Chapter 2
Protecting Privacy in the Child Health EHR

S. Andrew Spooner

Abstract In the United States and other industrialized countries, laws demand that all individually identifiable health information be secured from unintended disclosure and handled as private, sensitive information. While this protection extends equally to all information in a health record, information that pertains to mental health, reproductive health, physical abuse, and certain other areas with social impact is usually considered even more sensitive than other types of health information. The latter types of information may have special laws or professional standards that apply to how it is handled. All of these privacy and security issues become more complex in situations where minors are involved, because of real or perceived conflicts between the interests of the child and the interests of parents or guardians. In the care of adolescents, these issues become particularly difficult, and may affect how data are recorded or displayed in the EHR system, and the extent to which data may be available for research. Additional areas that present difficult challenges to privacy include fetal care, foster care, and situations where genetic information must be stored and interpreted. 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. In this chapter we will discuss the prevailing regulations in the United States and the European Union that apply to privacy and security, and highlight pediatric aspects of these rules that apply to data.

Keywords Data integrity • Privacy • Security • HIPAA

S.A. Spooner, M.D., M.S., FAAP (✉)
Departments of Pediatrics and Biomedical Informatics, Cincinnati Children's Hospital Medical Center, University of Cincinnati College of Medicine,
3333 Burnet Avenue, MLC-9009, Cincinnati, OH 45229, USA
e-mail: andrew.spooner@cchmc.org

J.J. Hutton (ed.), *Pediatric Biomedical Informatics*, Translational Bioinformatics 10,
DOI 10.1007/978-981-10-1104-7_2

2.1 The Information in an EHR

2.1.1 Basic EHR Data Integrity

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

- Unlike a research record, the EHR tends to be inclusive of all data--not just validated data. For example, a health record may contain two blood pressure recordings at an office visit because the clinician decided to repeat the measurement. One would not expect the original recording to be deleted. In a case where "the" encounter blood pressure needs to be recorded for research, the researcher has the dilemma of what to do with such an inclusive data set.
- Whereas data collection for research typically follows rigid and well-defined data collection processes, this is not so for the clinical health record. The result is that a clinical record is much less structured than a case report form. Automated extraction of data for research is therefore challenging.
- The data in the EHR belong to the patient, and must be provided to the patient or the applicable guardian 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 under HIPAA (OCR 2002) in the United States.
- The EHR plays an important role in legal defense of malpractice claims. Although the medical record is classified as hearsay (Elias 2003), 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.

2.1.2 Data Entry

Clinical care is documented typically by the recording of a large amount of free text and a small amount of discrete data. While EHRs can 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 with associated discrete data elements, but in academic medical centers where 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, that do contain a preponderance of discrete data, but there are some limitations to the uses of these data for research. 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 (CMS 2014; Kroger 1994) by federal law. Under these conditions, one is not free to set up investigational clinical laboratory tests as a part of routine care. Likewise, prescription data must conform to data standards that allow electronic prescribing (Liu et al. 2011), so investigational drugs present a challenge to represent in clinical EHRs. For example, if the investigational medication is not yet on the market, and therefore is not yet assigned a code from the system used to identify retail products, it might be difficult or impossible to encode as discrete data in the EHR. 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 deletion of data is not possible in an EHR, assuming the data were not collected in error. All data are retained, and deleting data—even if it is erroneous—must be done in a way that retains the 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.

2.2 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 (Chung et al. 2006), as well as state laws. Because every episode of pediatric care involves at least two people in a patient role (the patient and the patient's 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. 6, Data Governance and Strategies for Data Integration and Chap. 7, Laboratory Medicine and Biorepositories.

2.2.1 HIPAA

The U.S. Health Insurance Portability and Accountability Act of 1996 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' 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 2013) strengthen HIPAA's privacy and security requirement, and impose stiffer penalties.

2.2.2 HIPAA Business Associate Agreements

Those who work with health data, unless the data are suitably rendered anonymous, are 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. Recent changes in US law regarding business associates (2013) have reinforced the seriousness of the government in its intent to enforce these rules.

2.2.3 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).

2.2.4 FERPA

A law that existed many years before HIPAA was the Family Educational Rights and Privacy Act (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).

2.2.5 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 ROI today.

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 it may have been comforting to assume

that the information is "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.

2.2.6 Clinical Data Sharing vs. 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.

2.2.7 Parental Notification vs. 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 and Kenney 2003; Kerwin et al. 2015)) 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.

2.2.8 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 2010).

2.2.9 The European Data Protection Directive

In the European Union, the right to privacy and its effect on data management is reflected in Directive 95/46/EC, commonly known as the Data Protection Directive (DPD) of 1995 (Barber and Allaert 1997), and the subsequent 2012 proposed reforms of this law (Saracci et al. 2012). The scope of this directive is larger than health care, but does apply to EHR data. The focus of these laws is to ensure protection of inter-country transfer of information as part of clinical care, but any inter-country use of data, including research, would be affected. Of course, within-country handling of data would be governed by laws within that nation. In many European countries (e.g., Denmark, Finland), there are centralized database of health information, but the use of these databases for research is controversial (Lehtonen 2002) and the DPD does not specifically address how data might be used in medical research (Sheikh 2005). Similarly, adolescent privacy is not specifically addressed in the DPD, although it is reasonable to assume that the laws of individual countries would take precedence. As the "right to be forgotten" legislation from the European Union (Jones 2016) indicates, European privacy laws that might apply to medical data may be even more restrictive than in the United States. It is unclear whether this focus in privacy will work for or against an adolescent's interest, since parents' interests and the adolescents' interest can be in conflict.

2.3 Health Information Privacy in Adolescent Care

2.3.1 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 (Gray et al. 2014). 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. 1997; 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. 2004). 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 the establishment of special policies and procedures. 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.

2.3.2 *Data Access Policies in the Adolescent Patient*

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 Health and Medicine maintains guiding policies for these issues (Bayer et al. 2015; Santelli et al. 1995).

Confidential Care It is a basic principle of adolescent healthcare, endorsed by professional societies, that they be offered confidential care when appropriate (ACOG 2014; 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.

2.4 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 2001).

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.

2.5 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. American academy of pediatrics, committee on child abuse and neglect policy statement: child abuse, confidentiality, and the health insurance portability and accountability act. Pediatrics. 2010;125(1):197–201.

ACOG. American college of obstetrics and gynecology, committee opinion no. 599: committee on adoscent health care: adolescent confidentiality and electronic health records. Obstet Gynecol. 2014;123(5):1148–50.

Barber B, Allaert FA. Some systems implications of EU data protection directive. Stud Health Technol Inform. 1997;43 Pt B: 829–833.

Bayer R, Santelli J, Klitzman R. New challenges for electronic health records: confidentiality and access to sensitive health information about parents and adolescents. JAMA. 2015;313(1):29–30.

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

Chilton L, Berger JE, Melinkovich P, Nelson R, Rappo PD, Stoddard J, Swanson J, Vanchiere C, Lustig J, Gotlieb EM, Deutsch L, Gerstle R, Lieberthal A, Shiffman R, SA Spooner Stern M. 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.

Chung K, Chung D, Joo Y. Overview of administrative simplification provisions of HIPAA. J Med Syst. 2006;30(1):51–5.

CMS. Center for Medicare and Medicaid Services, CLIA program and HIPAA privacy rule; patients' access to test reports. Final rule. Fed Regist. 2014;79(25):7289–316.

Elias CE. Federal rules of evidence handbook. Durham: Carolina Academic Press; 2003.

English A, Kenney K. State minor consent laws: a summary. 2nd ed. Chapel Hill: Center for Adolescent Health and the Law; 2003.

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

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, Slap GB, Cnaan A, Forke CM, Balsley CM, Rouselle DM. Adolescents' perceptions of factors affecting their decisions to seek health care. JAMA. 1995;273(24):1913–8.

Ginsburg KR, Menapace AS, Slap GB. Factors affecting the decision to seek health care: the voice of adolescents. Pediatrics. 1997;100(6):922–30.
Gray SH, Pasternak RH, Gooding HC, Woodward K, Hawkins K, Sawyer S, Anoshiravani A. Society for adolescent health and medicine: recommendations for electronic health record use for delivery of adolescent health care. J Adolesc Health. 2014;54(4):487–90.
HHS. Does the HIPAA Privacy Rule allow parents the right to see their children's medical records? 2002;03/14/2006. Retrieved from http://www.hhs.gov/hipaa/for-professionals/faq/227/can-i-access-medical-record-if-i-have-power-of-attorney/.
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. Washington, DC. 2008. Retrieved from http://www2.ed.gov/policy/gen/guid/fpco/doc/ferpa-hippa-guidance.pdf. Accessed 4/02/2012.
HHS (U.S. Department of Health and Human Services). Title 45 – Public Welfare (October 1, 2001). 45 C.F.R. pt. 164.
HHS (U.S. Department of Health and Human Services). Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; other modifications to the HIPAA rules. Fed Regist. 2013;78(17), 5565–702.
How SKH, Shih A, Lau J, Schien C. Public views on U.S. health system organization: a call for new directions, vol. 11. New York: The Commonwealth Fund; 2008.
Jones ML. Ctrl+Z: the right to be forgotten. London: New York University Press; 2016.
Kerwin ME, Kirby KC, Speziali D, Duggan M, Mellitz C, Versek B, McNamara A. What can parents do? A review of state laws regarding decision making for adolescent drug abuse and mental health treatment. J Child Adolesc Subst Abuse. 2015;24(3):166–76.
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.
Lehtonen LA. Government registries containing sensitive health data and the implementation of EU directive on the protection of personal data in Finland. Med Law. 2002;21(3):419–25.
Liu H, Burkhart Q, Bell DS. Evaluation of the NCPDP structured and codified sig format for e-prescriptions. J Am Med Inform Assoc. 2011;18(5):645–51.
OCR (Office of Civil Rights, U.S. Department of Health and Human Services). Standards for privacy of individually identifiable health information.67 Fed.Reg. 53181 (August 14, 2002) (to be codified at 45 CFR pts. 160 & 164).
Santelli JS, Rosenfeld WD, DuRant RH, Dubler N, Morreale M, English A, Rogers AS. Guidelines for adolescent health research: a position paper of the society for adolescent medicine. J Adolesc Health. 1995;17(5):270–6.
Saracci R, Olsen J, Seniori-Costantini A, West R. Epidemiology and the planned new Data Protection Directive of the European Union: a symposium report. Public Health. 2012;126(3):253–5.
Sheikh AA. The Data Protection (Amendment) Act, 2003: the Data Protection Directive and its implications for medical research in Ireland. Eur J Health Law. 2005;12(4):357–72.
Weddle M, Kokotailo P. Adolescent substance abuse. Confidentiality and consent. Pediatr Clin North Am. 2002;49(2):301–15.