Best Practices for Implementing a Patient Portal for Teens Receiving Confidential Services

Introduction

Patient portals provide easy access to electronic health information for patients and families. They have become part of virtually all healthcare practices thanks to increased use of electronic health records (EHRs), lab and scheduling platforms, and medication management.

Despite the almost ubiquitous use of portals among medical practices, challenges remain related to access for confidential visits for minor patients receiving confidential services, including sexual and reproductive health services, behavioral health services, and substance abuse treatment.

This guide provides an overview of the key considerations for providing portal access to teens, guiding questions to help set up a confidential teen health record, marketing strategies to engage eligible patients, and resources from leaders in pediatric and adolescent medical information technology and health privacy.

Contents

- P.2. Challenges
- P.2. State Rules and Regulations
- P.3. ONC Final Rule and Information Blocking
- P.5. Assembling Your Implementation Team
- P.6 Guiding Questions for Building a Teen-friendly Portal
- P.8. Marketing Strategies
- P.9. Additional Resources

Challenges

Providing teenage patients access to their electronic health records presents several challenges.

- Legal and ethical considerations regarding privacy and consent, as minors may not have the legal authority to access their own records without parental consent
- Ensuring the information within the records is age-appropriate and understandable, as medical terminology may be unfamiliar to teenagers
- Concerns about sensitive information disclosure and potential psychological impact
- Maintaining security measures to safeguard record confidentiality, especially considering adolescents' vulnerability to identity theft and cyber threats.
- Controlling the flow of information when using a health information exchange, such as an automated immunization registry

State Rules and Regulations

Most likely, your practice has already assessed the legal landscape around instituting proper patient care protocols and workflows for patient access to sensitive services. To protect patient rights to privacy and confidentiality, the configuration settings for patient portal accounts should also reflect the your state's laws governing privacy and confidentiality. Patient age of consent for contraceptive services, sexually transmitted infection services, prenatal care, and abortion services varies by state. For contraceptive services, the Supreme Court's decision in the 1977 case, Carey v. Population Services International, established that minors have a constitutional right to access contraceptives on the same terms as adults.

In many states, minors ages 12 to 17 have the right to seek sexual and reproductive health services without parental consent. For some states, however, only certain categories of minors can consent to these services. These groups might include those of a certain age or developmental level, those who are married or pregnant, or those to whom there is a health hazard. Additionally, some states allow clinicians to inform the minor's parents of services provided, even when parental consent is not required.

In addition to laws governing access to confidential services, several states go a step further to protect communications from insurers for dependants receiving services confidentially. Be sure to stay up to date on the laws affecting your state: they are subject to change.

ONC Final Rule, Information Blocking, and Patient Privacy

In March 2020, the Office of the National Coordinator for Health Information Technology (ONC) issued a regulatory framework for the secure and interoperable exchange of electronic health information (EHI) in the U.S. This framework is called the 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program Final Rule. The overall aim of the Cures Act final rule is to promote greater transparency, interoperability, and patient access to EHI, ultimately improving the quality, safety, and efficiency of healthcare delivery.

The four key provisions of the Final Rule are: (1) information blocking prohibition, (2) interoperability standards, (3) certification requirements, and (4) patient access to EHI. The Information Blocking Prohibition bans practices that interfere with the exchange, access, and use of electronic health information. Practices by health IT developers, health information exchanges, health networks, and healthcare providers can all be subject to this provision.

The information blocking provision is intended to promote interoperability and increase patient electronic access to their health information. By complying, providers can enhance coordination of care, improve patient outcomes, and avoid potentially hefty penalties associated with non-compliance. However, potential risks to confidentiality for minor patients receiving sensitive services remain.

The HHS Office of the Inspector General (OIG) investigates complaints of information blocking, which can be reported anonymously through ONC's online information blocking portal or through the OIG Hotline. Health IT (HIT) developers, vendors of certified HIT, and health information exchanges or networks found to have committed information blocking are subject to a penalty up to $1 million. HHS has also published a separate rule establishing disincentives for health care providers, which affect payments for participation in interoperability programs or the Medicare Shared Savings Program.

ONC has identified eight exceptions to Information Blocking, divided into two categories. The two categories are 1) exceptions that involve not fulfilling requests to access, exchange, or use EHI, and 2) exceptions that involve procedures for fulfilling requests to access, exchange, or use EHI. Three of the exceptions in the first category are particularly relevant to health care providers with teenage patients. The preventing harm, privacy, and infeasibility exceptions are applicable in instances where there is a legitimate concern regarding a legal guardian accessing a minor patient's confidential EHI:

- **Preventing Harm Exception.** The exception for potential harm allows healthcare providers or IT developers to withhold access to EHI if disclosing it is reasonably determined to cause harm to a patient or another person.

- **Example Scenario:** A 14 year-old patient seeks contraceptive services from a healthcare provider without wanting their parents to know, due to fear of physical or emotional abuse. The provider documents the visit in the patient's EHR. Under state laws, the teen may have the right to confidential care in relation to reproductive health services.

  If the teen's parents request access to the full medical record, the healthcare provider may invoke the preventing harm exception to withhold the portion of the EHI that relates to the contraceptive services. The provider reasonably determines that disclosing this information to the parents could lead to significant emotional or physical harm to the patient, based on the patient's concerns and the provider's understanding of the family dynamics.

  In this situation, the provider can still give the parents access to other parts of the medical record while protecting the sensitive information. The individualized determination must be made following appropriate professional judgment and applicable laws that protect the patient's confidentiality.

- **Privacy Exception.** The privacy exception to the information blocking rule allows healthcare providers to withhold access to EHI when doing so is necessary to comply with state laws that protect the confidentiality of minors.

  - **Example Scenario:** A 17 year-old patient visits a healthcare provider for contraceptive services, such as birth control counseling or a prescription for contraceptives. Under state law, minors have the legal right to obtain certain reproductive health services confidentially, without parental consent or notification.

    The patient's parent later requests access to the teen's full medical record through the provider's patient portal. However, since state privacy laws protect the confidentiality of the teen's contraceptive services, the healthcare provider can invoke the privacy exception. The provider is required by law to maintain the confidentiality of the information related to reproductive health services and, therefore, withholds the specific portion of the EHI related to the contraceptive services from the parent.

    In this case, the provider is acting in compliance with privacy laws, which is a valid use of the information blocking exception. Other parts of the medical record that are not protected by these laws can still be made accessible to the parent.

- **Infeasibility Exception.** The infeasibility exception allows healthcare providers or health IT developers to decline sharing EHI if doing so is not technically or legally feasible. This exception applies when, despite reasonable efforts, a practice cannot effectively segment requested EHI from other confidential EHI. This could be due to a practical limitation of the EHR system, such as a lack of specific proxy settings for the portal.

    - **Example Scenario:** A 16-year-old patient receives contraceptive services from a healthcare provider, and the EHI related to this visit is recorded in the EHR system. The patient has a legal right to confidentiality under state law regarding reproductive health services, but the EHR system is not equipped with the capability to separate or segment sensitive information like contraceptive services from the rest of the patient's record.

      Later, the patient's parent requests access to the patient's full medical record through the portal. The healthcare provider attempts to fulfill the request but discovers that the EHR system cannot redact or withhold the specific section of the record related to the contraceptive services without also blocking access to unrelated parts of the record. Implementing a new system to segment this sensitive information is not immediately feasible due to technical limitations or the cost and time required to upgrade the system.

      In this case, the healthcare provider may invoke the infeasibility exception, explaining that it is not technically feasible at the moment to provide the requested information in a manner that complies with the patient's privacy rights. The provider may also work on implementing a solution for future access requests, but in the meantime, withholding the information is considered compliant under the infeasibility exception. The provider must notify the requester in writing within 10 days of the request with a reason as to why the request cannot be fulfilled.

Assembling Your Implementation Team

When putting together a team to provide portal access to teens, each staff role should be represented to ensure an informed planning process. Keep in mind the multiple points of contact with patients. Below are staff positions recommended for inclusion along with additional information about the perspective they may offer.

- Administrative
    - A successful project will require buy-in and support from administrative staff
    - Management is key in strategizing, securing the necessary resources to carry out the project, and communicating to all staff about the overall project goal(s) and timeline

- Clinicians
  - Clinical staff provide important insight into how visit information is documented
  - Go a step further than clinician interviews, and shadow a few different clinicians during visits with teens to identify any workarounds they may have in place for documenting confidential services
- Support Staff
  - Supportive staff positions such as medical assistants and health educators can also inform the team about how the system is currently being used and help identify opportunities for improvement
- Schedulers
  - Schedulers and front office staff are often the first point of contact with patients
  - Work closely with your scheduling team to understand the way patient needs are identified and visit types are assigned
- IT – Data Analyst, EHR Vendor
  - IT staff are familiar with the front-end user interface where clinical staff are storing information, as well as how that information is stored and secured on the back end
  - When working out new documentation strategies and workflows, team members from IT will be able to provide important information about what's feasible
  - The vendor for your EHR system can also inform workflow changes and provide information on useful features that are newly available (e.g., additional proxy settings to control access on a granular level)

Guiding Questions for Building a Teen-Friendly Portal

- **How can the patient enrollment process ensure teen privacy and confidentiality?**

Be transparent with patients and caregivers about patient rights and the age of consent for confidential services. Post information about patient rights in waiting areas and on your website. Provide schedulers with scripts to remind caregivers that visits will include time alone for the patient and staff at age of consent.

Train staff to reiterate patient rights during visits and ask patients to confirm their personal and private email address for portal registration. Require teen permission to provide proxy access to confidential information, and be clear about what information is included. (Proxy access is when patient portal access is granted to a legal parent or

guardian of a teen patient. Depending on the platform and settings, adults with proxy access may view some or all of a teenage patient's portal.)

Automatically remove parental proxy access at age of consent and require a new sign up with appropriate permissions.

- **What types of data need to be protected?**

  The following data should be protected:

  - Visit history
  - Clinical notes
  - Lab tests and results
  - Immunizations

  Bring together your clinical and IT staff to discuss the types of protected information currently being collected. Clinicians should note the various locations where protected information is entered. IT staff can then identify available options for restricting that information in the patient portal.

  Include your EHR vendor in these meetings so they can understand how the system is being used. They will also be able to inform your team of any new features available for controlling access to information through portal settings.

- **If your EHR allows encounter information, medications, and/or lab results to be marked "confidential", what system will you establish to protect patient privacy in the portal?**

  Depending on your EHR's available settings, the best way to limit access to confidential information is to ensure it is completely unavailable on the portal for patients between the ages of 12 and 17. Or, if your clinic offers visits categorized as pregnancy test or STI screening, you might standardize these visits to always be marked confidential for teen patients.

- **How will confidential records be handled in the portal?**

  Methods for controlling the availability of information in the patient portal will vary by EHR vendor. The level of granularity provided in the system settings will determine the best way to operationalize through your workflows.

  - How will you ensure consistency?
    - Policies and procedures to establish roles, responsibilities, and documentation requirements for confidential services
    - Conduct chart reviews for accountability

- Who will be responsible for identifying affected records?
  - Schedulers- the first point of contact can identify records through by selecting the appropriate visit type
  - Not all SRH needs are disclosed at the time of scheduling; the MA or nurse may identify need for confidential services during intake
  - Patients may disclose a need for services during the visit, such as when the parent/guardian leaves the room
- Can your system be programmed to flag confidential records automatically?
  - Automated settings can reduce the burden on staff
  - Ideally, your EHR system would automatically identify confidential services for minors based on the use of certain visit types or counseling, procedure and diagnosis codes. Portal settings should include an option to restrict visits or particular elements of a visit record with the appropriate criteria for age and services provided.
  - Another option would be for the system to support identification of visits with confidential services with the use of a confidential checkbox for staff to select

- **Will you post lab results to the portal?**
  - Lab result information can be difficult to interpret. Determine which lab results will automatically be posted in the portal and whether abnormal results will be treated differently.
  - Also consider whether there are any particular test types for which results will only be made available by request from the patient, or any that will never be published to the portal under any circumstances

Marketing Strategies

Drive patient engagement with portals through the use of conversation starters strategically placed around your health center. Use pins or t-shirts worn by staff that read, “Ask me about our portal,” or reminders for staff to inform patients about portal features like scheduling, provider messaging, and viewing lab results.

Increase patient awareness with signage such as posters in the waiting room or billboards in the community with information about patient rights and the options for accessing care. Descriptions of portal features should be widely available and easily accessible, and should include information about security, ease of use, and integration (i.e., lab interfaces).

In addition to physical signage, share portal information in various high visibility areas for patients, such as website banners/pages, social media posts, and community events.

Additional Resources

- An Overview of Consent to Reproductive Health Services by Young People- https://www.guttmacher.org/state-policy/explore/overview-minors-consent-law
- 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program- https://www.federalregister.gov/documents/2020/05/01/2020-07419/21st-century-cures-act-interoperability-information-blocking-and-the-onc-health-it-certification#h-141
- ONC Information Blocking information page- https://www.healthit.gov/topic/information-blocking
- Information Blocking Exceptions- https://www.healthit.gov/sites/default/files/2022-07/InformationBlockingExceptions.pdf
- HHS Finalizes Rule Establishing Disincentives for Healthcare Providers That Have Committed Information Blocking- https://www.hhs.gov/about/news/2024/06/24/hhs-finalizes-rule-establishing-disincentives-health-care-providers-that-have-committed-information-blocking.html
- The 21st Century Cures Act and Multiuser Electronic Health Record Access: Potential Pitfalls of Information Release- https://www.jmir.org/2022/2/e34085
- North American Society for Pediatric and Adolescent Gynecology (NASPAG) and the Society for Adolescent Health and Medicine (SAHM) Position Statement: The 21st Centry Cures Act & Adolescent Confidentiality- https://www.naspag.org/naspag-sahm-position-statement-the-21st-century-cures-act-adolescent-confidentiality
- Teenager, Parent, and Clinician Perspectives on the Electronic Health Record- https://publications.aap.org/pediatrics/article/145/3/e20190193/36800/Teenager-Parent-and-Clinician-Perspectives-on-the?autologincheck=redirected