Safeguards Needed in Transfer of Patient Data

Task Force on Medical Informatics, Section on Computers and Other Technologies, Committee on Practice and Ambulatory Medicine

ABSTRACT. The intent of this statement is to provide practitioners with information to assist them in safeguarding the electronic storage and transmission of patient data. It lists safeguards that should be in place in pediatric practices that send facsimiles of patient data. Issues of protecting patient and provider confidentiality, maintaining the security of these data, and state and federal health data legislation are also addressed.

The electronic storage and transmission of data can benefit children throughout the United States. The efficiency and versatility of a computer-based medical record promise advances in the delivery of health care services to children in a more cost-effective and comprehensive manner. The American Academy of Pediatrics looks forward to the benefits that will be obtained from electronically based patient records. Current research to establish a national immunization database registry, the development of clinical databases facilitating the treatment of children ingesting toxic substances, and the diagnosis of dysmorphism in children all illustrate the advantages of computerization.

The electronic storage and transfer of information is not without risk. The potential for losing these data exists, and a strict adherence to data backup must be followed. Other risks include patients' loss of privacy and confidentiality and the possible loss of physicians' autonomy and confidentiality. Pediatricians should be cognizant of these risks and protect their patients and themselves. Every pediatric practice should establish policies and procedures that protect the patient's record. Only those providers with a need to know specific medical information should be granted access to patient information, and that access should be limited to those portions of the patient's medical file that pertain to the provider's particular function. A log that tracks who has accessed the medical record should be maintained.

As health care providers and payers become more firmly committed to containing the costs of care, pediatricians are requested to submit more information about their patterns of practice and their patients. Hospitals and groups providing payments for care are eager to use data from the electronic record to profile and establish pediatricians' practice patterns, to identify patients' risk factors, and to secure both patients' and pediatricians' compliance with service standards. The precise use of these data should be prospectively stated to both the patient and the pediatrician, and both should be protected from inappropriate electronic access to a record. To protect their patients, pediatricians must also know why individual groups need access to electronic data. In cases in which data are needed for research purposes, patients' personal identifying information should not be disclosed so that their privacy will be protected.

It is obvious that the use of electronic records and the electronic transfer of information may undermine the physician-patient relationship and jeopardize the security and privacy of both the patient and the physician. These issues may be exacerbated by the security problems inherent in the electronic transfer of information, whether by computer or fax. Specifically, these problems are: (1) anyone with access to the record system being able to read the record, and (2) the lack of security associated with computer software. A system must be capable of providing indelible and author-identifiable markings for all entries and modifications made to the medical record. Any transmission of information should be recorded in the patient's chart.

The following safeguards should also be in place in pediatric offices that send facsimiles of patient data:

- Obtain patient authorization for release of data.
- If the payer requires signing of a blanket permission, it may be to the practice's advantage to explain the implications of a blanket permission to the family, if time permits.
- A cover sheet stating that confidential data are being transmitted should be appended to all facsimiles.
- Pediatricians should understand that medical records sent via telefax result in a hard copy of the patient record being present in an unprotected state at the receiving end.
- A secured facsimile machine should be used, one that is preferably located in the pediatrician's private office. If possible, the pediatrician should know to whom the information is being sent and who is responsible for protecting the information.

Pediatric practices should maintain records of any transmissions and request the authorized receivers to sign and return attached receipts when the facsimile data are received. In addition, pediatric practices should have in place a process that details how the

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.
been a basic tenet of the US medical system. Infor-
text patient privacy. This involves receipt of medical
practice handles patient-related information to pro-
cause the storage and transfer of patient information
Case law has upheld these principles. In addition,
considered confidential. Most states prohibit the dis-
mation imparted
records, as well as laboratory, consultation, and pa-
to a physician by a patient has been
mponential safeguards are ifiustrated by a recent re-
view of childhood immunization registries that re-
vealed the following:

- Federal statutes protecting the confidentiality of
unimmunization information do not exist.
- There are inconsistencies in the manner in which
states address confidentiality as it applies to vac-
cine registries.
- Parental consent should be required for use of
information for nonimmunization purposes.
- Both patients and parents could be potentially
harmed by inappropriate access to sensitive health
information.
- State and federal authorities should resolve the
privacy and confidentiality issues to assure the
public that registries will not invade a patient’s or
family’s privacy.
- Privacy safeguards should eliminate inappropri-
ate access to these data, provide strict penalties for
unauthorized disclosure, and protect these data
from court order or subpoena, in keeping with the
usual standards applied to any medical infor-
tion.3

Some agencies and institutions currently inter-
est in obtaining data from patients’ medical
records have tried to circumvent the issue of confi-
dentiality by separating “administrative” from “clini-
cal” information. Although certain information such
as demographic data may be purely administrative,
the lines rapidly blur with major consequence. For
example, if a pediatrician participating in an epide-
miologic study reports to a hospital that a patient has
a condition such as phenylketonuria, that informa-
tion may then be used by an insurer to deny the
family coverage. Disclosure of the results of a toxi-
cology screen could result in an adolescent being
denied admission to college.

RECOMMENDATIONS

The American Academy of Pediatrics advocates
the establishment of national standards that define
the elements and content of an electronic health care
record and that set forth protocols for the transmis-
and sharing of information electronically. Be-
cause of the lack of uniformity in state laws, the
Academy recognizes the need for the development of
establishment of federal legislation to ensure the integrity, confiden-
tiality, and privacy of the electronically recorded,
stored, and transmitted data. Such legislation should
establish guidelines for electronic transmission of
medical information that will protect the privacy of
patients and support the pediatrician-patient rela-
tionship.

In addition, the existing patchwork of state laws ren-
ders interstate transport of data difficult. For example, the
payer in one state may demand information that another
state would deem confidential. Because state laws may
vary, pediatricians should include a clause in their man-
ged care contracts that the laws in the state in which the
pediatrician practices will prevail.4

Pediatricians should also be knowledgeable about
both the local laws regulating the use and sharing of
information from the patient record and the conse-
quences of patient profiling as practiced by hospitals
and managed care providers.

Pediatricians should recognize that the electronic
transmission of patient-specific information should
not be assumed to be secure. Therefore, care must be
taken to protect the patient’s right to confidentiality.
Patient data must be safeguarded against tampering
and unintentional modification or destruction. Pro-
viders should also establish a system to track and
audit access to and alteration of patient information.

The electronic record has the capability of advanc-
ing the practice of medicine. It is the pediatricians’
right and responsibility to ensure that the develop-
ment of the electronic record and the transmission
and sharing of these records both benefit children
and their parents or guardians and protect patients’
and pediatricians’ rights to privacy.

TASK FORCE ON MEDICAL INFORMATICS, 1995 TO 1996
James Lustig, MD, Chairperson
Jerold Aronson, MD
Mitchell Feldman, MD
Edward Gotlieb, MD
Barbara Harley, MD
Mark Reuben, MD
Melvin Stern, MD
Jack T. Swanson, MD

COMMITTEE ON PRACTICE AND AMBULATORY
MEDICINE, 1995 TO 1996
Peter D. Rappo, MD, Chairperson
Edward O. Cox, MD
John L. Green, MD
James W. Herbert, MD
E. Susan Hodgson, MD
James Lustig, MD
Thomas C. Olsen, MD
Jack T. Swanson, MD

Downloaded from http://pediatrics.aappublications.org/ at Jack Swanson on October 3, 2017
REFERENCES


Safeguards Needed in Transfer of Patient Data
Task Force on Medical Informatics, Section on Computers and Other Technologies, Committee on Practice and Ambulatory Medicine
Pediatrics 1996;98;984

Updated Information & Services
including high resolution figures, can be found at:
http://pediatrics.aappublications.org/content/98/5/984

Permissions & Licensing
Information about reproducing this article in parts (figures, tables) or in its entirety can be found online at:
https://shop.aap.org/licensing-permissions/

Reprints
Information about ordering reprints can be found online:
http://classic.pediatrics.aappublications.org/content/reprints
Safeguards Needed in Transfer of Patient Data
Task Force on Medical Informatics, Section on Computers and Other Technologies, Committee on Practice and Ambulatory Medicine
*Pediatrics* 1996;98;984

The online version of this article, along with updated information and services, is located on the World Wide Web at:
http://pediatrics.aappublications.org/content/98/5/984