American Academy
of Pediatrics

DEDICATED TO THE HEALTH OF ALL CHILDREN™

Electronic Communication of the Health Record and Information With Pediatric Patients and Their Guardians

Emily C. Webber, MD, FAAP, FAMIA,[a] David Brick, MD, FAAP,[b] James P. Scibilia, MD, FAAP,[c] Peter Dehnel, MD, FAAP,[d] COUNCIL ON CLINICAL INFORMATION TECHNOLOGY, COMMITTEE ON MEDICAL LIABILITY AND RISK MANAGEMENT, SECTION ON TELEHEALTH CARE

Communication of health data has evolved rapidly with the widespread adoption of electronic health records (EHRs) and communication technology. What used to be sent to patients via paper mail, fax, or e-mail may now be accessed by patients via their EHRs, and patients may also communicate securely with their medical team via certified technology. Although EHR technologies have great potential, their most effective applications and uses for communication between pediatric and adolescent patients, guardians, and medical teams has not been realized. There are wide variations in available technologies, guiding policies, and practices; some physicians and patients are successful in using certified tools but others are forced to limit their patients' access to e-health data and associated communication altogether. In general, pediatric and adolescent patients are less likely than adult patients to have electronic access and the ability to exchange health data. There are several reasons for these limitations, including inconsistent standards and recommendations regarding the recommended age for independent access, lack of routine EHR support for the ability to filter or proxy such access, and conflicting laws about patients' and physicians' rights to access EHRs and ability to communicate electronically. Effective, safe electronic exchange of health data requires active collaboration between physicians, patients, policy makers, and health information technology vendors. This policy statement addresses current best practices for these stakeholders and delineates the continued gaps and how to address them.

abstract

[a]Department of Pediatrics, School of Medicine, Indiana University and Riley Hospital for Children at Indiana University Health, Indianapolis, Indiana; [b]Department of Pediatrics, School of Medicine, New York University, New York, New York; [c]Heritage Valley Health System, Beaver, Pennsylvania; and [d]Abbott Northwestern Hospital and Children's Hospitals and Clinics of Minnesota, Minneapolis, Minnesota

Drs Webber and Brick participated in the initial concept and design, analysis, drafting, and revision of the manuscript. Drs Webber, Brick, Scibilia, and Dehnel all reviewed and revised the manuscript and approve it as submitted.

This document is copyrighted and is property of the American Academy of Pediatrics and its Board of Directors. All authors have filed conflict of interest statements with the American Academy of Pediatrics. Any conflicts have been resolved through a process approved by the Board of Directors. The American Academy of Pediatrics has neither solicited nor accepted any commercial involvement in the development of the content of this publication.

Policy statements from the American Academy of Pediatrics benefit from expertise and resources of liaisons and internal (AAP) and external reviewers. However, policy statements from the American Academy of Pediatrics may not reflect the views of the liaisons or the organizations or government agencies that they represent.

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

All policy statements from the American Academy of Pediatrics automatically expire 5 years after publication unless reaffirmed, revised, or retired at or before that time.

DOI: https://doi.org/10.1542/peds.2019-1359

DEFINITIONS

In this document, the terms below are used with these definitions:

- Guardian: legal guardians, including parents, who have access to all or part of the child's medical record and/or patient portal.

FROM THE AMERICAN ACADEMY OF PEDIATRICS

- Health care team: includes physicians, nonphysician clinicians (nurses, pharmacists and others), and nonclinician personnel (eg, office managers, billing staff, etc).

BACKGROUND INFORMATION

The workflow, technologies, rules, and regulations regarding electronic communication of health data between health care teams and patients have evolved quickly over the last decade. As electronic health records (EHRs) have made medical data more rapidly accessible to patients and guardians, health care teams have struggled to sustain the traditional model of being the curator and guardian of a patient's health information.[1]

Although technology can facilitate more effective and timely care, it has been challenging to reach a consensus about the ideal uses of technology. Defining the most effective use requires aligning legislative policy, legal requirements, technology functionality, and clinical workflow and impact.[2,3] Although access to health data via electronic means is strongly recommended by professional medical organizations,[4-6] there has not been the accompanying change in legislative policy or practice to support consistent access, privacy, and electronic communication of clinical data in EHRs for patients (particularly for pediatric and adolescent patients). Health care teams, pediatric patients of all ages, and guardians need more guidance to effectively and safely use technology for electronic communication about health record information. In addition, successful adoption of existing guidance and future recommendations requires health care teams, policy makers, and EHR vendors to collaborate and optimize these technologies. This policy statement provides guidance for a broad audience; it includes recommendations for policy makers and EHR vendors on incorporating standards to improve electronic communication of health record information as well as health care teams for best use.

STATEMENT OF THE PROBLEM

Areas that present particular challenges for EHR communication include:

- Variable laws and regulations and rapidly changing non-EHR electronic communication;
- Variable definitions of a health record;
- Variable maturity of pediatric patients and guardianship roles as well as age of the majority;
- Limited pediatric functionality capabilities of EHRs and other health information technology (HIT)[5]; and
- Privacy and confidentiality needs of adolescent patients.

Variable Laws and Regulations and Rapidly Changing Non-EHR Electronic Communication

Most regulations regarding the communication of health record data have been focused on the requirements for "meaningful use," the federal regulations closely associated with use of a certified EHR and the Health Information Technology for Economic and Clinical Health Act in early 2009, which is now part of the Merit-Based Incentive Payment System. The operational requirements include the ability to exchange information with patients using a patient portal.[7] However, in addition to meaningful use, there is a broad range of federal and state rules, laws, statutes, and regulations that reference electronic communication of health record information between patients and guardians and health care teams,[8] particularly for adolescent patients.[9] These regulations can make it challenging to determine what practices are compliant and can result in restrictive policies for institutions and systems.

Although meaningful use regulations have stimulated the implementation of EHRs and patient portals, the regulations do not make recommendations regarding the best use of other modes of electronic communication of health record data, such as text messages and mobile applications, outside of portals attached to EHRs. This policy addresses electronic communication of the health record between health care teams and pediatric patients and their guardians.

Telehealth services are generally included in this non-EHR category. Telehealth has been expanded in definition by the federal government to include "the use of telecommunications and information technology to provide access to health assessment, diagnosis, intervention, consultation, supervision and information across distance."[10] The broad definition expands the notion of the health record to multiple access points and multiple new technologies, all of which require security, confidentiality, and accuracy. A summary of state definitions of telehealth can be found on the Web site of the Center for Connected Health Policy (https://www.cchpca.org/telehealth-policy/current-state-laws-and-reimbursement-policies).

The recommendations in this policy statement pertain to electronic communications not currently included in the telehealth summary, which are addressed in separate AAP policy statements.[11,12] Telehealth pertains to the delivery of health care; this policy speaks to electronic communication of the health record. Health care teams and patients communicating electronically to this point have not had widespread standards with regard to the technology they use.

Variable Definitions of a Health Record

The definition of what constitutes the "legal health record" may be brought into question when responding to requests for information, which is a form of communication. The American Health Information Management Association defines the legal health record as "the documentation of healthcare services provided to an individual during any aspect of healthcare delivery in any type of healthcare organization."[13]

In the United States, EHRs are certified on the basis of requirements for meaningful use. Although widely accepted, meaningful use legislation and regulations are not comprehensive in defining the components of EHRs deemed necessary by clinicians and their patients to promote clinical care. Communication, especially electronic communication by different members of the medical team, is 1 of those necessary features not yet clearly delineated. For example, if a physician, nurse, or other medical team member calls a patient's guardian or patient to share normal laboratory results, there are no widely accepted standards for whether and how the physician and medical team should capture this communication in the EHR. Similarly, if a radiology image is shared with the patient or guardian through the patient portal, there is no clear guidance as to whether the text of the report should be recorded in a note or if the image itself should be retained (because it may be stored in another system).

Variable Maturity and Guardianship of Pediatric Patients

As they mature, adolescents develop maturity and an increasing capacity to manage their own communications and health data over time. Accordingly, there need to be different types of communication of health record information supported by different types of technology for different levels of autonomy and maturity.

Sharing health information is part of teaching and empowering children and their guardians to assume responsibility for managing their illnesses and promoting their own health and occurs as a result of discussion between the patient, guardian, and physician. Children develop the ability to process information as they mature, and although general guidelines exist to predict readiness,[14] there are necessary exceptions and adaptions for individuals. This need to assess and support variable levels of autonomy existed before EHRs and electronic communication; however, EHR use has highlighted both the wide variation in patient capacity and readiness and the lack of granular functionality in EHRs to support best practices.

Pediatric patients may have individuals who serve as guardians who are not their parents. The rights to receive communications about care may also be different from the rights to authorize care.[15] The ability of technology to support different communications to multiple guardians of pediatric patients and the associated workflows involved in their validation are often limited.

Limited Ability of EHRs and Other HIT To Segment Information Access

Physicians and other clinical team members in clinical practice are able to both identify and control how to manage disclosure of information usually deemed "sensitive" (including but not limited to sexual health, mental health, and social history). This clinical practice pertains to patients of all ages but handling of sensitive information is particularly challenging for pediatric and adolescent patients and their guardians when sharing clinical information electronically.

There is no widely accepted or easily implemented set of standards defining exactly what data (documentation, clinical results, or other data) should be categorized consistently as sensitive

information in the medical record.[16] For example, medications for sexually transmitted diseases or mental health may be appropriate for 1 patient and his or her guardian to share, but for another patient, that information would need to be segmented (filtered) to maintain privacy.

EHRs do not yet provide widely available features to allow for granular filtering by the physician and clinical team or the patient to preserve confidentiality in these nuanced and complex situations. There is also not a consistent, widely available way for pediatric and adolescent patients to control the content and method by which they share their EHR data.

These limitations have left many physicians and clinical team members with a "first, do no harm" approach to providing access to EHRs using the provided portal and access tools, leading to either extensive customization of the EHRs when being used for pediatric populations or exclusion of pediatric and adolescent patients from electronic access to their records.[17] Many EHRs have an all-or-nothing privacy and confidentiality approach that is typically used by EHRs for communicating health data such as demographics, problems, medications, and other data (eg, laboratory results, radiology results, and progress notes) and do not support the granular filtering needed to provide the types of protection needed by patients; this is especially true in the special case of pediatric records.[18]

Privacy and Confidentiality Needs of Adolescent Patients

Adolescent privacy and/or confidentiality is a special case of the limited segmenting of functionality capabilities in EHRs that is compounded by variations in state laws regarding adolescent health records. Health care teams may experience difficulty complying with state requirements and professional recommendations for adolescent

privacy because of federal rules for disclosure. For example, 1 portion of care may be protected by law as confidential for which the patient consents independently, but other aspects of care may not be protected, turning a simple routine visit into a potential series of confidentiality challenges. As a result, meeting the requirements of broad federal mandates regarding the sharing of health data with patients is difficult to achieve. This challenge results in fewer pediatric patients enrolling in portals, thereby depriving of them of access to their own records. Adolescent access to their EHRs has been recommended by both the AAP and the Society of Adolescent Health and Medicine.[6,10]

All states have laws allowing minors to access medical care for certain types of medical conditions without consent of a guardian and with some expectation of privacy, although laws vary significantly by state.[19] EHR system access and data sharing can be multidirectional and used in a variety of ways, making it more challenging for the clinical teams as well as EHR vendors to maintain the privacy necessary to support confidentiality. Failure to maintain the confidentiality of this information can lead to fines or adverse licensure action against individual physician licenses. This may also result in civil litigation against health care teams and systems.[20–22]

As previously mentioned, managing and protecting sensitive clinical data is 1 challenge. Disclosure of other data, such as private health information through claims data and details of billing systems, can be automated in some EHRs and sent to guardians, which is another way in which confidentiality may be compromised. For example, testing for *Chlamydia* or other sexually transmitted infections may be noted on an itemized explanation of benefits. Sustaining an adolescent's privacy in this situation places additional burdens on the health care team.

The AAP policy statement "Standards for Health Information Technology to Ensure Adolescent Privacy"[6] contains recommended standards for EHR vendors, including the ability to filter data as previously mentioned, but most EHRs do not support these recommendations in a manner that is easy to adapt.[18] The Guttmacher Institute summarizes state laws aimed at remedying this problem in its report "Protecting confidentiality for individuals insured as dependents."[23] The problem is compounded when health record information is sent from EHRs to health information exchanges, as mandated by federal law, but a certified EHR does not routinely segment (ie, allow for filtering) confidential data to support adolescent privacy without completely blocking access to the entire record. This challenge results in fewer pediatric patients enrolling in portals, thereby depriving of them of the access recommended by multiple medical societies.[17]

CONCLUSIONS

It is important for physician-patient relationships to have clear expectations and safeguards for patients, guardians, and health care teams in electronic communication of health record information. Much of the published literature regarding this sharing pertains to adult patients leveraging patient portals, so there is little specification as to how shared access (eg, a "proxy" or "surrogate" relationship) of a guardian to a child's EHR is most effectively and appropriately established and governed unless using custom tools. The sharing of the clinical data in the EHR depends on the complex relationships that are rife with the variations previously detailed.

These factors have led to several examples of extensive customization of vendor EHRs and "homegrown" solutions that are difficult to scale outside of the hospital or system in which they were developed. Even with customization, EHRs may not comport with relevant federal and state laws, statutes, and regulations governing confidentiality. For example, the HIPAA Privacy Rule allows covered health care health care teams to communicate electronically, such as through e-mail, with their patients provided they apply reasonable safeguards when doing so; however, institutional policy makers and health care teams are left to determine those safeguards. Most health care teams are currently trying to adapt patient portals and other technologies designed for independent adults to children with diverse living situations, developing and changing levels of autonomy, and complex confidentiality needs.

The recommendations that follow are intended to address the challenges and pitfalls of using EHR and non-EHR electronic communication with patients and guardians regarding the child's or adolescent's health record.

RECOMMENDATIONS

These recommendations are suited for health care teams and health systems using electronic communication with their patients and guardians regarding a child's health record. Collaboration between health care teams, policy makers, and EHR and/or HIT developers is critical to implementation of the following recommendations.

Recommendations for Physicians and Health Care Teams

1. Health care teams should use secure platforms that protect communications with patients and guardians. Electronic communication of health record information should be incorporated directly into the standard EHR, making use of secured and certified technology

such as embedded secure messaging and portals to share clinical information and capture communication whenever appropriate.

2. Health care teams should provide a clear understanding of the limitations of electronic communication of health record information to guardians. Electronic communication should not be used in isolation to communicate or provide medical care unless there is confirmation of receipt and comprehension of the information (ie, "closed-loop communication"). For example, discussing changes in therapy or providing test results or a diagnosis may be more efficiently and safely accomplished in face-to-face or verbal communication because those methods provide a way to ask clarifying questions in real time. Electronic communication can provide appropriate support for many patients to seek guidance, ask questions, and provide feedback but may be asynchronous or more limited than face-to-face communication. Although electronic communication allows patients to receive and access their information differently, health care teams should continue clinical practices that best support patient care, including in-person counseling and assessments.

3. Health care teams should be aware of the risks of unsecured communication and take steps to minimize the risk to patients. EHR technology certified by the Office of the National Coordinator adheres to a consistent measure of security. EHR technology may be used for electronic communication as long as:

○ Adequate technology exists to allow adolescent patients privacy around protected laboratory results, diagnosis,

medications, and other clinical data; and

○ There is adequate understanding for use of the electronic communication between the patient, the guardian, the physician, and the health care team.

4. Health care teams and patients using electronic communication that is not HIPAA compliant should be aware that this technology may not be secure. All parties should be aware of these security risks and use the appropriate technology to support their communication. Technology that is not HIPAA compliant may not be secure and exposes the physician and patient to the risk of breach of protected health information.

Recommendations for Institutional Policy Makers and Health Care Organizations

5. Institutional policies and practices for electronic communications should support clear expectations between medical teams and patients. Because EHRs and other technology can make health data directly available and accessible to the patient and/or guardian without the physician or medical team as the intermediary, clear expectations about what information should be shared with which users are needed to provide context and support for patients. Policies that support the development of skills in counseling and use for health care teams and staff are needed. As new technology tools become available, communication between patients and health care teams will evolve and, therefore, policies must evolve with them.

6. Institutional policy should include a communication agreement between health care teams and patients and/or guardians to support safe and effective

electronic communication of health record information. This agreement could reflect but is not limited to the following aspects:

○ The consent of the patient and/or guardian to receive electronic communication and, when mandated by law, the guardian's consent for the minor patient to have electronic communication between physician and patient.

○ Respect for patients' privacy as well as their right to access their health information under the law while acknowledging the unique and changing needs of patients as they mature.

○ Expectations for both parties regarding the content of electronic communication, including appropriate requests and the timeliness of responses.

○ Circumstances appropriate for the use of unencrypted electronic communications such as unencrypted e-mails. For example, a reminder to get an influenza vaccination should not contain protected health information and does not necessarily require a private, secure electronic means of delivery. However, conveying specific results, such as laboratory or radiology tests, might require encryption.

7. Professional organizations and health institutions should have systems to ensure health care teams are aware of state and federal requirements and to assist them in complying with standards, rules, and regulations. These actions may include the following:

○ Establishing systems that promote patient and guardian awareness of the risks, benefits, and limitations of electronic communications.

○ Aligning consent for electronic communication with the general consent for care when possible.

○ Defining standards for when a patient may confidentially and reliably communicate electronically directly with his or her physician. This standard should be applicable to any patient for whom guardianship is a consideration, regardless of the patient's age. In the absence of specific regulations, it is reasonable for the clinician, using their clinical assessment and judgement in collaboration with the patient and family, to determine when a patient has the ability, cognitive skills, and maturity needed to safely and effectively use independent electronic communication so that the clinician may provide appropriate expectations and support.

Recommendations for Federal Policy Makers and Health Information Technology Developers

8. Standard EHR functionality should include the capacity for health care teams and patients to segment or filter clinical data that can compromise confidentiality. Although this filtering ability contains risks because it allows for an incomplete record to be shared or viewed, it is necessary to uphold the dual requirements of patient privacy as well as patient access when access is shared. This filtering may be needed for any patients who are accessing or sharing their electronic communication but is especially needed for pediatric and adolescent patients establishing independent communication and decision-making with their medical teams.

9. EHR vendors should enable safeguards for medical teams to restrict electronic communication in cases of acute patient safety risk (eg, when guardianship of a patient changes because of risk to patient safety such as in cases of child abuse and neglect).

LEAD AUTHORS

Emily C. Webber, MD, FAAP
David Brick, MD, FAAP
James P. Scibilia, MD, FAAP
Peter Dehnel, MD, FAAP

COUNCIL ON CLINICAL INFORMATION TECHNOLOGY EXECUTIVE COMMITTEE, 2016–2017

Stuart T. Weinberg, MD, FAAP
Emily C. Webber, MD, FAAP
Gregg M. Alexander, DO
Eric L. Beyer, MD, FAAP
Alexander M. Hamling, MD, FAAP
Eric S. Kirkendall, MD, MBI, FAAP
Donald E. Lighter, MD, MBA, FAAP
Ann M. Mann, MD, FAAP
Stephen J. Morgan, MD, FAAP
Eric Shelov, MD, FAAP
Jeffrey A. Wright, MD, FAAP

LIAISONS

Dale C. Alverson, MD, FAAP (Section on Telehealth Care)
Francis D. Chan, MD, FAAP (Section on Advances in Therapeutics and Technology)
Melissa S. Van Cain, MD (Section on Pediatric Trainees)

STAFF

Lisa A. Krams, MAHS

COMMITTEE ON MEDICAL LIABILITY AND RISK MANAGEMENT, 2016–2017

Robin L. Altman, MD, FAAP
Steven A. Bondi, JD, MD, FAAP
Jonathan M. Fanaroff, MD, JD, FCLM, FAAP
Sandeep K. Narang, MD, JD, FAAP
Richard L. Oken, MD, FAAP
John W. Rusher, MD, JD, FAAP
Karen A. Santucci, MD, FAAP
James P. Scibilia, MD, FAAP
Susan M. Scott, MD, JD, FAAP

STAFF

Julie Kersten Ake

SECTION ON TELEHEALTH CARE EXECUTIVE COMMITTEE, 2017–2018

Joshua J. Alexander, MD, FAAP (chairperson)
Chelsea E.F. Bodnar, MD, FAAP
Alison Curfman, MD, FAAP
Neil E. Herendeen, MD, MS, FAAP
Joseph A. Kahn, MD, FAAP
Steven D. McSwain, MD, FAAP

LIAISON

Kelli M. Garber, PPCNP-BC

STAFF

Trisha M. Calabrese, MPH

ABBREVIATIONS

EHR: e-health record
HIPAA: Health Insurance Portability and Accountability Act
HIT: health information technology

FROM THE AMERICAN ACADEMY OF PEDIATRICS

REFERENCES

1. Roscam Abbing HD. Medical confidentiality and electronic patient files. *Med Law*. 2000;19(1):107–112

2. Kruse CS, Bolton K, Freriks G. The effect of patient portals on quality outcomes and its implications to meaningful use: a systematic review. *J Med Internet Res*. 2015;17(2):e44

3. de Lusignan S, Mold F, Sheikh A, et al. Patients' online access to their electronic health records and linked online services: a systematic interpretative review. *BMJ Open*. 2014; 4(9):e006021

4. Thompson LA, Martinko T, Budd P, Mercado R, Schentrup AM. Meaningful use of a confidential adolescent patient portal. *J Adolesc Health*. 2016;58(2): 134–140

5. Lehmann CU; Council on Clinical Information Technology. Pediatric aspects of inpatient health information technology systems. *Pediatrics*. 2015; 135(3). Available at: www.pediatrics.org/cgi/content/full/135/3/e756

6. Committee on Adolescence; Council on Clinical and Information Technology, Blythe MJ, Del Beccaro MA. Standards for health information technology to ensure adolescent privacy. *Pediatrics*. 2012;130(5):987–990

7. HealthIT.gov. Meaningful use. Available at: https://www.healthit.gov/topic/meaningful-use-and-macra/meaningful-use. Accessed April 18, 2018

8. Anoshiravani A, Gaskin GL, Groshek MR, Kuelbs C, Longhurst CA. Special requirements for electronic medical records in adolescent medicine. *J Adolesc Health*. 2012;51(5):409–414

9. Society for Adolescent Health and Medicine, Gray SH, Pasternak RH, Gooding HC, et al. Recommendations for electronic health record use for delivery of adolescent health care. *J Adolesc Health*. 2014;54(4):487–490

10. Center for Connected Health Policy. About telehealth. Available at: https://www.cchpca.org/about/about-telehealth. Accessed April 18, 2018

11. Burke BL Jr, Hall RW; Section on Telehealth Care. Telemedicine: pediatric applications. *Pediatrics*. 2015;136(1). Available at: www.pediatrics.org/cgi/content/full/136/1/e293

12. Committee on Pediatric Workforce, Marcin JP, Rimsza ME, Moskowitz WB. The use of telemedicine to address access and physician workforce shortages. *Pediatrics*. 2015;136(1): 202–209

13. American Health Information Management Association. Fundamentals of the legal health record and designated record set. Available at: http://library.ahima.org/doc?oid=104008#.WLSV_G8rLX4. Accessed April 18, 2018

14. Weithorn LA, Campbell SB. The competency of children and adolescents to make informed treatment decisions. *Child Dev*. 1982; 53(6):1589–1598

15. Cohen GJ, Weitzman CC; Committee on Psychosocial Aspects of Child and Family Health; Section on Developmental and Behavioral Pediatrics. Helping children and families deal with divorce and separation. *Pediatrics*. 2016;138(6): e20163020

16. Bourgeois FC, Nigrin DJ, Harper MB. Preserving patient privacy and confidentiality in the era of personal health records. *Pediatrics*. 2015;135(5). Available at: www.pediatrics.org/cgi/content/full/135/5/e1125

17. Temple MW, Sisk B, Krams LA, Schneider JH, Kirkendall ES, Lehmann CU. Trends in use of electronic health records in pediatric office settings. *J Pediatr*. 2019; 206:134-171.e2

18. Sharko M, Wilcox L, Hong MK, Ancker JS. Variability in adolescent portal privacy features: how the unique privacy needs of the adolescent patient create a complex decision-making process. *J Am Med Inform Assoc*. 2018;25(8): 1008–1017

19. Guttmacher Institute. An overview of consent to reproductive health services by young people. Available at: https://www.guttmacher.org/state-policy/explore/overview-minors-consent-law. Accessed April 18, 2018

20. US Department of Health & Human Services. Health Insurance Portability and Accountability Act Enforcement Rule, 45 CFR §160(c–e) (2013)

21. *Byrne v Avery Center for Obstetrics and Gynecology*, No. 18904, 2014 WL 5507439 (Conn 2014)

22. *R.K. v St. Mary's Medical Center*, 735 S.E.2d 715 (WVa 2012)

23. Guttmacher Institute. Protecting confidentiality for individuals insured as dependents. Available at: https://www.guttmacher.org/print/state-policy/explore/protecting-confidentiality-individuals-insured-dependents. Accessed April 18, 2018

Updated Information & Services	including high resolution figures, can be found at: http://pediatrics.aappublications.org/content/144/1/e20191359
References	This article cites 15 articles, 7 of which you can access for free at: http://pediatrics.aappublications.org/content/144/1/e20191359#BIBL
Subspecialty Collections	This article, along with others on similar topics, appears in the following collection(s): **Current Policy** http://www.aappublications.org/cgi/collection/current_policy **Committee on Medical Liability and Risk Management** http://www.aappublications.org/cgi/collection/committee_on_medical_liability_and_risk_management **Council on Clinical Information Technology** http://www.aappublications.org/cgi/collection/council_on_clinical_information_technology **Section on Telehealth Care** http://www.aappublications.org/cgi/collection/section_on_telephone_care **Health Information Technology** http://www.aappublications.org/cgi/collection/health_information_technology_sub **Electronic Health Records** http://www.aappublications.org/cgi/collection/electronic_health_records_sub
Permissions & Licensing	Information about reproducing this article in parts (figures, tables) or in its entirety can be found online at: http://www.aappublications.org/site/misc/Permissions.xhtml
Reprints	Information about ordering reprints can be found online: http://www.aappublications.org/site/misc/reprints.xhtml

American Academy of Pediatrics

DEDICATED TO THE HEALTH OF ALL CHILDREN®

PEDIATRICS®

Electronic Communication of the Health Record and Information With Pediatric Patients and Their Guardians

Emily C. Webber, David Brick, James P. Scibilia, Peter Dehnel, COUNCIL ON CLINICAL INFORMATION TECHNOLOGY, COMMITTEE ON MEDICAL LIABILITY AND RISK MANAGEMENT and SECTION ON TELEHEALTH CARE

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/144/1/e20191359

American Academy of Pediatrics

DEDICATED TO THE HEALTH OF ALL CHILDREN®