Chapter 5
Protecting Privacy in the Child's Electronic Health Record

S. Andrew Spooner

Abstract With the increasing availability of electronic health records, translational researchers frequently wish to extract information from or add information to these records to support various research projects. It is important that investigators be familiar with laws and regulations that protect the privacy of patients and restrict who can view or extract information from their EHRs. Laws and professional standards demand that all individually identifiable health information be secured at a high level and handled as private, sensitive information. Some information (mental health, reproductive health, abuse) is generally regarded as more sensitive than others in the health care of a patient at any age. In a situation where minors are involved, these security and privacy policies become more complicated because of possible conflicts between the interests of the child and the interests of parents or guardians. Situations specific to pediatric clinical practice and research increase the difficulty of implementing these policies: adolescent care, adoption, fetal care, foster care, and genetic disease. Security policies for access to systems intended to be used by patients (personal health records and patient portals) are complex. They can become even more challenging when the child has participated in clinical research and unexpected clinically relevant results are obtained.

S.A. Spooner, M.D., M.S., FAAP (✉)
Department of Pediatrics, University of Cincinnati College of Medicine, Cincinnati, OH, USA

Division of Biomedical Informatics, Cincinnati Children's Hospital Medical Center, 3333 Burnet Avenue, ML-9009, Cincinnati, OH 45229-3039, USA
e-mail: andrew.spooner@cchmc.org

J.J. Hutton (ed.), *Pediatric Biomedical Informatics: Computer Applications in Pediatric Research*, Translational Bioinformatics 2, DOI 10.1007/978-94-007-5149-1_5,

5.1 The Information in an Electronic Health Record (EHR)

Investigators conducting translational research frequently wish to extract information from or add information to patients' EHRs to support various research projects. It is important that they be familiar with laws and regulations that protect the privacy of patients and restrict who can view or extract information from patients' EHRs.

5.1.1 Basic EHR Data Integrity

Like the research record, the electronic health record demands a high level of data integrity. While the goal of policies governing data integrity in the research record is to ensure scientific rigor, the goals of policies governing data integrity in the EHR are of a different nature and affect the use of the EHR to support research:

- The EHR is a medical record that supports clinical care of a patient
- The EHR must be clinically accurate, even in the absence of well-defined data collection processes
- The data in the EHR belong to the patient, and must be provide to the patient at any time. The patient can also request changes to the chart (although these requests do not have to be honored if they are inappropriate) and the patient/parent may also add documentation to the chart at any time.
- The EHR plays an important role in legal defense of malpractice claims. Although the medical record is classified as hearsay, one may still use it in court if one can show that the record is maintained in a businesslike way. Any evidence that the medical record is being used for purposes other than clinical care may render the record useless in legal defense. For this reason, there are usually limitations on which people in which job roles are allowed to make entries in the record.
- The medical record may be shared among many providers or even across institutions. As electronic EHRs gain in prevalence, electronic methods for doing this sharing also become more prevalent, and it becomes even more important for the records to be maintained by those in familiar job roles (physician, nurse, etc.).

5.1.2 Data Entry

Clinical care is accompanied by the recording of a large amount of free text and a small amount of discrete data. While EHRs vary in the extent to which they demand discrete data entry, it is accepted that free-text entry (in the form of dictation, text-generating macros, or typing) is necessary to capture the complexity of clinical care. One might be able to reduce very simple patient encounters to a series of check boxes, but in academic medical centers when even moderately complex disease

is addressed, it is not reasonable to expect clinicians to adhere to templates that generate primarily discrete data.

There are areas of the EHR, like laboratory test results and medication orders, which contain a preponderance of discrete data. In these areas there are usually a number of regulatory agencies that govern how these data are structured. For example, U.S. clinical laboratory procedures are certified through a program defined by federal law (Kroger 1994). Under these conditions, one is not free to set up investigational clinical laboratory tests as a part of routine care and incorporate them in the EHR. Likewise, prescription data must conform to data standards that allow electronic prescribing, so investigational drugs present a challenge to represent in clinical EHRs. These regulatory hurdles, while they serve a good purpose, may make it impossible to use the EHR itself as a research record, even if the proper institutional review board assurances are obtained. "Shadow records" that parallel the clinical record for research can cause confusion in the clinical operation, especially when the research activities overlap with normal clinical activities.

Another particular challenge of maintaining research data that parallels clinical data is how to handle discrepancies between the two. It is customary to apply data quality standards to research data. For example, one may want to select a particular blood pressure, collected under certain conditions, for a data point in a research study. One might then delete all other blood pressures from the research record in order to establish the data point of interest. This kind of selection of data is not usually possible in an EHR. All data are retained, and deleting data—even if it is erroneous—must be done in a way that retains all data for future inspection. Most clinical operations that allow corrections of data in the EHR have strict policies about how the change is documented. It would be unusual to see a situation where data from a clinical research study would flow back to the clinical record as a correction, regardless of how valid the correction might be. In any case, only those personnel authorized to make entries in the clinical record can initiate those changes.

5.2 Privacy Concepts in Pediatrics

Health care information is sensitive, and as such is protected by the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (National Committee on Vital and Health Statistics 1997), as well as state laws. Because most episodes of pediatric care involve at least two people in a patient role (the actual patient and the parent or guardian), and perhaps many more, the task of securing information while maintaining the appropriate level of access is especially challenging in pediatrics. As technology moves toward fulfilling the goal of faster information flow and higher transparency, these issues are exacerbated. Pediatric clinical research, especially in genomics, can also generate health care information that creates privacy concerns. These issues are discussed in Chap. 4, Institutional Cybersecurity in a Clinical Research Setting; Chap. 6, Research Patient Data Warehousing; and Chap. 7, Biobanking in Pediatric Research.

5.2.1 HIPAA – Health Insurance Portability and Accountability Act of 1996

The U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA) intended to provide for continuity of health insurance coverage after a change in employer. This initial goal never materialized, but the portion of the law that required electronic transmission of health care claims (Title 2) remained. This portion of the regulation, known as "Administrative Simplification," raised concerns about privacy and security of the claims information that was required to be sent. This concern spawned the HIPAA Privacy Rule and the HIPAA Security Rule, enacted in April 2003 and currently enforced by the U.S. Office of Civil Rights (HHS 2002). While the full detail of these rules is beyond the scope of this text, it is important to appreciate that HIPAA remains the main driver of how clinicians behave to protect health information (privacy rules, mostly) and how systems are designed to protect it (security). An important principle regarding the use of EHR information is the "minimum necessary" rule, which states that those who access the record see only that part of the record that is necessary for performance of their job. This principle affects (or should affect) users's behavior, but it also guides policies for who is given access to what parts of the EHR. A researcher wanting to examine records of patients solely for the purposes of research would violate this rule. The HITECH Act of the American Recovery and Reinvestment Act of 2009 (HHS 2009) strengthen HIPAA's privacy and security requirements, and imposed stiffer penalties for violations.

5.2.2 HIPAA Business Associate Agreements

Those who work with health data, unless the data are suitably rendered anonymous, may be subject to the HIPAA privacy and security rules and the attendant penalties, through business associate agreements. These agreements bind recipients of health care data to the same rules that the clinical originators of data must follow, and applies the same penalties for breaches of confidentiality.

5.2.3 Pediatric Aspects of HIPAA

The HIPAA Privacy Rule allows parents or guardians access to the child's health information in almost all situations. Exceptions include when the minor is the one who consents to care and the consent of the parent is not required under State or other applicable law; or when the minor obtains care at the direction of a court; or if the parent agrees that the minor and the health care provider may have a

confidential relationship (HHS 2002). Privacy laws vary from state to state, and providers are obliged to follow the most stringent one. Since control of children's health information is sometimes a hot political topic (as in the case of minors' access to reproductive health services) these legal conflicts can make control of data very complicated (Chilton et al. 1999).

5.2.4 *FERPA – Family Educational Rights and Privacy Act*

A law that existed many years before HIPAA was the Family Educational Rights and Privacy Act (FERPA) (Kiel and Knoblauch 2010) which attempts to give students some control over the use of their educational records. When healthcare is provided at a school, the line between health records and educational records is blurred, and there can appear to be conflicts between HIPAA and FERPA. If one is attempting to aggregate data from both educational and healthcare settings, these specific laws may come into play. The U.S. Department of Education and the U.S. Department of Health and Human Services published joint guidance on navigating these apparently conflicting laws in 2008 (HHS 2008).

5.2.5 *Release of Information*

A common function of the information systems in a healthcare organization is the release of information based on a request from a patient, parent, guardian, lawyer, State agency, or other suitably approved group. Release of information (ROI) in a hospital is typically handled via a controlled process through the Health Information Management department or similar entity. Before the age of EHRs, the actual conveyance of medical records was achieved by a tedious and time-consuming process of photocopying paper records or printing images of documents from archived storage. It was considered normal for this process to take several weeks. The difficulty of this process rendered the medical record effectively inaccessible to all, but the most dedicated patients and their representatives.

In the information age, expectations about the ease by which one can get information are changing. The Continuity of Care Document project (Ferranti et al. 2006) is a manifestation of the expectation that electronic health records can produce immediate summary information for the purposes of sharing across venues of care. The expectation of immediate access has spread to all areas of the EHR (How et al. 2008). These expectations entail more sophisticated authentication methods than the typical notarized permission form that usually initiates the process of Return of Information (ROI) in health care institutions using traditional paper based systems.

ROI is important to understand in pediatric care because it means that all information in the chart (or at least that part designated the "legal medical record") is available to the guardian at all times. While in the past it may have been comforting to a child/adolescent to assume that information would be "secure" from prying parental eyes because of a 6-week wait for photocopying, that wait will eventually be reduced to practically zero through electronic methods. Parents or guardians will have contemporaneous access to all details in a child or adolescent's chart. We have not yet had the opportunity to evolve habits in practice that take this into account, or sophisticated privacy policies that balance the need to keep things truly private between a provider and a minor patient under the assumption of immediate parental electronic access.

5.2.6 Clinical Data Sharing Versus Financial Data Sharing

Regardless of privacy policies put in place, the fact that guardians receive billing information about health services provided also runs counter to the concept of keeping things private between a minor and a provider. Doctors who treat adolescents have been known to write prescriptions on paper or provide samples rather than run the risk of notifying a parent via a pharmacy claim. Regardless of how one feels about the appropriateness of such confidential care, such practices do create holes in the protections set up in the electronic record.

5.2.7 Parental Notification Versus Consent to Treat

Adolescents can consent to treatment at an age younger than the age of majority in certain clinical contexts (Weddle and Kokotailo 2002). For example, an adolescent at age 12 can, in the states of California or Illinois (as of 2003, English et al. 2003) consent to treatment for mental health services. In North Carolina, the minor can consent at any age. This varying age of consent has little impact on EHR functionality or data storage, but it is often confused with the concept of parental notification just because an adolescent can consent to treat for his or her own care does not make the record of that treatment confidential, or obviate parental notification regulations. Once again, the availability of that information in the medical record may appear threatening to both patient and provider, to the point that the provider may record data in a non-standard place (like a "sticky note" field that is not part of the legal medical record). Once again, full appreciation of the workflow used to produce health data is necessary in order to construct meaningful queries and analysis.

5.2.8 *Mandated Reporting*

Child health workers are obliged under the law of all U.S. states to report suspected child abuse. This obligation overrides HIPAA or other concepts of health information privacy (AAP and C.o.C.A.a.N 2010).

5.3 Health Information Privacy in Adolescent Care

5.3.1 *The Nature of Adolescent Practice*

The care of adolescent patients—as in the care of all patients—must address issues of particular sensitivity: reproductive health, sexually transmitted disease, substance abuse, physical abuse, eating disorders, sexual abuse, mental health, and sexual orientation. The difference with adolescents that affects EHR implementation is that the patients are more sensitive to the effects of confidentiality on their decision to seek care (Ginsburg et al. 1995). Most agree that adolescents need to share in the decision-making about their care, regardless of their inability to legally consent to their treatment. For sensitive topics, adolescents may forego care in order to hide information from parents (Britto et al. 2010; Ford et al. 2001). Since a fundamental goal of health information technology is usually to make information *easier* to share, the adolescent's prerequisite to restrict information dissemination may be impossible to accommodate without non-standard methods of information management. As a result, clinical users may resort to obfuscation of data or the use of paper to manage the information that would otherwise be contained in the EHR. Obviously, this would have major downstream effects on the interpretation of data derived from these environments.

5.3.2 *Adolescent Health, Privacy, and Research*

Adolescents participate as subjects in clinical research, but the process for weighing the risks and benefits of parental consent are complex. Even when parental consent is not a sensitive issue, researchers intending to engage in clinical research involving adolescents should familiarize themselves with local legal issues regarding assent and consent at various ages. The Society for Adolescent Medicine maintains guiding policies for these issues (Santelli et al. 1995). It is a basic principal of adolescent healthcare, endorsed by professional societies, that they be offered confidential care when appropriate (Ford et al. 2004; Gans Epner 1996). Since health information is already considered confidential, a promise of confidential care essentially means

that information will be kept from parents or guardians, a concept that flies in the face of some state law and EHRs designed to provide information to parents or guardians in the form of printed summaries and on-line portals. As of this writing, there are no standards for adolescent privacy policies to govern such patient-accessible information, whether for clinical care or research.

5.4 Health Information Privacy and Mental Health

Mental health information was singled out in the HIPAA Administrative Simplification rules in the sense that "psychotherapy notes" do not have to be disclosed to patients or families as part of the usual release of information. These kinds of notes are usually made to record a therapist's thoughts during a patient's therapy, and, if a patient accessed these notes, they might be damaging to the patient's progress. The regulation specifies that these notes cannot contain "medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date" (HHS 2007).

This minor exception to the idea that a patient or family owns the information in the chart with complete access rights has no direct effects on data analysis. It does, however, impose requirements for more complex access control on developers of EHRs. It also has the potential to confuse clinical users, who are already struggling with how to practice medicine in the era of patients' immediate access to their information. For example, if psychotherapy notes should not be shared, are there not other classes of data in the chart that ought to be afforded this same protection, for the same reasons? HIPAA did not describe other exceptions, but clinicians' desire to document care without disrupting care may create new use cases that make data access policies even more complex than they are now.

5.5 Guardianship Issues (Adoption, Foster Care, Fetal Care)

In pediatrics, as with elder care, the patient is not assumed to be the main decision-maker in health care decisions. For most children, the parents are responsible for the child's care as well as the financial and administrative transactions involved in that care. In some cases, the guardian must be distinguished from the financial guarantor. For children whose parents have had their parental rights severed, or who have otherwise been taken from the care of their parents, other adults are designated guardians. In specific legal proceedings, a court may appoint a guardian ad litem with defined decision-making authority for the child. The only impact these complex arrangements may have on data used for research is that it may affect the consent processes associated with the study.

References

AAP, C.o.C.A.a.N. Policy statement – child abuse, confidentiality, and the health insurance portability and accountability act. Pediatrics. 2010;125(1):197–201.

Britto MT, Tivorsak TL, Slap GB. Adolescents' needs for health care privacy. Pediatrics. 2010;126(6):e1469–76.

Chilton L, et al. American Academy of Pediatrics. Pediatric Practice Action Group and Task Force on Medical Informatics. Privacy protection and health information: patient rights and pediatrician responsibilities. Pediatrics. 1999;104(4 Pt 1):973–7.

English A, et al. State minor consent laws: a summary. Chapel Hill: Center for Adolescent Health & the Law; 2003.

Ferranti JM, et al. The clinical document architecture and the continuity of care record: a critical analysis. J Am Med Inform Assoc. 2006;13(3):245–52.

Ford CA, Best D, Miller WC. The pediatric forum: confidentiality and adolescents' willingness to consent to sexually transmitted disease testing. Arch Pediatr Adolesc Med. 2001;155(9): 1072–3.

Ford C, English A, Sigman G. Confidential health care for adolescents: position paper for the society for adolescent medicine. J Adolesc Health. 2004;35(2):160–7.

Gans Epner JE. Policy compendium on reproductive health issues affecting adolescents. Chicago: American Medical Association; 1996.

Ginsburg KR, et al. Adolescents' perceptions of factors affecting their decisions to seek health care. JAMA. 1995;273(24):1913–18.

HHS. Does the HIPAA Privacy Rule allow parents the right to see their children's medical records? [Web page]. 2002 [2006 Mar 14; 2012 Apr 22]. Available from: http://www.hhs.gov/hipaafaq/personal/227.html

HHS. Title 45 – Public Welfare, Section 164.501 – definitions, in 45 C.F.R. § 164.501; 2007.

HHS. Joint guidance on the application of the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to student health records, E. Health and Human Services, editor, Washington, DC; 2008.

HHS. Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), in Pub. L. No. 111–5 (Feb. 17, 2009), U.S.D.o.H.a.H. Services, editor, Washington, DC; 2009.

How SKH, et al. Public views on U.S. health system organization: a call for new directions. New York: The Commonwealth Fund; 2008.

Kiel JM, Knoblauch LM. HIPAA and FERPA: competing or collaborating? J Allied Health. 2010;39(4):e161–5.

Kroger JS. Coping with CLIA. Clinical Laboratory Improvement Amendments. JAMA. 1994;271(20):1621–2.

National Committee on Vital and Health Statistics. Publication of recommendations relating to HIPAA health data standards–HHS. Notice. Fed Regist. 1997;62(195):52563–5.

Santelli JS, et al. Guidelines for adolescent health research: a position paper of the society for adolescent medicine. J Adolesc Health. 1995;17(5):270–6.

Weddle M, Kokotailo P. Adolescent substance abuse. Confidentiality and consent. Pediatr Clin North Am. 2002;49(2):301–15.