Healthcare
INBRIEF®

A Risk Management Bulletin for Allied Healthcare Facilities | 2025 Issue 1

Patient/Client Portals: Maximizing Benefits, Minimizing Risks

The electronic tools known as patient/client portals have become an important element of the healthcare delivery system over the last several years. Offering online, round-the-clock access to protected health information (PHI), portals can potentially strengthen the connection between patients/clients and providers, enhance treatment compliance and continuity, and reduce the likelihood of miscommunication and life-threatening mistakes.

There are two main varieties of portals: standalone and integrated. Standalone portals are typically limited to conveying provider visit summaries, allergy and immunization status, medication lists, and the results of diagnostic and laboratory testing. By contrast, integrated portals provide the same functions as standalone portals, but also are designed to interface with electronic healthcare records (EHRs), thus permitting secure email communication between patients/clients and providers, as well as a broader range of functions. (See the graphic to the right for a more comprehensive list of portal functions.)

By enhancing access to health-related data, portals can help patients/clients become more informed about and actively involved in their own care. However, healthcare organizations and providers should be cognizant of evolving liability exposures and incorporate appropriate measures to guard against communication breakdowns, privacy breaches and other potential mishaps. This issue of *AlertBulletin*® highlights the many benefits and efficiencies of portal use, notes common risks, and recommends practical strategies to protect patient/client confidentiality and ensure that portals are used safely, properly and efficiently.

Portal Functions

Standalone Portals

Facilitate patient/client viewing of select PHI, such as test results, visit notes, active medication lists and allergies.

Offer timely access to diagnostic findings.

Issue automatic reminders concerning needed screenings, immunizations and other services.

Deliver downloadable videos and information sheets, as well as other targeted educational materials.

Integrated Portals

Permit secure messaging between patients/clients and providers regarding health status, medical care and diagnostic findings.

Schedule appointments and maintain a record of past encounters and communications.

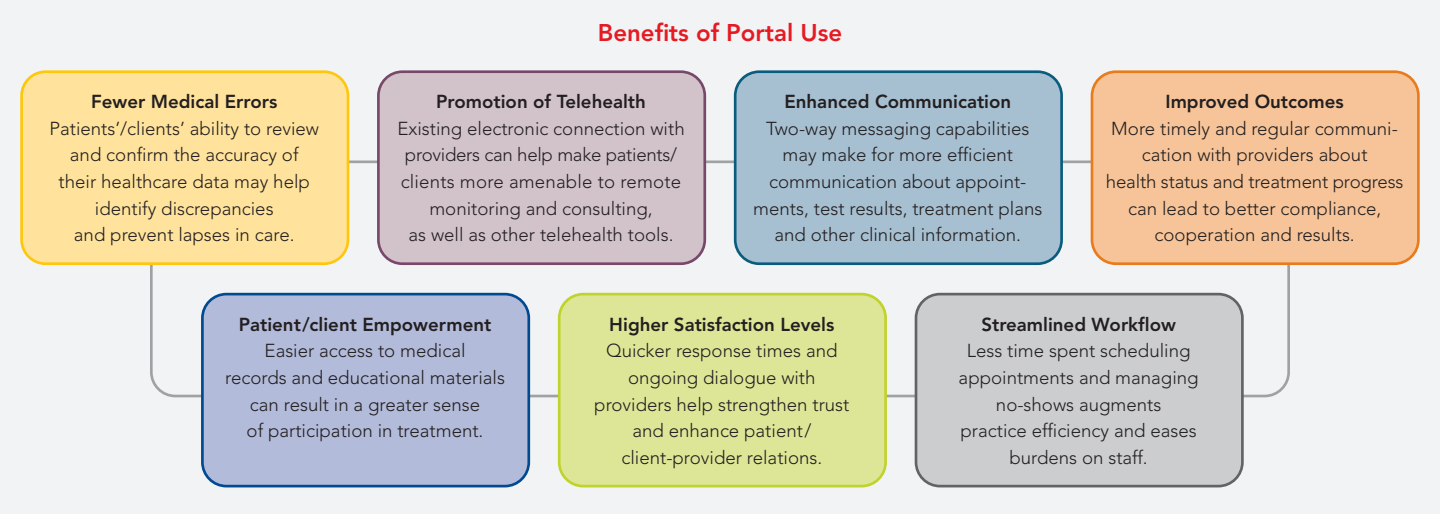
Track prescriptions and streamline refill requests.

Capture data from wearable medical devices to better manage both acute and chronic conditions.

View and download forms and notices, including emergency contacts and statements regarding payment responsibility and privacy.

Offer up-to-date financial information, including payments made and outstanding balances.

Source: "A Guide to the Top 10 Patient Portal Features" posted on the website of InteliChart, June 22, 2023.



Risk Exposures

When developing or upgrading a patient/client portal, bear in mind the following hazards and potential liabilities:

Security and privacy breaches. Anytime PHI is stored electronically, there is the possibility of unauthorized access. In accordance with the HIPAA Privacy Rule, healthcare organizations and providers are required to establish measures to secure PHI and other sensitive information against the risk of hacking, improper disclosure, data loss or corruption, and other cyber threats.

Inappropriate use. In general, providers should not use portals as a means to convey serious or life-threatening diagnoses, critical or significant laboratory results, or information on such confidential topics as mental health, genetic testing or STDs. As information disclosure may be governed by federal and state law, among other authorities, providers and organizational leaders are encouraged to review relevant requirements with legal counsel.

Misinterpretation of data. Patient/client access to health data without necessary context may create anxiety and lead to incorrect self-diagnosis. Therefore, the portal's disclaimer message should relay the risk of data misinterpretation when information is retrieved prior to consultation with a medical provider.

Overreliance on portals. Portals are meant to supplement face-to-face visits, not to replace them. Portal overuse at the expense of more traditional modes of communication can potentially result in claims alleging misdiagnosis, delayed treatment, failure to monitor or other causes of legal action.

Misuse of portals in emergencies. Written policy should strictly prohibit providers from treating patients/clients via a portal in emergent or urgent situations.

Failure to reply promptly. Portals should be monitored on a regular basis and a reasonable effort should be made to respond on the same day to messages that arrive within normal business hours. Depending upon the nature of the portal message and type of healthcare setting, some messages may be handled by staff, while others may require the attention of a physician or advanced practice provider. To help ensure prompt replies to incoming messages, delineate the response process in written protocol, including responsible parties and expectations.

Documentation lapses. While portals may seem like an informal channel of communication, the standard rules of documentation still apply. In the case of portals not integrated with the EHR, this includes the requirement that all provider responses and/or communications be filed in the patient/client healthcare information record. From a legal point of view, such an entry in the record may serve as evidence that a patient/client was informed of the necessity of pursuing a certain course of treatment, thus helping defend against potential claims.

For a list of safeguards designed to mitigate exposure to portal-related liabilities, see page 3.

Electronic portals can significantly enhance communication between providers and patients/clients. Like all innovations, however, portal use is not without its own risks. The measures suggested in this resource – especially those involving ongoing monitoring of incoming messages and continually reviewing and updating cyber security practices – can help ensure that portals are utilized safely and appropriately, thus strengthening patient/client engagement and compliance, while minimizing liability exposure.

Quick Links

- "Patient Portal Optimization: Engage Patients While Minimizing Care Team Burden." AMA STEPS Forward, posted August 20, 2024. (Toolkit.)
- Patient Portal Toolkit, issued by the American Health Information Management Association, 2016.

Portal Safeguards

The following risk mitigation strategies, among others, can help healthcare providers and organizations ensure that their portals are secure against data breaches and are utilized in a safe and proper manner:

Security and Privacy Measures

- **Encrypt the portal database** to ensure that information is securely stored and transmitted.
- **Implement a role-based access control (RBAC) protocol,** which authorizes access according to individual job description and information needs.
- **Control portal access using assigned usernames,** secure passwords, multi-factor authentication and account lockout features.
- **Utilize opt-in agreements,** requiring patients/clients to attest to their awareness of portal privacy and security policies, as well as the possibility of data breaches.
- **Provide cyber security training** to all providers and staff members who have access to patient/client portals.
- **Schedule regular security updates,** to be performed by authorized personnel.
- **Conduct periodic audits of the portal system** to track key user activities and identify instances of inappropriate access and/or potential HIPAA Privacy Rule violations.

User Agreements

- **Define permissible uses of the portal,** as well as user responsibilities. (See Quick Links for a sample patient/client portal user agreement issued by the American Health Information Management Association.)
- **Emphasize that portal use is limited to non-urgent conditions** and that it is not intended for dealing with emergency situations or for conveying sensitive information.
- **Note that technical problems may occur,** leading to unforeseen downtime.
- **Inform users that the portal is an optional service** and that access may be suspended or terminated at any time.

Proxy Users

- **Address access by patient/client proxies** – for example, a parent managing a child's portal – in the RBAC protocol.
- **Obtain written consent from patients/clients for any proxy user** prior to granting them access to the portal, in conformity with HIPAA requirements.
- **Consult legal counsel regarding the implications of granting proxy access to portals assigned to adolescent patients/clients,** particularly when the minor is receiving treatment without the parent's or legal guardian's consent, as allowed by law.

Patient/client Education

- **Provide written instructions on how to access and utilize the portal** in a secure and effective manner.
- **Explain the portal's basic uses,** e.g., relaying information about appointments, medication refills, referrals and laboratory reports, as well as downloading forms, documents and educational materials.
- **Reiterate that the portal is not to be used to discuss life-threatening matters,** evaluate or treat new problems, or respond to detailed inquiries that would require physical assessment.
- **Inform users of the provider's or facility's average response time,** without making express promises.
- **On a regular basis, remind users of security measures,** enrollment requirements and access restrictions.

Communication Policies

- **Designate a time frame for posting health data,** taking into account patient needs, staff capabilities and federal guidelines. (Note that according to the 21st Century Cures Act, patients/clients have the right to view electronically stored medical data as soon as it is available, unless immediate access is likely to endanger the life or safety of the patient/client.)
- **Respond to incoming patient/client portal messages within a reasonable time,** ideally on the same day if the message is received during normal business hours. (See "Responding to Patient Portal Messages," issued by the American Medical Association, 2024.)
- **Verify patient/client receipt of diagnostic results** through a message confirmation feature.
- **Monitor receipt of outbound messages,** and make a follow-up call to patients/clients when communications go unread, especially in regard to consequential diagnostic or treatment matters.
- **Authorize select staff members or alternate providers to reply to patients/clients** when the primary provider is not available.
- **Inform patients/clients when the portal is not functioning,** using either a notification on the practice or facility website, a prerecorded telephone message for inbound calls or an email message sent to patients/clients.
- **Establish backup communication arrangements** in the event the portal is not accessible, e.g., defer to designated phone lines and other forms of approved and secure messaging.
- **Monitor portal activity** and, if necessary, consider ways to encourage patient/client utilization, such as incorporating user-friendly design features or improving message response times, among other strategies.

Rules and Enforcement

- **Draft formal protocols governing portal access and conduct,** and measure compliance through regular audits.
- **Explain that all electronic messages to providers should be sent via a secure platform,** e.g., portal or secure texting, rather than providers' personal email accounts or other non-secure platforms.
- **Inform users that the portal exists to complement other modes of communication**, including face-to-face, telephone and mail.
- **Include a privacy/confidentiality statement** on outgoing messages.
- **Set character limits for both outgoing and inbound portal communications** to ensure that messages are brief and to the point.
- **Be prepared to answer users' questions about portal use and limitations,** assigning this task to a knowledgeable and articulate staff member.
- **Request that patients/clients inform the facility promptly when their email address changes,** as well as when they suspect that a breach of privacy has occurred or note inaccuracies in their personal information.
- **Restrict inbound messages if patients/clients have not been seen by a provider within a certain period,** e.g., the past one to two years, or if the patient is scheduled to see the provider soon and the matter could be addressed more efficiently at that time.
- **Terminate user access promptly when necessary** – e.g., when patients/clients leave the practice, die or intentionally misuse the portal – and assign this responsibility to an administrator, IT professional or compliance officer.

Disclaimers

- **Confer with legal counsel** about the scope and content of the portal's disclaimer message.
- **Post the disclaimer on the portal's start page,** noting, among other items, that...
  - **The portal has its limits** and is not a substitute for face-to-face care by a healthcare provider.
  - **General information provided through the portal is for educational purposes only** and is not to be construed as medical advice.
  - **The healthcare organization, as well as its providers and staff, are not liable for any portal malfunction,** suspension or disruption that may affect patients/clients.
  - **The portal is not to be used for emergent/urgent conditions,** and that individuals experiencing a medical emergency should call 911 or seek treatment at the nearest ED.

This table serves as a reference for healthcare organizations seeking to evaluate risk exposures associated with patient/client portal use. The content is not intended to represent a comprehensive listing of all actions needed to address the subject matter, but rather is a means of initiating internal discussion and self-examination. Your organization and risks may be different from those addressed herein, and you may wish to modify the activities and questions noted herein to suit your individual organizational practice and patient needs. The information contained herein is not intended to establish any standard of care, or address the circumstances of any specific healthcare organization. It is not intended to serve as legal advice appropriate for any particular factual situations, or to provide an acknowledgement that any given factual situation is covered under any CNA insurance policy. The material presented is not intended to constitute a binding contract. These statements do not constitute a risk management directive from CNA. No organization or individual should act upon this information without appropriate professional advice, including advice of legal counsel, given after a thorough examination of the individual situation, encompassing a review of relevant facts, laws and regulations. CNA assumes no responsibility for the consequences of the use or nonuse of this information.

Did someone forward this newsletter to you? If you would like to receive future issues of *inBrief*® by email, please register for a complimentary subscription at go.cna.com/HCsubscribe.

For more information, please call us at 888-288-3534 or visit www.nso.com or www.hpso.com.

888-288-3534 www.nso.com www.hpso.com