Ownership of Health Information in the Information Age

by Adele A. Waller, MA, JD, and Oscar L. Alcantara, JD

The question "Who owns health information?" has no simple answer. The authors examine problems related to traditional ownership in the age of aggregated information and offer suggestions as to how some of these issues can be clarified and resolved. A sidebar examines the traditional view of provider and patient ownership and how these structures are changing.

The question of who owns health information is arising more and more frequently in discussions between healthcare providers and vendors of healthcare information systems and between providers and companies supplying clinical data analysis or clinical outcomes-related products and services. Such vendors and companies may seek to obtain ownership rights in the data of their provider customers, whether such data can be linked to individual patients or not. They often seek such rights so that they can build comparative databases and other health data products, which can have substantial commercial value. Similarly, healthcare clearinghouses, which process health data into standardized formats and communicate the data electronically to payers and others, may seek to obtain rights in the data that they process.

The question of data ownership is also being discussed by healthcare providers who are integrating health information systems and patient data so that they can function as integrated delivery systems, delivering seamless healthcare across the continuum of care. It is increasingly common for providers in an integrated delivery system to have access to patient information maintained by every other provider in the system, perhaps through a shared clinical data repository. Master patient indices, which identify each patient uniquely, facilitate linking patient data across numerous care settings. Confidential patient information is now more widely disseminated through databases of patient information which permit participating providers to access all clinical data recorded about a patient at any point of care within an integrated delivery system.

In the information age, it is increasingly difficult to determine who controls or should control health information and who should control the value of the information that is shared or integrated. The issue of information ownership in the healthcare industry is even more complex because of special privacy and security laws and regulations that apply to the often sensitive information involved, based on traditional concerns for patient confidentiality. Another trend in health information law--that of stronger protection of patients' rights to access their medical information--further complicates the analysis of who owns health information.

When the question "Who owns health information?" is asked, the real meaning of the question may be any of the following:

1. Who may access data?
2. Who may mine or manipulate data?
3. Who may use data and for what purpose?
4. Who may sell data?
5. Who may disclose or publish data?
6. Who must pay to access, use, publish, or sell data?
7. Who is required to disclose data in response to subpoenas or court orders?

In many respects, the traditional concept of "ownership" is not a useful construct when applied to patient-identified information. If what is meant by ownership of patient information is the right to exercise complete sovereignty over information, it cannot be said that any one person or entity "owns" the information. A discussion of the various classes of persons' rights and responsibilities with respect to patient information is a more useful way to tease out what is often the real question being asked when the question, "Who owns health information?" arises--namely, "Who can do what to which data under what circumstances?"

This article will examine problems with traditional ownership in the age of aggregated information and offer suggestions as to how some of these issues can be clarified and resolved. A sidebar (see below) examines the traditional view of provider and patient ownership and how these structures are changing.

The Traditional Rule

The Provider as "Owner"

The classic statement of the rule concerning ownership of medical records is that the provider owns the medical records maintained by the provider, subject to the patient's rights in the information contained in the record.[1] This statement of the rule was developed in the era of paper records, when rights in the physical medical record and rights in the information contained in the record were more easily separated than they are in the information age. Generally speaking, the traditional notion that providers own their medical records gives them the right to possess the records as well as the right to access and use the records for patient care and other legitimate purposes. Even under the traditional rule, however, no one person or entity can be truly said to "own" patient-identifiable information (in which the identity of the patient may be derived or inferred from data), if what is meant by ownership is the ability to exercise complete sovereignty over the information--to disclose, sell, destroy, alter, or determine who shall have access to it at will.

Providers have traditionally been viewed as owners of medical records. Statutes and regulations stating that the providers own such records, however, all suggest that the type of ownership rights possessed by providers fall far short of permitting the "owners" to exercise sovereign rights over the owned records. In fact, current law grants healthcare providers limited rights and imposes on them responsibilities with respect to patient information that they maintain.

Patients' "Ownership" Rights

While some state statutes and regulations state that providers own medical records, many states also grant patients rights in their medical information. These rights may be viewed as "ownership" rights. Most of these statutes, however, do not expressly state that the patient "owns" the information, although there are exceptions.[2] Rather, such statutes confer various rights to patients with respect to their medical information. Such statutes may also provide penalties for violations of patients' rights in their information.

Patient rights in medical information generally fall into three categories: the right to access or obtain copies of the information, the right to request correction of such information, and the right to confidentiality.

The rights of a provider who "owns" a patient's physical medical record are subject both to the provider's duties to patients and to patients' privacy rights and rights to access and "correct" the information contained in their records. This means that "ownership" of patient-identifiable data in the traditional sense does not reside with any one person or entity. Individuals' rights in their medical information will exist independent of any contracts. For this reason, providers and others cannot assume that "ownership" of patient records permits them to share or sell patient-identified medical information as they see fit. It is wise to avoid contract provisions that purport to transfer ownership of patient-identified data in a manner that violates patients' rights or providers' obligations with respect to the information.

Ownership of Masked and Aggregated Data

Ownership of Non-identifiable Patient Information

When medical record information is cleansed of identifiers, the law generally places few restrictions on the use of this information and generally terminates patient rights. Most statutes and regulations protecting the confidentiality of personal health information apply only if the information is linked to, or can be linked to, the identity of the patient.

If the identity of individuals cannot be determined from data, whether by itself or combined or crossmatched with other data or databases, the general rule is that anyone who has acquired a legitimate right in the data can own it. This rule is implied by statutory definitions of the medical information protected by confidentiality statutes. For example, the California Confidentiality of Medical Information Act defines protected "medical information" as "any individually identifiable information in possession of or derived from a provider of health care regarding an individual's medical history, mental or physical condition, or treatment."[3]

From this definition, it is apparent that this act does not protect such information if it is not individually identifiable. Likewise, the California statute providing civil and criminal penalties for wrongful disclosure of HIV test results provides those penalties for a variety of unauthorized disclosures of HIV test results to a third party "in a manner that identifies or provides identifying characteristics of the person to whom the test results apply."[4] From this statute, it can be inferred that an individual's rights with respect to disclosure of the individual's HIV test results terminate when such results no longer identify or provide identifying characteristics of individual.

In evaluating whether the identity of a patient can be determined from data, two concepts are useful—namely, those of patient-identified and patient-identifiable data. Data is patient-identified if the subject of the information is disclosed by the data. Patient-identifiable data need not explicitly identify the patient; rather, if the identity of the patient can be derived or inferred from the data, with or without the assistance of computers and artificial intelligence, data is patient-identifiable.

The concept of patient-identifiable data is becoming increasingly important in determining whether the data has been sufficiently anonymized to terminate a patient's rights and make it freely transferable. The Health Insurance Portability and Accountability Act's (HIPAA) confidentiality provisions protect patient-identifiable health information, which is defined as:

Any information, including demographic information collected from an individual, that:

1. *Is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse; and*
2. *Relates to the past, present, or future physical or mental health or condition of an individual, the provision of healthcare to an individual, or the past, present or future payment for the provision of healthcare to an individual, and:*

- *Identifies the individual; or*
- *With respect to which there is a reasonable basis to believe that the information can be used to identify the individual*

This raises the question of whether data from records in which the identity of individuals has been masked, but which still exists in discrete individual records, may be freely sold or transferred. Masking the identity of individuals in the information age may require more than merely stripping the data of common interface such as name, address, and social security number. Because of computers and inference engines and the existence of nonmedical databases that link individual identities to demographic and other information concerning an individual, it is possible to associate information with the identity of an individual, even when the information has been stripped of obvious identifying data elements. Thus, masking the most obvious identifiers in individual records may not always be sufficient to make the information truly anonymous.

If a patient's address, zip code, or telephone number are left unmasked, such crossmatching becomes much easier than if these elements are masked. If data are to be used for public health or outcomes research, it may be necessary to include the zip code of a patient's residence in the unmasked data to support the purposes of the research.

Given the increasing legal importance of the notion of patient-identifiable data, it may be unwise for healthcare providers to sell or transfer ownership of data that has been masked, cleansed, or blinded at the individual record level but has not been rendered truly anonymous by aggregating individual records in cells of adequate size (e.g., records concerning five individuals in each cell) to make inference of individual identities using information age techniques infeasible. If there are compelling reasons to permit a vendor or other party to use masked data, it may be preferable to grant a license to use the data, subject to an obligation of the licensee not to manipulate or permit manipulation of data to determine the identity of any subject of a record included in the licensed data, rather than transferring ownership of the data outright. This preserves some control by the licenser over what the licensee does with the licensed data.

In instances where data has been masked or aggregated so that the identities of individuals cannot be determined from the data, contractual provisions, possession of data, or copyright laws will generally determine rights in the data. This means that, if medical data has been sufficiently anonymized or aggregated so that determining the identity of individuals is unlikely or impossible, the individual's rights in the data will generally terminate, and a person with a legitimate claim to such data can own, sell, and license it. This makes copyright protection and contractual provisions spelling out ownership and rights in anonymized and aggregated data very important.

Problems with Traditional Ownership in the Age of Aggregated Information

Multiprovider Systems Integration Arrangements

Ten years ago, most clinical information systems maintained the records of a single institutional healthcare provider, such as a hospital. At that time, electronic record keeping still reflected traditional provider-based medical record keeping, with each provider maintaining a separate medical record on the patient. Since that time, hospitals, physicians, other healthcare providers and, in many cases, health plans have come together in integrated delivery systems to provide seamless care to patients across the continuum of care and to manage the health of populations. To effect this integration, healthcare organizations are integrating their information systems and acquiring and developing shared information systems (e.g., clinical data repositories and master patient indexes). The integration of patient information and information systems raises complex questions as to the relative rights in the data of the provider originating patient data, the entity operating the shared or integrated information system, and the integrated delivery system or network entity (if there is one).

In fashioning contracts to support multiprovider systems integration initiatives, it is important that participants avoid the pitfalls that ill-advised contractual provisions concerning information ownership can create. It is not uncommon for a primary organization within an integrated delivery system to insist that the contract provide that it is the owner of the information maintained in the shared or integrated system(s). Such a provision should be avoided. First, the provision may be unenforceable, because it conflicts with the originating provider's responsibilities with respect to the data and will often also conflict with patients' rights in the data. In addition, a provision purporting to transfer ownership of shared or integrated clinical data may provide a platform for malpractice plaintiffs' lawyers and others to argue that the information is or should be discoverable (or that it is discoverable if the data are not patient-identified) and that the purported "owner" of the data can be forced to conduct "computer peer review" to test whether the defendant provider is guilty of negligent credentialing or has pervasive quality problems of a type present in the alleged malpractice at issue in the case. For this reason, it is advisable for the contract among participants in the systems integration initiative to state that, as among the parties, each party shall be deemed to own the data it originates. In some instances, it may be advisable to tag certain data, such as laboratory results, to multiple "owners" to mirror what would be included in the medical records maintained by participating providers in a paper record environment.

Contracts among providers participating in systems integration arrangements should also specify the procedures to be followed when one participant receives a subpoena, court order, or other demand for a compulsory disclosure of data originating with another. For example, consider a provision that a party receiving a demand for compulsory disclosure of data originating elsewhere must promptly notify the party originating the data of the demand and must cooperate with the originating provider in contesting disclosure. Such a provision will minimize inadvertent violations of patient confidentiality and reduce the risk of one party's proprietary information being disclosed without the originator's receiving notice and having the opportunity to contest disclosure.

To address the problems that could arise when one provider participating in a shared clinical information system relies on data originating with another provider to provide care to a patient who suffers a therapeutic misadventure, it is also wise for a contract among participating providers to grant the entity operating the shared or integrated system a perpetual license to maintain the data in the system. This license should be subject to a continuing obligation to comply with security and confidentiality obligations. The licensee also should agree to make available to any participating provider information necessary to defend or respond to any claim or suit involving allegations of malpractice or to respond to any governmental or other investigation. Such provisions should survive termination of the contract, as well as termination or withdrawal of any participating provider.

Ownership provisions in contracts among providers integrating or sharing information systems should further address rights to the data in the event that one provider within the network withdraws or is otherwise terminated. At a minimum, the systems integration or network agreement should provide that, upon termination or withdrawal, a participating provider is entitled to copy the data originated by such provider and documentation of the chain of copying. This provision should be drafted so as not to compromise the agreement of the parties with respect to rights in aggregated/ anonymized data.

Contracts among participating providers should also set forth the rights of any provider to access and mine the data originated by other providers.[5] For a variety of reasons, providers participating in a shared or integrated system may wish to have the right to mine the data of one or more of the other participants for purposes such as physician profiling or obtaining competitive intelligence. The contract entered into by the parties should clearly state whether any mining of the data of another party is

permitted and, if so, under what circumstances, for what purposes, and subject to what restrictions on dissemination of the results.

Because the data of providers sharing or integrating information systems will often have value when viewed in the aggregate, the contract among participating providers should also provide a mechanism whereby the parties can collectively exploit the value of their data and state a formula or mechanism for allocating such value among the participants. So long as such data are not patient-identifiable, participating providers are free to enter into sales or licensing arrangements to realize the value of their aggregate information.

Information Systems Vendors and Clearinghouses

All agreements between healthcare providers' external computer service or data organizations should address whether the outside entity will be permitted to use patient information or create comparative databases or other proprietary information products for distribution to third parties. Permitting a vendor to include patient-identifiable data of a provider or an integrated delivery system in a database or other information product will result in the provider or integrated system losing an important degree of control over patient data. The vendor's manipulation of such data for purposes of conducting statistical analysis or for constructing comparative databases will be substantially different from the way the vendor processes data for purposes of performing its obligations under its contract with the provider or the integrated delivery system. Permitting vendors to process patient data in this manner may expose participating providers to potentially serious liability for the vendor's improper disclosure of patient-identifiable information. This increased liability exposure may be sufficient to prevent providers and integrated delivery systems from agreeing to permit vendors to use patient-identifiable data in this manner. Such use should be permitted by contract only if the contract includes detailed vendor confidentiality obligations also applicable:

- to the vendor's agents, employees, and subcontractors and protecting patient-identifiable data; and
- to information identified as proprietary information of the provider, system, or network and to practitioner- or provider-identified data.

The contract should also include detailed procedures and protocols the vendor must follow in processing all such data. The vendor should be required to provide indemnification for all losses resulting from breach of these obligations, including the provider's or integrated delivery system's attorneys' fees and costs.

System vendors may seek to gain access to the masked patient data of their customers and may try to negotiate contract provisions making the vendor the "owner" of the masked data transmitted to them by their customers. It is inadvisable to grant vendors ownership rights in data composed of masked individual patient records. If a delivery system or provider wants to permit the vendor to utilize such data in creating data products, it should consider granting the vendor a license to use the data, subject to the vendor's continuing obligations not to manipulate or permit manipulation of the data in any manner that would reveal the identity of any patient and not to disclose to any third party the licensed data (unless it has been further aggregated to make it truly anonymous).

If a third party (such as a clearinghouse) will perform the data masking, it is important that a contract be executed prior to any transfer of patient-identifiable data to the entity charged with performing the masking. The contract should require the entity to preserve the confidentiality of all patient-identifiable data in perpetuity and to use such data only to perform its contractual obligations. It should not contain any provisions limiting the entity's liability for breaches and should require the entity to indemnify providers from which the entity receives data for any breaches of confidentiality. The contract should also provide for return or destruction of all patient-identifiable data in the possession of the third party in any form at the conclusion of the contract.

Ownership of Health Databases under Copyright Law

The aggregation of health data into databases or other compilations of data may result in the creation of a database protectable under copyright law, and, therefore, the creation of yet another set of rights and responsibilities with respect to health information. The Copyright Act of 1976 affords copyright protection to all "original works of authorship fixed in any tangible medium of expression."[6] Such works can include compilations and databases of health information.[7]

The scope of copyright protection in databases, however, extends only to the "expression" of ideas or facts and does not afford authors exclusive rights in the facts, raw data, or ideas that underlie the protectable expression. In order for copyright protection to attach to a database, therefore, the underlying facts and data must be selected and arranged in an original format.[8]

Once an original selection or arrangement of data has been created, however, the author or "owner" of the database obtains several valuable and exclusive ownership rights. These rights include the right to control the creation of copies of the database, the distribution of such copies, and the alteration or modification of the database into a new "derivative" work.[9]

Given the value of these ownership rights, it is of utmost importance to determine by agreement who will own the copyrights attaching to a health information database. In the absence of an effective written agreement, the participants and providers integrating their data run the risk that each provider will be considered a joint author.[10] There is a very low threshold for the degree of originality required for work product to be protected by copyright. Each provider of information to a networked database may conceivably contribute copyrightable expression merely in his or her selection of what words to use in text fields.[11] If all of the provider-authors who contribute information and language to a repository intend that their contributions be merged with those of other providers, the resulting database may well be considered a joint work.[12] In that event, each provider of protectable expression would be entitled to the status of "co-owner" and entitled to exercise any of the several ownership rights set forth in the Copyright Act. Each provider would, therefore, enjoy the individual right to exploit the copyright in the entire work. This potentially unworkable result underscores the importance of addressing copyright ownership rights by agreement among all the providers integrating their data.

Copyrights may be freely assigned, but such assignments must be in writing and should be recorded with the Copyright Office in order for the assignment to be effective against third-party claimants.[13] Integrated delivery systems should consider including "work-made-for-hire" language in their systems and data integration agreements. If providers participating in a systems or data integration project contribute information to a compilation of health data pursuant to a written "work-made-for-hire" agreement, then the entity specified by contract as "hiring" the work will be deemed the "author" of the entire compilation and, therefore, the owner of the copyrights.[14] Even if many providers contribute copyrightable material, the party specified by contract as commissioning such contributions, not the individual contributors, who will be considered the "author" of the work.

It is also important that, when retaining independent vendors and consultants to develop software, data products, or electronic expressions of medical logic, healthcare providers and integrated delivery systems enter into appropriate agreements that address data rights and copyright issues appropriately. For example, if an integrated delivery system retains an independent contractor consultant to develop a clinical outcomes database, using the clinical data of participating hospitals and other providers, the consultant will be deemed to be the author of the copyrightable work and the owner of the copyright, unless the agreement states that the database is a "work-for-hire" or that the copyrights are assigned to the integrated delivery system. In such a case, the owner of the copyright will have sole control over the right to create copies of the copyrighted work and the right to create derivative works that enhance the copyrighted work (for example, clinical pathways derived from outcomes information produced from the database). Even if the integrated delivery system decides that the independent consultant should own the copyright, the contract should specifically restrict the consultant's use and disclosure of any patient-identifiable data used in creating the database.

It is also important to appropriately address ownership of copyrights in works created by employees. The original copyrightable works of an employee acting within the scope of his or her employment are by statute considered works-made-for-hire and belong to the employer.[15] In such a case, the employer is deemed the author of the work (and the owner of the copyright) rather than the individual employee. Whether an employee is working within the scope of his or her employ when creating copyrightable expression, however, can be subject to dispute. Healthcare providers may rely heavily upon the work product of technologically proficient employees in developing databases and other data products. It is wise for such providers to have written agreements with employees developing such copyrightable works that make the provider's ownership of the copyright clear so that a valuable copyright does not vest in the employee, based on the employee's successful argument that development of the copyrightable work was outside the scope of employment.

Whether the transfer of copyright ownership in a health-information database is effected by work-made-for-hire language or by a more straightforward assignment, it is essential that such ownership issues be addressed in a written agreement setting forth which party or parties are to enjoy the exclusive rights granted under the Copyright Act.

Conclusion

A clear understanding of ownership rights in various forms of health data can assist healthcare providers and integrated delivery systems in avoiding contracts that may give them unnecessary legal exposure and in making sure that their valuable rights in health data are explicitly and appropriately protected.

Notes

1. See, e.g., "Position Statement, Confidentiality of Patient Health Information." Journal of the American Medical Record Association 56, no. 12 (1985); W.H. Roach, Jr., and Aspen Health Law Center, Medical Records and the Law. Gaithersburg, MD: Aspen Publishing, 1994.
2. See, e.g., New Hampshire's Patients' Bill of Rights, which provides that "medical information contained in the medical records at any facility licensed under this chapter shall be deemed to be the property of the patient." NH Rev. Stat. Ann. 151:21 (1997).
3. Cal. Civ. Code § 56.05(b) (1996).
4. Cal. Health & Safety Code § 120980 (1996).
5. The law generally does not afford healthcare providers the same privacy protections as are afforded patients. Therefore, absent a contractual restriction on provider profiling, it will be permitted under the law of many states.
6. 17 USC § 102(a) (1997).
7. 17 USC §101 (1997).
8. Feist Publications, Inc. v Rural Telephone Service Co., 499 US 340 (1991).
9. 17 USC § 106 (1997).
10. 17 USC § 201(a) (1997).
11. See Thomson v Larson, No. 96 Civ. 8876 (LAK) (S.D.N.Y. 1997) (transcript of bench decision).
12. Kaplan v Vincent, 937 F.Supp. 307 (S.D.N.Y. 1996).
13. 17 USC §§ 204-205.
14. 17 USC § 101 (1997).
15. 17 USC § 101 (1997).

Adele A. Waller *and* ***Oscar L. Alcantara*** *are attorneys at law at the Chicago, IL, firm of Goldberg, Kohn, Bell, Black, Rosenbloom & Moritz, Ltd.*

Rights and Responsibilities Under Traditional Law

The traditional rule concerning ownership of medical records is reflected in the statutes and regulations of several states. When state statutes and regulations address ownership, they generally state that medical records are the property of the provider. For example, the California regulation concerning medical records maintained by hospitals and ambulatory care facilities provides, in part:

The medical record, including x-ray films, is the property of the hospital and is maintained for the benefit of the patient, the medical staff and the hospital. The hospital shall safeguard the information in the record against loss, defacement, tampering or use by unauthorized persons.[1]

According to this regulation, a California hospital's property interest in the medical record does not give it complete sovereignty over the record and its contents. Under this regulation, the provider's "ownership" of its medical records is similar to trusteeship. Under traditional principles of trust law, legal title resides in a trustee, but beneficial title resides in the trust's beneficiaries. This regulation suggests that while the record itself is the property of the hospital, the hospital is required to act in a role akin to that of trustee, maintaining the record for the benefit of the patient and the medical staff as well as of the hospital itself. Thus, a provider's "ownership" of a medical record is limited by the rights accorded the patient and the medical staff with respect to the record.

The law places several responsibilities on providers limiting their ability to exercise the sovereignty over the medical record that is normally associated with notions of ownership. For example, state statutes and regulations limit access to medical records to authorized personnel and require that access be granted to certain persons upon request. The California Code of Regulations provides, in part, that all required records should be maintained in a form that is legible and readily available on the request of: "the attending physician; the hospital or its medical staff or any authorized officer, agent or employee of either; authorized representatives of the Department; or any other person authorized by law to make such a request."[2]

Medical information is also regulated through statutes pertaining to medical records services in hospitals, which may contain restrictions on the physical removal of the records from hospital premises--another type of limitation on a hospital's ability to exercise the sovereign rights of an owner over its medical records. For example, the Kansas Code detailing the requirements of medical records services provides, in part:

Medical records shall be the property of the hospital and shall not be removed from the hospital premises except as authorized by the governing body of the hospital or for purposes of litigation when specifically authorized by Kansas law or appropriate court order.[3]

Providers' ability to exercise the rights of an owner over patient information is also limited by patients' rights in the information. Numerous states have statutes protecting patients' rights. In Illinois, for example, hospitals are required to permit a patient to examine and copy a patient's records after the patient's discharge from the hospital.[4] In approximately 28 states, individuals have some right to access or copy their medical records.[5] In some states, patients may only access hospital records, while in other states they may access both hospital and physician records.[6] A New Hampshire statute specifically states that medical records shall be deemed the property of the patient and that the patient is entitled to copy his or her medical record for a reasonable cost.[7]

The new Medicare Conditions of Participation proposed by the Health Care Financing Administration would require that hospitals provide patients with access to and copies of their medical records at a reasonable cost.8 In addition, the Secretary of Health and Human Services, concerning the confidentiality of individually identifiable health information pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), has recommended to Congress that patients be given the right to inspect and copy their information.[9]

Along with the right of access, some states accord patients the right to correct or amend (or request correction to) their medical records. For example, Washington's Uniform Health Information Act provides that, for purposes of accuracy or completeness, a patient may request in writing that a healthcare provider correct or amend the record of healthcare information to which a patient has access.[10] In her recommendations to Congress concerning the confidentiality of individually identifiable health information, the Secretary of Health and Human Services has proposed that individuals have the right to request amendment of their information.[11]

Another right granted to patients by some laws is the right to confidentiality. In some states, this is explicitly stated as a right. For example, the Illinois Medical Patient Rights Act establishes a general patient right to confidentiality:

Each physician, health care provider, health services corporation and insurance company shall refrain from disclosing the nature or details of services provided to patients, except that such information may be disclosed to the patient, the party making treatment decisions if the patient is incapable of making decisions regarding the health services provided, those parties directly involved with providing treatment to the patient or processing the payment for that treatment, those parties responsible for peer review, utilization review and quality assurance, and those parties required to be notified under the Abused and Neglected Child Reporting Act [325 ILCS 325/1 et seq.], the Illinois Sexually Transmissible Disease Control Act [410 ILCS

325/1 et seq.] or where otherwise authorized or required by law. This right may be waived in writing by the patient or the patient's guardian, but the physician or other health care provided may not condition the provision of services on the patient's or guardian's agreement to sign such a waiver.[12]

Even where the applicable statute or regulation does not state that a patient has a right to confidentiality, state laws concerning the confidentiality of medical information generally or the confidentiality of specific types of medical information, such as AIDS-related information and HIV test results, limit the ability of healthcare providers, as "owners" of medical records, to exercise sovereignty over medical records by, for example, disclosing the content of a record at will or selling the information in patient-identified form.[13]

A Colorado statute provides a unique example of a criminal code defining ownership rights in medical records. The Colorado statute defines a felony offense of theft of medical records or medical information as knowingly to obtain a medical record or medical information with the intent to appropriate the record or information to one's own use or the use of another, to steal or disclose to an unauthorized person a medical record or medical information, or to make or cause to be made a copy of a medical record or medical information without authorization.[14]The Colorado statute defines "proper authorization" as:

[W]ritten authorization signed by the patient or his duly designated representative or an appropriate order of court or authorized possession pursuant to law or regulation for claims processing, possession for medical audit or quality assurance purposes, possession by a consulting physician to the patient, or possession by hospital personnel for record-keeping and billing purposes.[15]

From this Colorado statute, one can infer that the patient has a property interest in his or her personal medical records and medical information, which can be violated by theft.

In some cases, the patient's rights in the information contained in the patient's record may not follow the information after it leaves the hands of the healthcare provider maintaining the original record. However, in at least some states, the patient's rights will survive any transfer of the information. For example, the California Confidentiality of Medical Information Act restricts redisclosure of medical information by a recipient of a disclosure.[16] In addition, the more sensitive the information, the more likely the patient's rights are to survive transfer of the information from the healthcare provider maintaining the original medical record.

HIPAA creates a new federal felony offense of wrongful disclosure of individually identifiable health information.[17] Specifically, Section 262 of HIPAA prohibits wrongfully disclosing or obtaining individually identifiable health information. Although what constitutes a "wrongful" disclosure has not yet been defined, penalties for violation of this criminal statute will include a fine of not more than $50,000, imprisonment of not more than one year, or both, with increased penalties if the violation is committed under false pretenses or with the intent to sell, transfer, or use the information for commercial advantage. This provision, when it becomes effective, will provide the first general federal right to the confidentiality of health information.

Statutes regulating genetic testing generally impose stringent requirements on the use of genetic information and the responsibilities of those who possess such information. For example, Oregon has enacted a Genetic Privacy Act, which designates the individual as the "owner" of his/her genetic information.[18] The act requires the informed consent of the individual before the genetic information can be used for most purposes.[19] Exceptions to the informed consent requirement include circumstances when genetic information is used for anonymous research where the identity of the subject will not be revealed.[20] The act includes safeguards to protect against disclosing the identity of the individual when genetic information is used anonymously.

The Oregon act also places restrictions on obtaining individually identified genetic information. The statute provides that no person shall obtain genetic information from an individual or from an individual's DNA sample without first obtaining the informed consent of the individual or the individual's representative, unless an exception applies.[21] This relatively recent statute represents an erosion of what is generally assumed to be a provider's right to record, in a patient's medical record, medical information that comes into the provider's possession.

As can be seen from this statute, specific, sensitive medical information may be declared the property of the patient by statute, further limiting the rights of healthcare providers to disclose and dispose of the information as they see fit.

Regardless of what a state statute specifies as to ownership of a medical record or the information contained therein, the patient almost always has confidentiality and access rights to the individual's medical record. Likewise, a healthcare provider, payer, or other entity authorized to maintain medical information concerning an individual almost always has rights to access and use its records for legitimate purposes, even though applicable confidentiality laws may require that some or all individually identifiable medical information be subject to special access controls (e.g., accessible only to employees with a need to access such information to provide care or for other permissible purposes).

As we have seen, a certain amount of complications arise under traditional medical record law in determining rights and responsibilities in patient data. An additional set of complexities arises in the information age, when physical medical records cannot be separated from the data they contain. Principles of provider rights and responsibilities with respect to medical records and patients' rights in their medical information must be applied to the patient data itself. This requires that healthcare providers take into consideration all of the relevant rights and responsibilities when making decisions about patient data.

Notes

1. Cal. Code Regs. tit. 22, § 70751 (1997).
2. Cal. Code Regs. tit. 22, § 71551 (1997).
3. Kan. Admin. Regs. § 28-34-9a (1996).
4. 735 S.H.A. ILCS 5/8-2001 (1997).
5. On September 11, 1997, the Secretary of Health and Human Services submitted recommendations to Congress regarding privacy rights in individually identifiable health information, pursuant to the requirements of the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996). The legislation recommended by the secretary would give, among other rights, patients a new right under federal law to inspect and copy information about them that is held by providers, payers, and public health authorities.
6. Frawley, Kathleen A. Testimony before the Subcommittee on Government Management, Information, and Technology, House Government Reform and Oversight Committee, June 14, 1996.
7. NH Rev. Stat. Ann. § 151:21 (1997).
8. 62 Fed. Reg. 66, 725 (December 19, 1997).
9. "Confidentiality of Individually-Identifiable Health Information." Recommendations of the Secretary of Health and Human Services pursuant to section 264 of the Health Insurance Portability and Accountability Act of 1996, submitted to the Committee on Labor and Human Resources and the Committee on Finance of the Senate, and the Committee on Commerce and the Committee on Ways and Means of the House of Representatives, September 11, 1997.
10. Wash. Rev. Code § 70.02.100(1) (1997).
11. "Confidentiality of Individually-Identifiable Health Information." Recommendations of the Secretary of Health and Human Services pursuant to section 264 of the Health Insurance

Portability and Accountability Act of 1996, submitted to the Committee on Labor and Human Resources and the Committee on Finance of the Senate, and the Committee on Commerce and the Committee on Ways and Means of the House of Representatives, September 11, 1997.
12. 410 S.H.A. ILCS 50/3 (1997).
13. See, e.g., A.R.S. §12-2292(1997) (Arizona statute concerning confidentiality and disclosure of medical records generally); NY Public Health Law § 2780 (1997) (statute concerning the confidentiality of HIV test results and AIDS-related information); NY Mental Hygiene Law § 33.13 (1997) (statute concerning the confidentiality of mental health records); Fla. Stat. § 397.501 (1996) (statute concerning the confidentiality of alcohol and drug abuse information.); NJ Stat. § 10:5-45 (1997) and § 10:5-47 (1997) (statutes concerning obtaining and disclosing genetic information.).
14. Colo. Rev. Stat. § 18-4-412 (1997).
15. Id.
16. Cal. Civ. Code § 56.13 (1996).
17. Pub. L. No. 104-191, 110 Stat. 1936 (1996).
18. Or. Rev. Stat. § 659.715 (1997).
19. Or. Rev. Stat. § 659.705 (1997).
20. Or. Rev. Stat. § 659.715 (1997).
21. Or. Rev. Stat. § 659.710 (1996).

Article citation:
Waller, Adele A., and Oscar L. Alcantara. "Ownership of Health Information in the Information Age". *Journal of AHIMA* 69, no.3 (1998): 28-38.