# AMERICAN ACADEMY OF PEDIATRICS

Pediatric Practice Action Group and Task Force on Medical Informatics

# Privacy Protection of Health Information: Patient Rights and Pediatrician Responsibilities

**ABSTRACT. Pediatricians and pediatric medical and surgical subspecialists should know their legal responsibilities to protect the privacy of identifiable patient health information. Although paper and electronic medical records have the same privacy standards, health data that are stored or transmitted electronically are vulnerable to unique security breaches. This statement describes the privacy and confidentiality needs and rights of pediatric patients and suggests appropriate security strategies to deter unauthorized access and inappropriate use of patient data. Limitations to physician liability are discussed for transferred data. Any new standards for patient privacy and confidentiality must balance the health needs of the community and the rights of the patient without compromising the ability of pediatricians to provide quality care.**

ABBREVIATIONS. HIPAA, Health Insurance Portability and Accountability Act of 1996; IRB, institutional review board; EDI, electronic data interchange; UPI, unique patient identification (number).

Pediatricians or their affiliated institutions are responsible for the security and confidentiality of medical records in their possession. Federal and state legislation has been enacted to regulate the privacy and protection of these records.[1] Currently more than 40 states have statutes imposing civil or criminal penalties for impermissible disclosure of medical information.[2]

The Health Insurance Portability and Accountability Act of 1996 (HIPAA)[3] authorizes the federal government to establish a national standard for medical record privacy either by legislative or regulatory action. Such federal standards are important, and care should be taken to balance the needs of society to advance public health and individual rights to privacy. The benefits to a community that may result from clinical and outcomes research, enforcement of health regulations, and risk management audits based on data harvested from patient records must be weighed against the risks of unauthorized access to individual health data. The American Academy of Pediatrics recommends that legislated or regulated provisions accommodate the unique needs of pediatric patients—newborns, infants, children, adolescents, and young adults. Furthermore, the American Academy of Pediatrics urges that legislated or regulated standards also address security requirements for electronic data transmission of health information.

These requirements should be reasonable and appropriate for the technology used to store, update, and transmit data. Most importantly, the security provisions should not unduly burden physicians or impede the provision of health care. The ability to transmit data electronically and the emergence of computerized medical records raise new issues about the responsibility of pediatricians transmitting patient-specific information.[4]

Although the principles of privacy protection apply equally to paper and electronic records, electronic data files are disseminated more easily than paper records and therefore may be more easily subject to unintended use. For example, data that include patient identification may be transmitted electronically to personnel of a health insurance payer to facilitate claim adjudication for reimbursement. Health insurers may also be required to use these data to comply with regulating organizations such as the National Committee for Quality Assurance (NCQA) Health Plan Employer Data and Information Set (HEDIS) measurements. However, these data can also be used to link a diagnosis code or demographic data to other clinical data or laboratory results. Data that disclose health conditions potentially associated with high financial costs may be used to discriminate unfairly against patients. Misuse of patient information for purposes unintended by the patient or pediatrician or not delineated in the providers' contractual documentation violates the right to privacy of patients.

Pediatricians or their affiliated institutions are obligated to protect the confidentiality of all patient medical records. Protection can be achieved by implementing security policies to control access to patient records, requiring appropriate authorization before releasing health data, and providing additional security measures to more sensitive data.

## PRIMARY AND SECONDARY USES OF HEALTH DATA

Decisions to monitor, restrict, or control access to individual medical records may be evaluated by determining whether those accessing information are primary or secondary users of health information.[5] Primary users are clinicians (physicians, nurses, nursing assistants, therapists, and other allied health professionals) who need access to patient informa-

The recommendations in this statement do not indicate an exclusive course of treatment or serve as a standard of medical care. Variations, taking into account individual circumstances, may be appropriate.

tion to provide appropriate health care to the patient. At least one state has enacted legislation prohibiting the transfer of maternal health information to the child's hospital nursery. The restrictions on providing information may put the health of the newborn at risk by not allowing essential maternal history to be available to the newborn's clinicians.

Secondary users of health data include researchers, educators, third-party payers, business administrators, legal representatives, auditors, employers, public health officials, and quality assurance and utilization review staff who may or may not also be clinicians. The secondary users' need for access to health data may be unrelated to the patient's treatment. Patients have a right to be notified of the individuals, organizations, and government agencies that have authority to access or receive data from their medical records. Health insurers or payers who require access to patient records as part of their ongoing quality improvement program or utilization review should be required to notify insured patients of this requirement. Disclosures about the need to review or excerpt patient data should specify whether these aggregate data or data that identify individuals are analyzed and for what purpose. If traceable patient data are used, secondary users should be required to abide by federal security provisions to protect patient confidentiality.

## ACCESS TO MEDICAL RECORDS

Medical records are the property of the institution at which they were created, but patients generally have certain rights to the information contained in the records, which vary from state to state.[6] Pediatricians and their patients (and/or custodial parents) decide who may have limited or comprehensive access to information contained in the medical records. Generally, custodial parents are entitled to review their children's medical record at any time, except for emancipated minors or minors with other specific rights to confidentiality. Pediatricians have a crucial role in mediating discussions between parents and adolescents to minimize conflicts over access to this information. Preadolescents and adolescents may also have other rights to confidentiality and may limit access to their medical records based on their age, the nature of their diagnosis, or other factors delineated by state or federal law.[6,7] These rights must be recognized and protected by all parties with access to the patient's medical record and should not be diminished by federally mandated standards for privacy of health information.

Patients (and/or custodial parents) should be aware of the risks associated with authorizing the release of health information for purposes unrelated to patient treatment and consider the following:

- the sensitivity of the information,
- whether the data have been requested by a primary or secondary user,
- the stated use for the data,
- whether limited or complete access to patient data has been requested,
- whether the data identify patients or are blinded, and
- whether the data are analyzed and reported as independent or combined with other patient information and analyzed and reported as aggregate.

The Institute of Medicine has delineated three levels of security based on the nature of the specific health information in a patient record: nonprivileged (least sensitive), privileged (sensitive and traditionally confidential), and deniable (extremely sensitive and confidential).[8] Electronic security tools such as electronic signatures, passwords, encryption, patient identifiers, clinician authentication, and audit trails may permit graduated levels of security, with extremely sensitive information receiving the most security protection. Required data collection and reporting to secondary users, however, may make it difficult to protect sensitive information about sexually transmitted diseases,[9] adoption,[10–12] physical abuse,[13] substance abuse,[14,15] human immunodeficiency virus infection,[16,17] sexuality,[18–21] genetic disorders, cancer, and mental health. Health information that is divided to permit only limited access to or selective release of required data may afford additional security, such as the use of separate sections (in paper-based medical records) or password protected data fields (in electronic medical records).

## MEDICAL RECORD RELEASE FORMS

Patients should not be required to give unconditional release of their medical records to unknown sources. Unlimited permission may expose patient records to inappropriate use of the medical information. In group practices, in practices owned by corporate entities, and for the purpose of obtaining consultation, clinicians may share medical information as needed to provide treatment. Clinical and administrative staff need to understand the limitations of their access to patient information and their responsibility to protect the patient's right to privacy. Pediatricians or their affiliated institutions should enforce disciplinary action for inappropriate access to or disclosure of patient health information by clinical or administrative staff. Signed release forms should be obtained to document authorized releases of health information. Pediatricians or their affiliated institution should keep all original medical record documents.

Anonymous patient information and data to be used for medical education, research, or public health functions should be accessible under standard protocols monitored by appropriate bodies, such as institutional review boards (IRBs).[22] There may be situations, however, in which researchers need access to medical records that identify patients' records only accessible by entities under the purview of an IRB with appropriate security to protect the patient's privacy. Specific statutes may mandate disclosure without informed consent, as in cases of child abuse.[23] In the absence of appropriate IRB approval of access to medical records for research purposes, the individual medical record should only be ac-

cessed or transferred with the informed consent of the patient (and/or custodial parents).[24]

### ACCURACY AND INTEGRITY OF MEDICAL RECORDS

Pediatricians or their affiliated institutions are responsible for the accuracy and integrity of their medical records. Information contained in medical records should be accurate, objective, legible, timely, and comprehensive. Once an entry is made into the medical record, it should never be deleted.[25] If it is later determined that specific information in an entry is incorrect, it may be changed by the clinician as long as the original entry remains legible and the corrected entry is clearly marked, dated, and initialed. Changes made to electronic medical records are done more easily and may be more difficult to discern. Clinicians using electronic information systems should verify that security protocols are in place to ensure against unauthorized changes or attempts to modify the electronic record. With the same procedure as that used by clinicians, patients (and/or custodial parents) also may append written comments to the medical record.

### ELECTRONIC TRANSMISSION OF HEALTH DATA

Pediatricians should use reasonable security practices to safeguard the confidentiality of patient data when patient records are transmitted electronically, whether by facsimile, electronic mail, the Internet, or other channels. Ideally, patient information transmitted electronically should be sent to a specific person who agrees to be responsible for the information once it is received. Health information should not be transmitted to an unidentified receiving station. To maintain confidentiality, use of cover sheets with privacy disclaimers and requests for return receipts for transmitted data are appropriate and prudent strategies. Software products are available to encrypt sensitive medical information and may improve the security of the transmission. Once the transmission of the medical record has occurred, federal regulations should mandate that the privacy of the health information is the responsibility of the receiving party and that the information is used exclusively for those purposes stated in obtaining the record. Informed consent from the patient must be obtained to use the information for any other purpose.

### ELECTRONIC BILLING

The shift from paper-based accounting to electronic billing and reimbursement with federally mandated uniform format requirements may prompt clinicians to use outside sources for certain electronic data interchange (EDI) functions. These EDI clearinghouses or value added networks receive electronic transmissions from an affiliated institution (for example, a physician office or pediatric clinic), translate the data into the required electronic format, and transmit the data electronically to the payer. EDI vendors should be accredited to ensure that their data security systems meet the federal standards for patient privacy and security. Under current HIPAA regulations, penalties of $100 per violation, not to exceed $25 000 per person per year, may be imposed for failing to comply with these standards. Consequently, institutions that have used an accredited EDI vendor should not be liable for vendor errors. Federal standards for electronic transmissions supersede state law unless the state receives a waiver from the Secretary of Health and Human Services. State Medicaid programs should be required to comply with federal EDI standards.

### HEALTH REGISTRIES

The development of health registries indicates that certain elements of an individual's medical record may need to be accessible by the public.[26] Health registries are organized systems for collecting, storing, retrieving, analyzing, or disseminating information on individuals with a particular disease, risk factors, or exposures to a substance or circumstance known to cause adverse health effects. Registries may be operated by federal government agencies (eg, the National Exposure Registry), universities (eg, Surveillance, Epidemiology and End Results, a cancer registry), nonprofit organizations (eg, United States Eye Injury Registry), private groups (eg, transplant registries), or state governments (eg, electronic birth registries, newborn laboratory screening systems, and immunization registries). Plans for implementing a unique patient identification (UPI) number as part of the HIPAA administrative simplification provisions were stopped when it was perceived that the establishment of the UPI could create a national health databank. This raised concerns regarding patient privacy and medical record confidentiality. The federal government decided to halt development of the UPI standard until federal statutes or regulations protecting the privacy of health information are in place.

More than 20 states have begun to establish immunization registries and many others are considering legislative proposals to authorize them. Such public health measures are intended to protect the community from outbreaks of vaccine-preventable diseases, to assess the cost-effectiveness of care, and to simplify the reporting of data to state health agencies or local schools. However, without appropriate security protections and prospective patient authorization to release immunization data, vaccine registries may contribute to the erosion of privacy of patient health information. California has recently enacted legislation granting health care professionals access to immunization databases without the patient's consent. When the benefits to the public outweigh the need for patient privacy, pediatricians may choose to support such a program[27] but should ensure that potential liability risks associated with releasing patient data to a registry are minimized. Before collection of immunization registry data commences, adequate privacy protections need to be in place, including restricted access to data entry, update, review and release; strict penalties for unauthorized disclosure; and protection of the registry system from court order or subpoena. The registry staff should provide written policies describing the privacy and security standards, which should be dis-

seminated to registry employees, immunization providers, patients, and parents. These policies should explain the purposes for which the data are to be used, the parties that will be allowed to input and receive data, and the requirement for written authorization before any data are released for purposes not intended by registry policies and regulations.

Pediatricians need to protect the information in their patients' medical records. Federal requirements supersede less protective state laws and no existing rights to privacy presently afforded to patients, particularly to minors, should be expunged, limited, or restricted by new federal privacy standards. HIPAA legislation does not intend to reduce the privacy protections currently afforded pediatric patients.

## RECOMMENDATIONS

1. Pediatricians should understand and abide by legislative and regulatory requirements that address the confidentiality, secure transmission and storage, and public accessibility of patient medical information.
2. Pediatricians or their affiliated institutions should accept the responsibility for protecting the confidentiality of their medical records by personnel education, office procedures, and security strategies that are in compliance with federal standards.
3. Pediatricians should advocate for the ability to access medical information for properly regulated medical education, research, and public health functions that undergo periodic and systematic review of their appropriateness and that comply with applicable patient confidentiality and research regulations.
4. Pediatricians should urge policy makers to weigh the administrative burdens and risks to patient confidentiality against the projected benefits to be derived from medical data being collected, protected, analyzed, or disseminated either publicly or privately.
5. Pediatricians should support legislation to require payers to notify their insured at least annually whether the payers may review their medical records. Such notification should identify the reviewers and the data, and purposes (for example, continuous quality improvement, review of claims, or accreditation) for which the data are to be used.
6. Patients (and/or custodial parents) should be advised of the risks associated with signing unconditional releases for their health information.
7. Patients (and/or custodial parents) should know their rights to keep their medical information confidential. Insurers should be required to inform them of the consequences to their insurance coverage should they refuse the insurer access to medical information. Patients should be notified of regulatory or legislative requirements that may require outside access to their record.
8. Patients (and/or custodial parents), within the limits of statute, should have the right to review their medical records. They should be permitted to append comments to chart notations that they believe incorrect or incomplete, to authorize the release of health information, and to request in writing a copy of their medical records.
9. Pediatricians or their affiliated institutions have a right to retain original medical records. On receipt of a written request from the patient authorizing the release of their medical record, pediatricians or their affiliated institutions may provide a summary or photocopy of the complete record and may charge reasonable fees for providing copies.



## REFERENCES


1. Gostin LO, Lazzarini Z, Neslund VS, Osterholm MT. The public health information infrastructure: a national review of the law on health information privacy. *JAMA*. 1996;275:1921–1927
2. Computer-based Patient Record Institute, Workgroup on Confidentiality, Privacy and Legislation. Access to patient data. Available at: http://www.cpri.org/docs/access.html, April 15, 1994. Accessed May 23,1999
3. The Health Insurance Portability and Accountability Act of 1996. Available at: http://www.hcfa.gov/hipaa/hipaahm.htm. Accessed May 23, 1999
4. American Academy of Pediatrics, Task Force on Medical Informatics, Section on Computers and Other Technologies, Committee on Practice and Ambulatory Medicine. Safeguards needed in the transfer of patient data. *Pediatrics*. 1996;98:984–986. Available at: http://www.aap.org/policy/00984.html. Accessed May 23, 1999
5. Dick RS, Steen EB, eds. *The Computer-Based Patient Record: An Essential Technology for Health Care*. Washington, DC: Institute of Medicine, National Academy Press; 1991:33–34. Available at: http://books.nap.edu/books/0309044952/html/33.html. Accessed May 23, 1999
6. American Academy of Pediatrics. Confidentiality in adolescent health care. *AAP News*. April 1989. Available at: http://www.aap.org/policy/104.html. Accessed May 23, 1999
7. American Academy of Pediatrics, Committee on Adolescence. Sexual assault and the adolescent. *Pediatrics*. 1994;94:761–765. Available at: http://www.aap.org/policy/00465.html. Accessed May 23, 1999
8. National Research Council, Committee on Human Genome Diversity. *Evaluating Human Genetic Diversity*. Washington, DC: National Academy Press; 1997:52–53. Available at: http://pompeii.nap.edu/0309059313/html/52.html. Accessed May 23, 1999
9. American Academy of Pediatrics, Committee on Adolescence. Sexually transmitted diseases. *Pediatrics*. 1994;94:568–572. Available at: http://www.aap.org/policy/0041.html. Accessed May 23, 1999
10. American Academy of Pediatrics, Committee on Early Childhood, Adoption, and Dependent Care. Issues of confidentiality in adoption: the role of the pediatrician. *Pediatrics*. 1994;93:339–341. Available at: http://www.aap.org/policy/00072.html. Accessed May 23, 1999
11. American Academy of Pediatrics, Committee on Early Childhood, Adoption, and Dependent Care. Families and adoption: the pediatrician's role in supporting communication. *AAP News*. February 1992. http://www.aap.org/policy/194.html. Accessed May 23, 1999
12. American Academy of Pediatrics, Committee on Adolescence. Counseling the adolescent about pregnancy options. *Pediatrics*. 1998;101:938–940. Available at: http://www.aap.org/policy/re9743.html. Accessed May 23, 1999

13. American Academy of Pediatrics, Committee on Child Abuse and Neglect. Public disclosure of private information about victims of abuse. *Pediatrics*. 1991;87:261. Available at: http://www.aap.org/policy/03774.html. Accessed May 23, 1999
14. American Academy of Pediatrics, Committee on Substance Abuse. Testing for drugs of abuse in children and adolescents. *Pediatrics*. 1996;98:305–307. Available at: http://www.aap.org/policy/01495.html. Accessed May 23, 1999
15. American Academy of Pediatrics, Committee on Substance Abuse. Tobacco, alcohol, and other drugs: role of the pediatrician in prevention and management of substance abuse. *Pediatrics*. 1998;101:125–128. Available at: http://www.aap.org/policy/re9801.html. Accessed May 23, 1999
16. American Academy of Pediatrics, Task Force on Pediatric AIDS. Adolescents and human deficiency virus infection: the role of the pediatrician in prevention and intervention. *Pediatrics*. 1993;92:626–630. Available at: http://www.aap.org/policy/05071.html. Accessed May 23, 1999
17. American Academy of Pediatrics, Committee on Pediatric AIDS. Surveillance of pediatric HIV infection. *Pediatrics*. 1998;101:315–319. Available at: http://www.aap.org/policy/re9732.html. Accessed May 23, 1999
18. American Academy of Pediatrics, Committee on Adolescence. Homosexuality and adolescence. *Pediatrics*. 1993;92:631–634. Available at: http://www.aap.org/policy/05072.html. Accessed May 23, 1999
19. American Academy of Pediatrics, Committee on Adolescence. Contraception and adolescence. *Pediatrics*. 1990;86:134–138. Available at: http://www.aap.org.policy/03122.html. Accessed May 23, 1999
20. American Academy of Pediatrics, Committee on Adolescence. Adolescent pregnancy: current trends and issues, 1998. *Pediatrics*. 1999;103:516–520. Available at: http://www.aap.org/policy/re9828.html. Accessed May 23, 1999
21. American Academy of Pediatrics, Committee on Adolescence. The adolescent's right to confidential care when considering an abortion. *Pediatrics*. 1996;97:746–751. Available at: http://www.aap.org/policy/01348.html. Accessed May 23, 1999
22. American Academy of Pediatrics, Committee on Drugs. Guidelines for the ethical conduct of studies to evaluate drugs in pediatric populations. *Pediatrics*. 1995;95:286–294. Available at: http://www.aap.org/policy/00655.html. Accessed May 23, 1999
23. American Academy of Pediatrics, Committee on Child Abuse and Neglect. Guidelines for the evaluation of sexual abuse of children: subject review. *Pediatrics*. 1999;103:186–191. Available at: http://www.aap.org/policy/re9819.html. Accessed May 23, 1999
24. American Academy of Pediatrics, Committee on Bioethics. Informed consent, parental permission, and assent in pediatric practice. *Pediatrics*. 1995;95:314–317. Available at: http://www.aap.org/policy/00662.html. Accessed May 23, 1999
25. Robertson, WO, Lockhart JD, eds. *Medical Liability for Pediatricians*. 5th ed. Elk Grove Village, IL: American Academy of Pediatrics; 1995:26–27
26. American Academy of Pediatrics, Committee on Practice and Ambulatory Medicine. Policy on the development of immunization tracking systems. *Pediatrics*. 1996;97:927. Available at: http://www.aap.org/policy/01398.html. Accessed May 23, 1999
27. American Academy of Pediatrics. Testimony presented to the Centers for Disease Control and Prevention National Vaccine Advisory Committee Immunization Workgroup on Ensuring Provider Participation. Available at: http://www.cdc.gov/nip/registry/fourthmeeting/I_4_t_22.htm. July 17, 1998. Accessed May 23, 1999