirements under the Security Rule.

State Law Requirements

States often have more stringent patient confidentiality, privacy and consent laws that could affect any disease management program. For example, some states may require a form of consent of the patient before any use or disclosure of the patient’s health information, even when the information is being used by or disclosed to the patient’s treating physician or medical team. Organizations adopting and implementing disease management programs need to comply with these requirements before providing physicians access to patient information. Because consent requirements vary from state to state, no “one-size fits all” consent document can be used. Many jurisdictions also have more stringent requirements for using or disclosing certain types or classes of highly sensitive health information.

Pennsylvania, for example, provides much greater protections over the use and disclosure of mental health, drug and alcohol, and HIV information. With respect to drug and alcohol information, patient records prepared or obtained under the Drug and Alcohol Abuse Control Act may be disclosed only with patient consent and only to a limited number of recipients, such as medical personnel. If a disease management program permits access to a patient’s entire medical record, this type of sensitive information may be at risk of being disclosed without the proper patient authorization. Physicians and other providers using or licensing any disease management program should ensure that the program is designed to permit access only to that information for which consent has or can be obtained in advance, or for which no consent is required.

Disease management programs can be an invaluable tool for assisting physicians and other providers with patient care management and treatment. Their use, however, is not without risk. Organizations that license such programs and physicians who utilize them need to be fully aware of the challenges presented and ensure that any use or disclosure of patient information complies with both federal and state law.

Author:

John W. Jones, Jr.
215.981.4706
jonesj@pepperlaw.com

Privacy Implications, continued from page 2

Author:

Rebekah A. Z. Monson
215.981.4031
monsonr@pepperlaw.com