American Health Information Management Association

PATIENT PORTAL

TOOLKIT

AHIMA
American Health Information
Management Association®

PATIENT PORTAL TOOLKIT

Copyright ©2016 by the American Health Information Management Association. All rights reserved. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, photocopying, recording, or otherwise, without the prior written permission of AHIMA, 233 N. Michigan Ave., 21st Fl., Chicago, IL, 60601 (https://secure.ahima.org/publications/reprint/index.aspx).

ISBN 978-1-58426-498-9
Product code: ONB199016
AHIMA Staff:
Caitlin Wilson, Assistant Editor
Pamela Woolf, Director of Publications, AHIMA Press
Anne Zender, Senior Director, Periodicals

Limit of Liability/Disclaimer of Warranty: This book is sold, as is, without warranty of any kind, either express or implied. While every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Neither is any liability assumed for damages resulting from the use of the information or instructions contained herein. It is further stated that the publisher and author are not responsible for any damage or loss to your data or your equipment that results directly or indirectly from your use of this book.

The websites listed in this book were current and valid as of the date of publication. However, webpage addresses and the information on them may change at any time. The user is encouraged to perform his or her own general web searches to locate any site addresses listed here that are no longer valid.

CPT® is a registered trademark of the American Medical Association. All other copyrights and trademarks mentioned in this book are the possession of their respective owners. AHIMA makes no claim of ownership by mentioning products that contain such marks.

For more information about AHIMA Press publications, including updates, visit http://www.ahima.org/education/press?tabid=Updates

American Health Information Management Association
233 N. Michigan Ave., 21st Fl.
Chicago, IL 60601

TABLE OF CONTENTS

FOREWORD

In 2014, Stage 2 of the Centers for Medicare and Medicaid Services (CMS) “meaningful use” EHR Incentive Program required eligible providers and hospitals to meet the “Patient Electronic Access” objective. This objective is comprised of various measures requiring the online availability of health information and the patient’s ability to transmit their health information. These measures are largely met by the implementation of patient portals.

AHIMA recognized the continued growth of patient portal implementation and the need for related guidance. In April 2015, AHIMA published the practice brief “The Implementation and Management of Patient Portals” and provided recommended practices for the implementation and management of patient portals. The practice brief addressed topic areas from stakeholders and selection to overall portal management and patient education. This toolkit supplements the practice brief and takes a deeper dive into the challenges and issues of managing a patient portal as well as provides recommended practices. Sections have been added to address the latest regulatory requirements and the significance of education and training on patient portals within the industry.

Note: *As this toolkit was being completed, (CMS) announced that the meaningful use program would be phased out by 2017.*

AUTHORS

Lucia Aschettino, HITPro-IT, HITPro-CP, HITPro-TR

LeAnne Bouma, RHIA

Benjamin Burton, JD, MBA, RHIA, CHP, CHC, CRC

Mindy Davis, RHIT, CCS, CDIP (Foreword)

Cindy Gardner, RHIT

Elisa Gorton, MAHSM, RHIA, CHPS

Leah Grebner, PhD, RHIA, CCS, FAHIMA

Margaret Hennings, MBA, RHIA

Nancy LaFianza, MBA, RHIA, CHPS

Kevin Baldwin, MPH, CPHIMS

Michael Nelson, DPM

Patti Reisinger, RHIT, CCS

Angela Rose, MHA, RHIA, CHPS, FAHIMA

Alisha Smith, MS, RHIA, CHPS

ACKNOWLEDGEMENTS

Katherine Andersen, RHIT, CCS, CRCS-I, CRCS-P

Maria Barbetta, RHIA

Rebecca A. Buegel, RHIA, CHP, CHC

Patricia Buttner, RHIA, CDIP, CHDA, CCS

Crystal Clack, MS, RHIA, CCS

Tammy Combs, RN, MSN, CCS, CCDS, CDIP

Nancy Davis, MS, RHIA, CHPS

Elizabeth Delahoussaye, RHIA, CHPS

Jeanne M. Fernandes, RHIA, CHDA

Karen Gibson, MS, RHIA, FAHIMA

Aviva Halpert, RHIA, CHPS

Judi Hofman, BCRT, CHPS, CHP, CHSS

Lesley Kadlec, MA, RHIA, CHDA

Beth Liette, MS, RHIA

Carol Maimone, RHIT, CCS

Kelly McLendon, RHIA, CHPS

Jennifer Mueller, MBA, RHIA

Deanna Peterson, MHA, RHIA, CHPS

Andrea Romero, RHIT, CCS, CPC

Donna Rugg, RHIT, CCS, CDIP

Kathleen Scott, RHIA

Tracy Stanley, RHIT

Nicole Van Andel, MS, RHIA, CHPS

Lou Ann Wiedemann, MS, RHIA, CDIP, CHDA, FAHIMA

Holly Woemmel, MA, RHIA, CHPS

Kerry Taylor Wolford, RHIA

Donna Young, RHIA, CCS

INTRODUCTION

The “meaningful use” EHR Incentive Program and patient-centered healthcare have helped to fuel the consumer engagement movement in which patients are taking responsibility for their care and actively becoming a part of decisions made regarding their health. The use of patient portals is one of the main tools for meeting the meaningful use patient electronic access criteria and thus one of the reasons why portals have pervaded the healthcare industry. Patient portals have advanced the patient/provider relationship into the technology era by allowing patients to communicate with their providers via messaging functionality or virtual encounters. Patient portals also empower patients to be more accountable for and to manage their own health by allowing 24-hour online access at their fingertips, viewing lab results, scheduling appointments, and more.

The implementation of patient portals continues to increase, as will their functionalities and capabilities. Like any other piece of technology, portals will mature quickly and with that come issues and challenges involved in selection, implementation, and overall management. More importantly, the safeguards required to protect the health information contained within will be paramount.

The purpose of this toolkit is to provide guidance on the issues and challenges that should be considered when implementing a patient portal, such as the types of policies and procedures that will need to be put into place, workforce and consumer education and training, and the legal requirements and considerations that must be accounted for a successful portal implementation. Sample forms, portal use agreement, and patient portal FAQs are also included.

SECTION I: DEFINING THE PATIENT PORTAL

Definition of a Patient Portal

A patient portal is a secure online tool (i.e., website, mobile app) that gives patients convenient 24/7 access to personal health information using a username and password. This health information is accessible anywhere an Internet connection is available. The information contained within a portal can include doctor visits, medications, immunizations, allergies, and diagnostic lab results. It can also incorporate secure e-mail communications, requests for prescription refills, scheduling appointments, updating contact information, making payments, downloading initial visit forms, and viewing educational materials.

A patient portal improves an organization’s patient-provider relationship by fostering stronger patient-provider communication, empowering patients with healthcare data and information, supporting patient-provider care between office visits, and most importantly, promoting the goal of improving patient engagement to ultimately achieve successful outcomes.

Stand-alone Portal vs. System Integrated Portal

There are two types of patient portals, a stand-alone patient portal and a system integrated patient portal. Stand-alone patient portals are generally used for smaller provider practices and do not offer full portal functionality such as two-way communications. A stand-alone patient portal generally does not interface with a provider’s electronic health record (EHR) system and often requires more work for office staff since this would be additional software to manage.[1]

Integrated patient portals are often part of an EHR or from a vendor that partners with an EHR vendor so that the interface between the systems functions properly. When an integrated patient portal is used, functionality can include, but is not limited to, the ability to have uploads occur automatically, utilize online bill pay, send automated messages to patients without office staff assistance, and allow messaging between provider and patient. If the portal does allow messaging, providers must have staff available to monitor incoming messages for timely receipt and response.

In either situation, the following must be considered:

- Is the portal on a secure network?
- How are invitations to join a portal sent (i.e., in person vs. e-mail)?
- Is it password protected?
- Are proxies permitted?
- How are passwords reset?

Portal Ownership

Today, as the healthcare landscape changes, healthcare is becoming more patient centered and patients are engaging in their healthcare as never before. Patient portals provide patients the ability to have their health information available at their fingertips and allow for contact with their provider via the portal.

Before patient portals, it was generally accepted that the health record was the property of the healthcare facility and the information contained within was the property of the patient. With the implementation of EHRs, specifically patient portals, there has not yet been any concrete clarification on who owns a patient portal. Of various state laws governing the ownership of health records, in 2012, only the state of New Hampshire had a law that clearly defined the owner of the health record as the patient.[2]

Patient portals provide patients with the ability to have their health information at their fingertips and allows for contact with their provider via the portal. Access to health information through a portal allows a patient more ownership of their healthcare, but not necessarily ownership of their patient portal.[3] With messaging capability, the question then becomes, if the patient creates the information (e.g., a question to the provider), does it become part of their legal health record? If so, is it owned by the provider or because it is part of the patient portal and generated by the patient, does the ownership of the incoming communication become that of the patient?

HIM professionals generally hold that the information in the health record belongs to the patient. However, the portal is different from the health record itself. Although the information in the portal is derived from the record, only certain pieces of the record, from laboratory results to bill payment to messaging, may be represented. A general conclusion may be that the patient owns their information in their health record, not the portal itself.

Regardless of the medium in which the protected health information (PHI) is stored, the provider is responsible for the portal and all information uploaded to it, the maintenance of it and the day-to-day monitoring of any incoming messages.

Patient Portal Trends

The major transformation that continues to drive change in the healthcare industry is the movement away from the practice of "old medicine," the provider-centric healthcare delivery process, to the "new medicine" delivery model where there is a convergence of digital information systems, imaging, genomics, wireless sensors, social networking, Internet, and mobile connectivity. Readily available patient health data is the catalyst to this transformation. Patients need health information to become actively engaged participants in their health delivery process. Technology continues to set expectations and drive the features and functionalities that consumers use to access and communicate.

Some of the major technology trends for patient portal solutions include:

- **Personalization:** Personalization is the underlying principal of delivering patient-specific information. The ability to personalize the patient portal experience is fundamental to increased patient engagement. Targeted content that can be leveraged by the patient to better understand the state of their health provides important data and content for a third party to assist in the healthcare delivery process and drive successful outcomes. An increasingly important criterion for the meaningful use incentive program requirements is to provide educational material to the patient. A highly personalized patient portal experience can assist with the process of delivering specific educational resources to map against the patient's health condition.
- **Mobile device access:** Patients and providers want to be able to access, transfer, and communicate 24/7 seamlessly. The ability to have this flexibility will become a non-negotiable expectation. Caregivers and patients will be looking to a patient portal solution to deliver efficiency and effectiveness and to improve the patient's overall healthcare experience.
- **Wearable technology devices** (e.g., FitBit, smartphone applications): These devices provide a single view of health data such as blood pressure and heart rates and are beneficial to both the patient and the entire health care support staff. "If we had data from home monitoring devices, that would fit well with personal health records (PHRs) and could be reviewed by a clinician over time as a longitudinal record," said consultant Chris Giancola in a 2013 iHealthbeat article. "As a consumer, I can submit that information through a portal, or I can interact with an application that is a patient portal app on my iPhone. This

could potentially drive a lot of value for both patients and providers." [4] ***Note:*** *Consideration should be taken regarding how to incorporate patient-generated data into the organization's health record.*

- **Communications:** Two-way dialogue between patients and providers will continue to evolve and will go beyond the office visit. The portal becomes the channel for patients to set up appointments, request prescription refills, ask questions, provide reminders (e.g., immunizations, follow-up), and push out educational resources. This will promote patient engagement and encourage accountability for individual healthcare.

Portal Implementation and Management Challenges

Implementation of a patient portal can present many challenges, including management and organizational implementation challenges, technological system challenges, patient engagement challenges, and above all privacy and security of health information challenges.

Challenges related to management and organization implementation start with the very first conversation of patient portal implementation and continue beyond go-live. Key organizational stakeholders must be involved in implementation and include all departments associated with the information posted to the portal (i.e. billing, laboratory, diagnostic imaging, pharmacy, marketing, and health information). A point person should take ownership of implementation and training. The organization must decide what information would be available to the patient, how access is obtained (e.g. password assignment, proxy access) and if the portal will allow for bi-directional communication. If bi-directional conversations are to occur, the implementation of monitoring the incoming communication must be clearly defined.

Two significant challenges for management and the organization are ensuring that portals are accessed solely by the patient and/or their proxy and ensuring incoming communication is monitored and that any patient issues with the portal are quickly responded to. The timeliness of information posted to the portal must also be clearly defined so that the information is relevant and pertinent for the patient to use and share with providers and caregivers.

In order to meet meaningful use stage 2 criteria for patient portal usage, organizations must market their portals to their providers and staff as well as to the public. Staff must be skilled at answering questions, concerns, and issues that providers and patients may encounter. Patients may well have questions, as portal awareness remains low across the country.[5]

A patient portal creates many technological challenges for both the organization and the patient. Patients may have multiple patient portals with different providers, which can add to already existing challenges. With cyber attacks and medical identify theft on the rise,[6] the security of information during transmission and access to the portal must be tightly monitored. Guidance must be provided to the patient/proxy on appropriate portal use to ensure that the privacy of all protected health information (PHI) is maintained. This would include posting an organization's privacy notice, contact information, and usage guidelines to the patient portal landing page. In addition to providing guidance, an organization should determine if portal access will be compatible with all computers and programs.

There are other policy considerations. The use of a patient portal should not require any cost to the patient or proxy. Additional considerations include user friendliness, output reader friendliness, and how the information in a patient portal can be converted or transmitted to another portal or website for patient use. The organization's patient portal terms and conditions of use must be reviewed and agreed upon with the patient prior to granting access. Privacy notices should also be made available to ensure that patients understand that any downloaded PHI from the portal is no longer covered by the provider and can be redisclosed. Finally, a statement should be included on the portal that an account can be deactivated due to misuse, abuse, or inappropriate usage by the patient or their proxy.

SECTION II: SELECTION AND IMPLEMENTATION

Patient portals have become a necessity for healthcare providers due to meaningful use stage 2 requirements and increasing consumer interest in being more active in their healthcare. Healthcare providers should perform an assessment of what the best type of portal would be for their patients. The assessment must include stakeholders and a request for proposal to various patient portal vendors. Additionally, a project plan should be developed so that all areas identified in the assessment are included (health information management [HIM], patient billing, lab services, etc.). This section outlines a more detailed process on the selection and implementation of a patient portal.

Stakeholders

A committee of key stakeholders must be formed to manage the overall selection and implementation of the patient portal within the organization. Internal stakeholders should be selected throughout the organization based on the impact of the patient portal. External stakeholders should include members of the community, including patients.

Internal stakeholders can include but are not limited to information technology (IT), HIM, pharmacy, nursing, lab, radiology, physicians, business office, ambulatory care, and any other department that might schedule patients for outpatient services, compliance, legal, and risk management.

External stakeholders can include but are not limited to patients, parents, legal guardians, external physicians, other healthcare facilities, and portal vendor.

Assessment/Evaluation Plan

The members of the committee should develop a list of the desired functionalities of the portal. The functionalities can include, but are not limited to:

- Patient viewing of pre-determined PHI (i.e., allergy list, medication list, test results)
- Messaging (with providers)
- Scheduling and managing current and future appointments
- Managing account balances and making payments
- Downloading, printing, and transferring PHI

The list should then be developed into an assessment sheet to allow a subcommittee to evaluate potential vendors. Some items to consider include the benefits and drawbacks of each proposed vendor, including cost to set up, implementation, maintenance, and future modifications and/or updates to the portal. The subcommittee should include the IT department, HIM department, and others that can determine the vendor that best fits the facility's IT structure, privacy and security environment, and overall organizational goals and needs.

The assessment should include all financial costs, staffing costs, set-up fees, customization fees, and maintenance fees for ongoing support. They should also include who will be responsible for training and support for the patients and external users, how the application process is completed, who grants access, and what department monitors access to the portal.

Request for Proposal

After the assessment team determines what will be included in the patient portal, the request for proposal should be developed and sent to various vendors. As vendor presentations are reviewed, the team should develop the pros and cons of each vendor presentation. It is important that the patient portal team work cohesively with the vendor. The selection of the vendor is then made and contracts and business associate agreements developed and executed.

The following, at a minimum, should be considered prior to selection:[7]

- **Regulatory and/or voluntary incentive requirements:** Ensure compliance with all federal and state laws and regulations
- **Clinician and patient participation:** Determine who will generate and use the portal information, including when and which information will be made available

- **Administrative (bill paying, appointments):** Determine which administrative tasks will be available to patients on the portal such as release of information, customer service, appointments, registration, profile updates, billing, and e-mail
- **Resource needs:**
  - **Workforce:** Evaluate staffing needs (internal and/or external) to build, maintain, and manage the portal system (i.e., ongoing integrity assurance, answering user questions, or providing internal/external training on policies and procedures)
  - **Budget:** Ensure budgetary needs to meet the organizational goals and vision for the portal implementation and maintenance
  - **Vendor:** Assess external vendor capability needs for development, implementation, and ongoing support
- **Information access:** Establish who will have access to the portal and for what purpose. Determine the process for the provisioning and de-provisioning of user access
- **Technology capabilities:** Support tasks related to interoperability needs and privacy and security considerations
  - **Interoperability:** Ensure the portal will integrate with other systems (internal and, if needed, external) including the organization's EHR system while validating continued maintenance of information integrity
  - **Privacy and security:** Make certain the privacy and security of information is understood and maintained at all times
- **Usability:** Ease of use of the portal for the user (both workforce and patient) is critical to the success of the overall system

Steps to Implementation

A detailed work plan and program charter should be created, and all members of the patient portal team should sign off on the assigned tasks and timelines. This includes the frequency of meetings and the assignment of both a project manager and program manager. All timelines must be realistic. The detailed work plan will include testing phases, the roll-out timeline (full go-live or phased approach), and post go-live analysis. Marketing must also be included to ensure that patients are aware of this new service as well.

Rollout of the portal will require the careful minding, at a minimum, of at least several important steps:[8]

1. **Timeline:** Establish a realistic timeline to achieve the goals and objectives of the portal system with adequate flexibility for unforeseen obstacles
2. **Portal content:** An interdisciplinary team (i.e., clinicians, HIM, IT, pharmacy, laboratory, radiology) determines what type of health information will be made available to the patient in the portal. Content determinations are not all driven by meaningful use obligations.
3. **Testing:** The portal will be used by patients, patient representatives, and associated workforce members and therefore must be tested by a number of patients to determine if it functions well for all segments of the population. The project team needs to conduct user acceptance testing for different population types (i.e., ages, education levels) that best represent the population that will use the portal on a regular basis. Ongoing testing can create a need to make changes in the portal system. In addition to the functionality and comprehension testing, the confidentiality, security, and integrity of the data will also need to be validated. Such testing would need to be directed toward the information flowing into the portal from other related systems as well as any information that might flow from patients or their surrogates.
4. **Access and authentication:** Access to the portal should ideally be initiated during a patient visit or hospital stay. This allows the organization to establish its authentication process (verify user identity), ensure the patient has access to the training and other materials that can accentuate the use of the portal, and explain how the portal can increase the patient's involvement in their care. Such information will vary by portal and patient. For an initial period it would be an extra benefit if the organization could facilitate some sort of hands-on training at the organization location, but at a minimum workforce should encourage participation.

5. **Information governance:** A portal's information is not static as long as the patient is receiving care. Any changes in the source information or the systems involved, new information, and so forth requires constant governance to ensure information integrity, including the information in the portal. Portals will evolve and expand as resources and requirements change.

SECTION III: OPERATIONS AND MANAGEMENT

Organizations must reach consensus on well-defined business processes, workflows, governance, and policies that are essential for a patient portal to succeed. The roles and responsibilities of those overseeing the initial rollout, maintenance, and ongoing evolution of the patient portal must be well defined, and there must be strict adherence to privacy and security safeguards. Determinations of the information that will be made available through the portal, the integrity of that data, and the most effective ways to facilitate patient portal enrollment will also be crucial. In addition, policies and procedures must be put in place to handle all legal, compliance, and operational contingencies that may impact patient portal usage.

Registration/Enrollment

The process for enrolling patients and/or their proxies or representatives for patient portal use must be as pain-free and easy as possible. Recommended practice is for patients to be enrolled in person at the point of care. A form is usually completed to document and initiate the patient portal enrollment/registration process (see Appendix A). The patient should also designate in writing his or her proxy or representation at this time. An office staff member should be available to validate the patient's identity and assist him/her through the process. Familiarity with a patient does not constitute validation of identity. Validation and verification can be accomplished by examining a government issued photo ID such as a driver's license or passport or a birth certificate.

However, one must bear in mind that in today's environment of rampant identity theft, fraudulent identity credentials are becoming increasingly easy to obtain. A provider organization should consider training its staff to detect fraudulent driver's licenses using the same quick and simple procedure utilized by the Transportation Security Administration at airports—a quick scan of the license with a small black light will detect holograms embedded in the license.

Staff should be familiar with an organization's policy if there is a question about a person's identity. Many provider organizations do not have the resources it takes to register patients for patient portal usage. Online registration is a practical alternative to rapidly increase the number of enrollees as it removes the enrollment burden from the provider office and enables patients to enroll when it is more convenient. The online enrollment application should also include fields to capture the patient's proxy or representative.

Many provider offices will give their patients a patient portal URL and an access code to log into the portal registration process. However, online enrollment presents its own set of challenges. The identity of the patient must still be validated.

There are a number of services and technologies available today for remote identity-proofing. These include web services to authenticate whether an identity is real or synthetic as well as to verify that the real identity belongs to the person asserting it. This is done by asking a few knowledge-based authentication challenge questions about the person that only the right person should be able to answer. A number of vendors offer such a service and one should first investigate which data sources these vendors use to generate their questions. Questions derived from public web sites and social media sites are easier for an individual to research and answer, correctly thereby fooling the system. Questions derived from non-public data sources are the most difficult to scam.

There are other safeguard technologies. Fraud alerts at the time of registration can notify the portal administrator that the identity entered on the registration page has been reported as stolen or linked to some fraudulent activity. Device reputation services can send alerts that the remote device that is accessing the portal registration site has been linked to fraudulent activity, in or out of healthcare. There are also smart phone apps that perform facial recognition, comparing the photo on a driver's license or passport to a selfie of the registrant. In addition, there is software available that can authenticate a driver's license or passport from a smartphone photo of the document. These services and technologies are now affordable, and portal administrators should collaborate with their IT departments for such validation processes.

Periodically, the patient should go through the identity-proofing process again, especially if he/she has not accessed the portal for a specified amount of time (i.e., annually). Lastly, once a patient is enrolled, an organization should consider some form of multifactor authentication for ongoing access to the portal. The National Institute for Standards and Technology (NIST) has issued guidance on identity proofing.

Policies and Procedures

Policies and procedures will need to be completed prior to implementation. During the implementation phase, each facility will need to establish internal polices for the management and control of the portal and policies for external users of the portal.

Establishing Internal Policies

Internal policy considerations include:

1. Management and ownership of the patient portal within the facility:
   Establishing ownership of the patient portal within the facility prior to implementation.[9] Consideration will need to be made for registration of patients, customer support, and technical support. This can be provided by one department or a collaboration of multiple departments. Clear policies on the roles of each will be crucial to the implementation as well.
2. Timeframe in which information will be transmitted to the portal:
   Create a timeframe in which information is transmitted to the portal. There will need to be a balance between meaningful use considerations, patient demand, and medical staff concerns. For meaningful use, patients must have the ability to view online, download, and transmit their health information within four business days (or within 36 hours of discharge for eligible hospitals). Be sure to consult with your medical staff and make them aware that information will be available within the established timeframe. Patients may be able to view the clinical documents before the provider has reviewed the information and discussed with the patient.
3. Current functionality and information being transmitted and received into the portal:
   Explain the overall functionality of the patient portal to the user. This could include bill pay, messaging, prescription refill, and appointment scheduling.

   In order to protect sensitive (e.g., mental health, substance abuse, HIV) or protected information, a policy will need to be created. Federal and state guidelines must be followed. Information that is not being transmitted will need to be stated in this policy and in the information provided to the patient.
4. Registration process:
   The registration process will need to be established. (Refer to Appendix B for a sample policy.) Decisions such as who can register and whether or not the patient can self-register need to be made. The portal vendor will need to be consulted on the viability of these options.

   Proxy users must be given access by the patient through the forms required by HIPAA and the healthcare organization. The HIPAA privacy rule indicates that written consent is required for a proxy user to access a patient's health information. All information in the patient's portal is available to the proxy user(s). Organizations should determine if proxy access is permitted. A policy regarding minors' access to the patient portal will also need to be established.

   Review of state and federal guidelines will stipulate what is further protected.

External Policy: Customer Terms and Agreements

These policies will be the terms and conditions for the patient portal users. Each registered user will need to agree to the terms outlined in order to access the portal. Facility legal counsel should be consulted prior to posting terms and conditions. Here is a basic outline to follow with a sample form attached.

1. General use
   a. Subject matter
   b. Functionality
   c. Communication

   d. Technical and user support
      i. Contact information
      ii. Expected response times
   e. Medical advice and information
2. Terms of Use
   a. Privacy and security
   b. Availability
   c. Access
   d. Termination

Data Integrity

Organizations must have policies and procedures in place to ensure integrity of the information. The integrity of information within a patient's health record can be impacted by multiple sources, including intentional or unintentional self-reported information from the patient as well as the source EHR and any external systems that feed into it. Processes must be in place to make any necessary corrections in the EHR, all source systems, and in the portal itself. Inaccuracies created when information is entered or imported incorrectly into the wrong patient's health record can be released into the portal, resulting in not only incorrect information being used in the care of the patient, but also a HIPAA breach. This is a risk to the patient and to the organization.

It is important for organizations to continually educate and train staff documenting in the patient health record about the significance of capturing and documenting information correctly (verify and validate), appropriately and in a format patients can understand. Some options to help ensure validation of a patient include optical character recognition of the patient's identification credentials and insurance cards to prevent data entry errors as well as third-party data sources to confirm self-reported demographic information.

A new and emerging HIM role helping to ensure data integrity is known as a portal screener.[10] This role screens the patient chart looking for misfiles and can potentially identify other areas of concern that could impact the integrity of the record. Errors identified can be remediated prior to releasing the information to the portal which will help to prevent breaches of information and ensure the integrity of the record.

Violations/Breaches

A lab result scanned to the wrong patient, a provider documenting on the wrong patient's health record, and incorrectly entering information into a health record are all errors that, if not corrected, can lead to a breach. Procedures should be in place to identify this information (perhaps via portal screeners) before it is uploaded to the portal to help limit potential breaches and violations. Data integrity or correction workflows must also be documented to correct errors identified.

A policy and procedure must be in place providing direction on how to report possible breaches. Patient portals should also be included in the organization's security risk analyses to assess for potential vulnerabilities and threats, including third-party vendor assessments.

The investigation and management of incidents/breaches is beyond the scope of this toolkit. Refer to AHIMA's Breach Management Toolkit for further guidance.[11]

Release of Information Function Changes

The purpose of the patient portal is to increase patient engagement regarding healthcare. The portal can foster better communication between the patient and the provider and help the patient better understand their care. Depending upon the organization, some information may already be available without going through traditional release of information processes. Patient portals are not designed for other types of release of information functions such as requests for life insurance or disability determination.

Some portals allow for information to be requested directly through the portal. Requested records already in an electronic format can be released directly through the portal. Once the documentation is delivered, the patient can view, download, and transmit them, allowing for access as often as needed. Because patient portals are only for information created in an electronic format, paper records may not be deliverable via the portal.

For further guidance, refer to AHIMA's Release of Information Toolkit.[12]

PHI Selection for the Portal

Different patients have different reasons for accessing protected health information (PHI) through a patient portal. When selecting the PHI to be posted to the portal, the organization should take into account its specific patient population (e.g., the provider organization may be a Beacon Community for diabetes, asthma, or other disease cohorts) and ensure that the patient portal will display PHI that meets the needs of its patient population.

Most frequently displayed portal PHI:

- Lab results
- Radiology results
- Medication history
- Immunization history
- Surgical history
- Vital signs history
- Problem list
- Appointments
- Insurance information
- Messages

The patient portal should allow the patient to "customize" his/her screens to view PHI that is of greatest interest to him/her in a local and easy to read format.

Note: Since HIPAA considers individually identifiable health information to be a subset of PHI, the portal should also have the ability to limit how much information is displayed (e.g., hiding date of birth and social security number can hinder identity theft).

SECTION IV: LEGAL CONSIDERATIONS AND REQUIREMENTS

This section of the toolkit identifies the legal issues and challenges that need to be addressed prior to creating a patient portal. These issues include how HIPAA impacts the patient portal, what should be included in a portal agreement, and how organizations are using portals to meet meaningful use requirements. The issues surrounding proxy accounts and minors are also discussed.

HIPAA and the Patient Portal

The patient portal should not be confused with a personal health record (PHR). Although PHRs may contain the same or similar information as the patient portal, the PHR is a record created and maintained by the patient,[13] whereas the patient portal is created by the EHR vendor or other third party, contains information that is created either by the patient or the healthcare provider, and is maintained and controlled by the provider. It is this control of the information that is the main difference between portals and PHRs. Information controlled and maintained by the provider is subject to additional privacy and security protections. The provider is a covered entity (CE) under HIPAA, and as a CE they must comply with the HIPAA privacy and security rules when handling PHI. 45 CFR 160.103 defines PHI as individually identifiable information that is maintained or transmitted in electronic form by a covered entity.

When examining the law as it applies to patient portals, organizations should start by answering two basic questions:

1. Does HIPAA apply to information in the portal?
2. If so, which section of the regulation applies?

Any information contained within the patient portal is considered PHI and is therefore covered by HIPAA. CEs need to look to the next question. Which HIPAA regulation applies to this information? With a carefully crafted portal agreement, the CE should make it clear that information published to the portal will be treated the same as information that is directly shared with the patient. Therefore, information may be published to the portal without needing to obtain a separate signed authorization. 45 CFR 164.502 502 (a)(1)(i) ("Uses and disclosures of protected health information: General rules") allows information to be shared with the patient without an authorization. Once the patient has signed the portal agreement, the CE is free to publish information about that patient to the portal as stated in the agreement. After the organization has created a patient portal and the patient has signed a well-drafted agreement, the next issue the organization should address is third-party access.

The Portal Agreement

The portal agreement (see Appendix C) needs to accurately describe how the portal will be used and list the responsibilities of the patient as well as the provider. The patient needs to understand information published to the portal will only be accessible to authorized users as identified by the patient. The portal agreement should also state that information is protected and the password/access information may **only** be given to the patient. Access request to a portal is initiated by the patient or their proxy. Access is granted when the invitation to a patient portal is accepted by the patient. If the organization allows proxy access, then a separate agreement should be signed by the patient and the HIPAA rules around releases and disclosures to third parties should be followed.[14] If access to the portal is compromised in any way, this agreement should list the procedure for deleting or locking the account. If the information is breached the CE must follow the HIPAA breach rules 45 CFR 164 subpart D ("Notification in the Case of Breach of Unsecured Protected Health Information").

Proxy Accounts

Proxy accounts are created to allow other people and/or entities access to a patient's portal. The proxy account is different because PHI may be viewed by someone other than the patient. Therefore, information published to the portal and accessed by proxy would fall under 45 CFR 164.508, "Uses and disclosures for which an authorization is required." If the organization chooses to grant proxy access to the patient portal, a proxy request should be submitted (see Appendix D). This type of access must also accurately be defined in a proxy user agreement. This agreement needs to be signed by the patient as well as the proxy user; it must adequately inform the patient that they are authorizing the proxy user access to potentially sensitive PHI. The proxy agreement also needs to define how this access may be terminated and that it should be renewed annually to comply with HIPAA authorization rules. Refer to Appendix E for a sample proxy revocation form.

CEs that choose to offer proxy access should review the elements of a valid authorization as well as the required statements outlined in 45 CFR 164.508 ("Uses and disclosures for which an authorization is required"). Prior to allowing proxy access, the organization needs to weigh the benefits and risks of such an arrangement.

Security Protections for Portal Information

When handling PHI, the CE needs to ensure the information is secure and protected from unauthorized use. The CE should consult HIPAA regulations[15] to ensure adequate administrative, physical, and technical safeguards are maintained. The overall security of the patient portal should also be included in the organization's HIPAA security risk assessment. Additionally, CEs must ensure that PHI transmission is encrypted and secure by following the necessary standards and organizational policy. The initial creation of a patient portal account should allow for authentication of the user (e.g., unique username and password), clear explanation of a CE's privacy notice, and contact information for any concerns related to the information or access. As stated previously, it must be clearly stated to the user that any information downloaded, printed, or shared may be subject to redisclosure; therefore, it is no longer protected under HIPAA.

The CE entity must follow all the same security rules that it would ordinarily follow with any electronic PHI under its control. For an in-depth discussion and a good place to start, see AHIMA's practice brief "Security Risk Analysis and Management: An Overview."[16]

Meaningful Use

Organizations may use the patient portal to comply with meaningful use requirements and objectives by providing timely access to medical information.[17] Patients can view online, download, and transmit as soon as the information is posted.[18] It should be noted that an eligible hospital has different requirements in the program than an eligible provider. In order to meet the specific requirements, the marketing of the patient portal must be done by a healthcare provider/entity explaining the benefits of use including when and why a patient might use portal information. The portal must contain information that explains the benefits of the patient portal to the patient.

Minors/State Law

The federal HIPAA rule defers to state law on the issue of when a minor becomes emancipated as well as who can consent for the treatment of an unemancipated minor.[19] States differ on these issues and it is important for the CE to consult with their legal counsel. When creating a pediatric portal the CE needs to decide who will have access to the portal and what information will be published to the portal. Many states require the pediatric patient to consent to the release of certain PHI, especially if the law allows the pediatric patient to seek treatment without parental consent. Patient portals should also have the ability to be "turned off" once a patient reaches the age of majority (if a proxy is set up for the parent) to ensure that privacy is further maintained.

SECTION V: EDUCATION AND TRAINING

Patient portals have generated a need for training for patients, employees, and providers. Employees (including providers) need to be trained not only regarding the use of the portal, but also to prepare them to field questions from patients. It is imperative that they be trained on the legal aspects of portal use and communication with patients using the portal.

Physician offices should be a common place for patient education about portals to take place. This is where many patients may first learn about portal availability. Staff should be trained in how to provide education to patients about the following items:

- How to sign up for a portal log in and password
- How to access the portal
- Functionality of the portal
- How to opt out of the portal

Patients also need to be provided with the information about how to protect their personal health information. They need to be educated about when it is appropriate to use the portal to communicate with their provider and when it is not. For example, if a patient is experiencing potentially life-threatening symptoms, it is not appropriate to send a message to the provider via the portal, but rather call 911 instead.

Patients should be educated about proxy use of a patient portal. This includes additional legal information and instruction related to accessing information on another individual's records. Parents using proxy access in the patient portal must be educated about age-specific state rights, especially those specific to reproductive health, mental health, and substance abuse treatment.

HIM professionals may be trained to provide patient portal education to providers, as well as to the general public. Educational materials are provided to AHIMA component state associations for use by members to provide educational services in their communities. Refer to Appendices F and G for two samples of tools that can be used for patient education.

SECTION VI: THE FUTURE OF PATIENT PORTALS

Consumer engagement is a high priority in the US healthcare system today and will continue to be so as health information technologies evolve. Although healthcare delivery was historically provider-centric, we are witnessing a profound shift toward a patient-centered healthcare system. Patient portals are a technological catalyst that allows patients to interact, transact, and communicate with their healthcare providers. This is not a new phenomenon; other industries have been using similar technologies to engage, communicate, and retain their customers for many years. The patient portal is roughly analogous to the electronic financial portals at our financial institutions. Consumers have had the ability to pay bills, view their balances, and transfer funds for several years. Similarly, many patient portals already have core functionalities in place including viewing test results and visit summaries, viewing and refilling medications, viewing and making appointments, accessing educational materials, and sending secure messages to providers.

With this core functionality in place, the future of patient portals promises an expansion of services offered as technology advances. Patients may have the option to edit their doctor's notes and even share data from their medical devices and apps with their providers. The patient portal is a useful tool for the Internet of Things in healthcare, with the patient at the center of it all. In essence, the patient portal provides a gateway to a world in which personal health data gets big, gets shared, and ultimately gets results with the potential to improve patient satisfaction and health outcomes.

The authors envision a few possible use cases; the reader may be able to think of others.

As patient portals become a tool that most consumers become familiar with, healthcare organizations will start using it more for virtual healthcare delivery. Some organizations are slowly introducing the concept of providing remote healthcare services for non-acute care conditions. Linking the patient portal or portions of the patient portal to the virtual healthcare provider may allow better communication to the provider of the patient history. Patients who desire healthcare "on demand" will be more inclined to share their health history electronically with providers.

Another potential use of the patient portals may be better monitoring of chronic conditions. Patients who have diabetes may record their glucose measurements in their patient portal and results could automatically be uploaded to their health record for the provider to view. Should adjustments be needed to treatment based on those results, communication could be done electronically allowing for more timely management of the disease.

Consumers will ultimately become the driver for the information that is made available to them as well as their healthcare providers. They will have the ability to update their record of self-monitored data or other designated elements of their health record. The patient portal presents the ability to increase consumer engagement and its use will be a key to delivery of healthcare in many circumstances.

As with any new technology, adoption is one of the major challenges faced by healthcare providers. Again, we can learn from how other industries have approached this challenge. Adoption of electronic financial portals, for example, has been widespread across various demographics and age groups because they promise convenience, automation, and privacy and security of sensitive information. In fact, the companies who have the most successful adoption listen to their customers and ensure that the user experience of the product is optimized. User experience is one of the key drivers behind the adoption of new technologies. Because of this, patient portals should be continuously reviewed and updated to sustain a user interface that is well structured, cohesive, and easy to understand.

Personalization and globalization are among the trends shaping today's healthcare industry, and patient portals provide the healthcare industry a mechanism to truly innovate the patient experience. With issues such as language barriers, racial/ethnic disparities, and generational differences to overcome, future patient portals should be designed to meet the healthcare needs of specific patient populations. Healthcare providers must seize the opportunity to engage their patients in ways that differentiate themselves from their competitors in the marketplace.

NOTES

1. Needle, Sheldon. “EMR Patient Portals.” CTS Medical Blog, December 1, 2012. http://www.ctsguides.com/medical/emr-patient-portals/.
2. Health Information & the Law Project. “Who Owns Medical Records: 50 State Comparison. Health Information and the Law.” 2012. http://www.healthinfolaw.org/comparative-analysis/who-owns-medical-records-50-state-comparison.
3. Stratton, Bridget. “Taking Ownership of Patient Engagement.” AHIMA press release, October 29, 2013. www.ahima.org.
4. Terry, Ken. “Patient Portal Explosion Has Major Health Care Implications.” IHealthbeat, February 12, 2013.
5. Tuttle, Kate. “Patient Portals–7 Features the Market is Demanding.” Healthcare Industry Trends blog, April 22, 2015. https://blogs.perficient.com/healthcare/blog/2015/04/22/infographic-7-features-of-a-market-driven-patient-portal/.
6. Terry, Ken. “Five Trends for Healthcare CIOs in 2014.” *Information Week*, December 23, 2013. http://www.informationweek.com/healthcare/mobile-and-wireless/5-trends-for-health-cios-in-2014/d/d-id/111313.
7. Baldwin, Kevin, et al. “Implementation and Management of Patient Portals” *Journal of AHIMA* 86, no. 4 (April 2015): 50–55. http://bok.ahima.org/doc?oid=107601.
8. Ibid.
9. Venditto, Gus. “Patient Portals Pose New Security issues.” *Healthcare IT News*, October 29, 2013. www.healthcareitnews.com/news/patient-portals-pose-new-security-issues.
10. Eramo, Lisa A. “Patient Portals: Express Lane on the Health Information Highway.” *Journal of AHIMA* 83, no. 9 (September 2012): 24–28. http://bok.ahima.org/doc?oid=105665.
11. AHIMA. “Breach Management Toolkit.” 2014. http://bok.ahima.org/doc?oid=300305.
12. AHIMA. “Release of Information Toolkit.” 2013. http://bok.ahima.org/doc?oid=106371.
13. HealthIT.gov. “What are the differences between electronic medical records, electronic health records, and personal health records?” https://www.healthit.gov/providers-professionals/faqs/what-are-differences-between-electronic-medical-records-electronic.
14. Department of Health and Human Services. “Administrative Data Standards and Related Requirements: Security and Privacy: Uses and Disclosures for Which an Authorization Is Required.” Code of Federal Regulations, 2002. 45 CFR, Part 164, Section 508.
15. Department of Health and Human Services. “Administrative Data Standards and Related Requirements: Security and Privacy: Security Standards for the Protection of Electronic Protected Health Information.” Code of Federal Regulations, 2003. 45 CFR, Part 164, Section 308-312.
16. AHIMA. “Security Risk Analysis and Management: An Overview (Updated).” *Journal of AHIMA* 84, no. 11 (November–December 2013): expanded web version. http://bok.ahima.org/doc?oid=300266.
17. CMS.gov. Frequently Asked Questions. https://questions.cms.gov/faq.php?faqId=7735.
18. HealthIT.gov. “Patient Ability to Electronically View, Download & Transmit (VDT) Health Information.” https://www.healthit.gov/providers-professionals/achieve-meaningful-use/core-measures-2/patient-ability-electronically-view-download-transmit-vdt-health-information.
19. Department of Health and Human Services. “Security and Privacy: Privacy of Individually Identifiable Health Information: Uses and disclosures of protected health information: General rules.” Code of Federal Regulations, 2000. 45 CFR 164.502 (g)(3)(i).

REFERENCES

Sherek, Penny D, and Emmlee Gray. “Case Study: Managing Pediatric Health Information in a Patient Portal.” *Journal of AHIMA* 85, no. 4 (April 2014): 46–47.

AHIMA. “The Implementation and Management of Patient Portals.” *Journal of AHIMA* 86, no. 4 (April 2015): 50–55.

Office for Civil Rights. “Personal Health Records and the HIPAA Privacy Rule.” http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/healthit/phrs.pdf.

SECTION VII: APPENDICES

APPENDIX A

ABC Healthcare Organization

Sample Patient Portal Registration Form

The patient portal provides secure online access to portions of your Medical Record.

Patient Name: ______________________________ **Date of Birth:** ____________

(if patient is under the age of 16 parent/guardian must be listed)

Parent/Guardian *(if applicable)*: ____

E-mail Address:__________________________

(For user information and notification purposes only)

By signing and dating this form, I am authorizing ABC Hospital to create a patient portal Logon ID and password for the patient listed above. I understand that this information will be e-mailed to me within three business days at the e-mail I have given above.

Signature:__________________________________ **Date:** ________________

- -

Hospital Portal Information

Once the registration form is completed and returned to the Health Information Management (HIM) Department, you will receive an e-mail with a link to the patient portal (within three business days). This will include your one-time login ID and one-time password information. Please make sure you check your bulk, junk or spam e-mail, because it may have filtered there. Once you receive your one-time logon ID and one-time password, please follow the prompts. Copy and paste your one-time user ID and password into the fields. You will then be prompted to create a new user name and password. You will need to read and accept the Terms and Conditions of the patient portal before it can be accessed.

Whenever a new item is posted to your patient portal, such as results, reports, appointments etc., you will receive an e-mail notification. There will be a link at the bottom of the e-mail directing you to the portal log-in screen. No health information is relayed in any e-mail. All e-mail addresses will be kept confidential and will not be used for marketing or solicitation.

Go to www.ABC.com to access your portal or learn more about the patient portal.

OFFICE USE ONLY: ID Verified: ______________ Date Received: ______________

Date Completed: ________ Initial: ______

APPENDIX B

ABC Healthcare Organization

Sample Policy and Procedure: Patient Portal Registration/Access

POLICY STATEMENT

ABC Healthcare Organization's policy is to engage patients and their authorized proxies by providing an electronic option for timely and convenient access to their health information.

INTENT

The purpose of this policy is to define the terms for releasing medical record information through the patient portal. ABC Healthcare Organization will provide a method in which patients or legal representatives request access to the patient portal.

DEFINITIONS

a. **Authentication:** The act of completing, signing, dating, and timing a document or entry to the medical record by the author or, if the author requires clinical supervision, the supervising physician of the author.

b. **Care Provider:** An individual who provides medical treatment or care to a patient within his or her scope of practice and who, in accordance with ABC Healthcare Organization policy, may document care or treatment in the medical record for that patient.

c. **Meaningful Use:** Requirements under the Health Information Technology for Economic and Clinical Health (HITECH) Act for eligible healthcare professionals and hospitals to qualify for Medicare and Medicaid incentive payments upon adoption of certified electronic health record technology that meets mandated measureable objectives.

d. **Minor Proxy:** Legal parent or guardian of a minor patient authorized by ABC Healthcare Organization policy to access a minor patient's medical records. Proxy access will be automatically deactivated when the patient reaches the age of ___. *(Note: Refer to specific state laws for appropriate age.)*

POLICY

1. For the patient's benefit and convenience, access to the patient portal shall be provided within the parameters established by this policy.
2. Except as restricted pursuant to this policy, an electronic view of portions of a patient's medical record shall be provided through the patient portal.
3. A certified copy of the record for legal purposes will be obtained through a separate process in the health information management (HIM) department and will not be provided via the patient portal.
4. To provide greater protection for sensitive records (e.g., substance abuse, mental health, HIV), such as documentation by providers or for records that have been specifically flagged by the provider as "Confidential," such records will not be accessible through the patient portal. The patient or proxy will be directed to the HIM department for release of such records.
5. Adult Patient Access (patient 18 and older)
   a. The Patient Portal Registration Form (Appendix A) must be completed and verification of picture identification documented.

   b. Patient will be registered for the patient portal access in the EHR and receive an invitation via the e-mail address provided on the form.

   c. The Patient Portal Registration Form must be forwarded to the HIM department to be scanned to the patient's record.

6. Minor Proxy Access

   a. Minor proxy access can be requested by completing the Proxy Request Form.

   b. Picture identification must be verified and documentation of verification must be noted on the Proxy Request Form.

   c. Proxy Request Form must be forwarded to the HIM department for approval and scanning into the patient's medical record.

   d. Once approved, the parent or legal guardian will be set up in the EHR and receive an invitation via e-mail address provided on Patient Portal Registration Form.

APPENDIX C

ABC Healthcare Organization

Sample Patient Portal User Agreement

Policy and Procedures and Patient Agreement to Abide by Terms of Use
The ABC Healthcare Organization patient portal offers secure viewing and communication as a service to patients who wish to view parts of their records online. Secure messaging can be a valuable communications tool, but has certain risks. By signing the agreement to abide by the terms of use, you accept the risks and agree to follow terms of use, as described below.

I. Terms of Use General Policies and Procedures

DO NOT use the patient portal to communicate (i) an emergency, (ii) an urgent issue or (iii) sensitive information (e.g., HIV, mental health, work excuses, etc.)

Recommended Subject Matter:

- Use the patient portal for non-urgent medical portal related questions, lab results, select reports, appointment reminders, or requests.
- Use the patient portal to update your demographic information.
- Be sure that all information that you enter is true, accurate, complete, and updated whenever there is a change.
- Be concise when typing a message.

The patient portal offers the following functions *(list will vary by organization)***:**

- View lab results.
- View, download, print, and/or transmit your protected health information
- View and submit updates to your health information.
- View your home medications list entered by your physician or clinical staff during a past hospital admission
- View selected health information (allergies, medications, current problems, past medical history), view hospital appointments.
- Update your demographic information (i.e., address, phone numbers, etc.)

Communications May Become a Part of the Health Record
Communication via the patient portal may be included in your permanent health record.

Privacy:

- All messages sent to you in the patient portal will be encrypted. See section "Terms of Use patient portal guidelines and security" for explanation.
- E-mails from you to any staff member should be through the patient portal or they are not secure.
- All e-mail address lists will be kept confidential and such lists will not be shared with other parties, unless necessary to carry out patient portal operations (e.g. perform system upgrades to the portal) or required by law.
- A variety of healthcare and administrative personnel (such as nurse practitioners, physician assistants, registered nurses, certified medical assistants, clerks, etc.) will be involved in reading, processing, and replying to your messages and information submitted through the patient portal (similar to how phone communication is handled). There is no need to notify us that you have read a message, unless you have a question or need further information.

- Read our HIPAA notice of privacy practices brochure for information on how private health information is handled in our facility. The notice of privacy practices can be viewed, printed, or downloaded at www.ABChospital.com.
- If you have any concerns, please contact the patient portal Support Line at 123-456-7890 or e-mail at patientportal@ABChospital.com.

Response Time:

- After signing your agreement to abide by the patient portal terms of use, a "Welcome E-mail" will be sent to you. This will provide a link to the portal login screen. If you have not received an e-mail from us within three business days, please contact patient portal support line at 123-456-7890. We will return messages within one business day, but no later than three business days, after receipt.
- Reasonable efforts will be made to respond to e-mail and telephone inquiries within one business day, but no later than three business days, after receipt. Response time may be longer if the patient portal service is interrupted for maintenance, upgrades, or emergency repairs related to events beyond our control. In this respect, you agree not to hold ABC Healthcare Organization Inc., its physician practices, physicians, providers or any of its staff, in any way liable or responsible to you for such modification, suspension, or disruption of the patient portal.
- The patient portal support normal hours of operation are 9 a.m. to 4 p.m. Monday through Friday. You are encouraged to use the patient portal at any time; however, e-mail and telephone messages submitted after hours will receive a response the next business day.
- If e-mail is not accessible for any reason, please contact patient portal support line at 123-456-7890. We will return messages within one business day, but no later than three business days, after receipt.

Medical Advice and Information Disclaimer

The patient portal may from time to time include information posted by ABC Healthcare Organization in the form of news, opinions, or general educational materials that should not be construed as specific medical advice or instruction from ABC Healthcare Organization. The information posted by ABC Healthcare Organization on the patient portal should not be considered complete, nor should it be relied on to suggest a course of treatment for a particular individual. You should always seek the advice of your physician with any questions you may have regarding a medical condition.

II. Terms of Use Patient Portal Guidelines and Security

Security

The patient portal is a webpage that uses encryption and other security measures designed to keep unauthorized persons from reading communications, information, or attachments. Secure messages and information are designed to be read only by the patient or other authorized individual.

At the time of patient portal enrollment, you may be asked for documentation and/or a request to answer knowledge-based authentication questions to prove that you are who you say you are. This is meant to ensure the privacy of your health information.

Availability of the Patient Portal

Access to this secure patient portal is an optional service, and may be suspended or terminated at any time and for any reason. If service is suspended or terminated, we will notify you promptly, no later than three business days.

Enrolling in the patient portal program:

Request access from ABC Healthcare Organization. To register you must be at least ____ years old. *(Note: Refer to specific state laws for appropriate age.)*

1. Review the patient portal user agreement and electronically submit the agreement by clicking Accept. **Note: If enrolling electronically by selecting "Accept" you are indicating that you have read and fully understand the user agreement, therefore creating an electronic signature of acceptance.*

2. If enrolling in person, please sign and bring in the completed agreement to abide by the patient portal terms of use.
3. After Agreement to Abide by the Patient Portal Terms of use is completed or accepted, you can expect to see a "Welcome" e-mail. This e-mail will instruct you on how to complete enrollment and create login and password.
4. If enrolled by medical records, once logged into the portal, you should go to "Preferences" on the bottom of the page to change your password to something only you will know. This is essential to ensure your information remains secure and private.
5. After the above steps are completed you should be all set to use the patient portal.

Available Components:

Homepage: Allows you to view components of your health record.

Health Record: Allows you to view information entered into your electronic health record (e.g. allergies, lab results, radiology reports, medication lists, and visit history, etc.). These are available for you to review and check for accuracy as well as print for other physicians or to keep for your records. If needed, you may obtain a full copy of your electronic health record by contacting the health information management (HIM) department at 123-456-7890. **Note: If this portion is not complete, we still have the information. Not all portions of your health record will be made available for viewing via the patient portal.*

Medications: Allows you to view your current and past medications entered by your physician or other clinical staff.

Appointments: Allows you to view upcoming appointments. The appointment section **does not** include appointments you may have at another facility or private practitioner's office.

Profile: Contains your personal contact information and insurance information. Allows you to view and request changes to your information.

Additional components may be available in the future.

Protecting Your Private Health Information:

You should protect your patient portal login information and notify us immediately of any unauthorized use of your login information or if you believe that your login is no longer confidential.

Refer to our notice of privacy practices for additional information.

APPENDIX D

ABC Healthcare Organization

Sample Proxy Request Form

This form must be completed by the patient and will be used to request access to your patient portal via proxy access. Proxy requests must be reapproved annually.

Patient information (individual requesting a proxy)
Do you currently have patient portal access? Yes / No

Name: ____ Date: ________________

Address: ____

Phone Number: __________________________ Date of Birth: _______________________

E-mail Address: ____

a. Please list all persons that you are allowing to view your patient portal via proxy access. You will need to complete all of the information below before proxy access can be granted. You may at any time revoke the proxy access by contacting (ABC Hospital at 123-456-7890) and filling out the proxy revocation form. Your designated proxy will have access to your patient portal records until that time. By signing the form below, you understand that records accessed by your proxy maybe be re-disclosed without your knowledge and are no longer protected by state or federal privacy regulations. You further understand that information in the patient portal may include treatment and testing regarding drug/alcohol abuse, mental health, HIV status, genetic testing and reproductive medicine. If you are requesting proxy access for a minor child, proxy access will automatically terminate when the child turns ___ years old or becomes legally emancipated. (Note: Refer to specific state laws for appropriate age.)

Proxy Name	Date of Birth	Relation to Patient	Proxy's e-mail address	Patient Signature (Parent/Legal Guardian if Patient Is a Minor or Legal Representative)	Date

OFFICE USE ONLY: ID Verified: _______________ Date Received: _______________

Date Completed: __________ Initial: ________

APPENDIX E

ABC Healthcare Organization

Sample Proxy Revocation Form

This form must be completed to revoke proxy access to your patient portal.

Patient information:

Name: ____ Date: ________________

Address: ____

Phone Number: __________________________ Date of Birth: _______________________

E-mail Address: ____

Please list all persons that you are revoking access to view your patient portal via proxy access. Please allow one business day after submission of this revocation request to health information management before the access is deactivated. The designated proxy individuals listed below will no longer have access your patient portal records. By signing this form you understand that any records previously accessed by your designated proxy maybe released by them and may no longer be protected by ABC Hospital.

Proxy Name	Date of Birth	Relation to Patient	Proxy's e-mail address	Patient Signature (Parent/Legal Guardian if Patient Is a Minor or Legal Representative)	Date

OFFICE USE ONLY: ID Verified: _______________ Date Received: _______________

Date Completed: __________ Initial: ________

APPENDIX F

ABC Healthcare Organization

Sample Patient Portal Information Sheet

ABC Healthcare Organization offers access to the patient portal as a courtesy to our patients. The patient portal is a secure web-based tool that provides patients the ability to access their health information online and communicate with their healthcare team. This handout is intended to inform you of the facts and risks surrounding the use of the patient portal.

1. The patient portal provides electronic access to a portion of your medical record, such as medical history, medications, most lab results and other medical reports. Certain lab results that may be considered to be of sensitive nature may not be viewable in the portal.
2. The patient portal allows non-urgent communication with physicians' offices via secure messaging.
3. The patient portal is not a replacement for a clinical visit. It is not appropriate to use this portal for emergency diagnosis or treatment.
4. Patient enrollment is by request at any registration desk or in the health information management department located in the hospital. After the initial registration, you will be sent an e-mail confirmation invitation that requires response within 90 days. You will be asked to create a unique username and password for the portal. These steps are all required to complete your registration and to access the patient portal.
5. Patient and proxy (having authority to represent someone—substitute or additional) access:
   a. Patient's age ____ to ____: No access for the child or parent/legal guardian. *(Note: Refer to specific state laws for appropriate age.)*

   b. Patient's age ____ or older: May have own access and may grant proxy access to any other adult(s). *(Note: Refer to specific state laws for appropriate age.)*

   c. Patient's age 0 to ____: No access for the child. Only the parent(s)/legal guardian is allowed access as a proxy. *(Note: Refer to specific state laws for appropriate age.)*
6. The patient or legally authorized representative must complete and sign the patient portal access form to enroll in the patient portal, to authorize proxy access, or to revoke proxy access.
7. The health information management department is responsible for handling all requests to revoke proxy access and can be reached at (telephone number).
8. Use of shared e-mail accounts (i.e. Thejoneses@e-mailprovider.com) for portal access is allowed, although not recommended. All persons sharing an e-mail account and password will have access to the patient's health information via the portal. You will need to notify the health information management department if you would like to unlink an e-mail address from your portal account.

Responsibilities of Patient Portal Users

You are responsible to protect the confidentiality of your username and password, as well as the health information you access using the portal. Healthcare organization is not liable or responsible for misuse of your password or username. If you suspect that someone has learned your password, you should access the portal site immediately and change it. If you become aware of an issue or concern, for whatever reason, of this confidentiality, please promptly report it to the privacy officer at (telephone number). If you, for whatever reason, gain access to another person's health records, you agree to not access, use, disclose (e.g., read or print) the information in any manner and agree to report the issue immediately to the privacy officer by calling (telephone number).

APPENDIX G
ABC Healthcare Organization

Sample Patient Portal FAQs

Welcome to the ABC Hospital Patient Portal

The patient portal provides secure online access for ABC patients.

You will be able to:

- Access lab results, provider reports, and radiology reports
- Review upcoming appointments
- View your personal medical records (i.e., immunization history, medication list, allergy list)

The portal will be expanded in the future to include additional functionality.

Frequently Asked Questions:

1. **What do I need to do first?**

   Download and print the patient portal authorization form. Forms are also available at every physician's office. You can also go to the hospital website and use the online registration.

2. **What do I do with my form after I filled it out?**

   You can drop it off at any of our office locations or mail it directly to ABC Hospital at 123 Main Street, Main Town, State 12345.

3. **What happens after I have submitted my form?**

   Please allow seven days for processing. You will receive an e-mail with a temporary password and a letter from the patient portal team.

4. **Who can sign up for patient portal?**

   We currently offer this option to our patients ages ____ and older. (*Note: Refer to specific state laws for appropriate age.*)

5. **What if both my spouse and I want to sign up, but we only have one e-mail address?**

   You need to know that messages will be sent to the e-mail provided, user name and password, as well as notifications that information on your portal has been updated. It is your responsibility to provide us with a secure e-mail address that can be used for those types of messages.

6. **How do I sign on and access the patient portal?**

   The patient portal is used only by patients who have been enabled by the hospital to access the system. The features available for the patients depend upon the settings established by the healthcare organization.

7. **How do I use the patient portal after logging in?**

   After logging in, as a patient, you will see the hospital's customized patient portal home page. There you can access information, ask medical or administrative questions of the practice, receive reminders from the practice, and review specific documents, results, and reports regarding your healthcare.

8. **What if I don't remember my user name?**

   You will need to call the patient portal team at 123-456-7890 to request that your account be reset. It is recommended that you confirm your e-mail address with the team member as they will send you an e-mail with your user name.

9. **What if I don't remember my password?**

   You can reset your own password from the portal website by following the instructions and answering security questions.

10. **What happens if my account is locked out?**

    You are allowed three attempts to successfully log into the patient portal. After the third failed attempt, for your protection, your account will be locked out. You will need to call the patient portal team at 123-456-7890 to request that your account be reset. It is recommended that you confirm your e-mail address with the team member as they will send you an e-mail with your new password.

11. **Why are there no lab results when I select a certain lab test?**

    In general, lab tests and x-ray orders will be published if the results were received on or after September 1, 2011. Tests before that date were not formatted for the patient portal system. Lab results are available within 24 hours of the test being resulted.

12. **Why are reports not available when I select the visit?**

    Radiology and provider notes are available 36 hours after the provider has signed the report.

13. **What if I notice something is not correct on the portal, such as allergy medication?**

    You should contact your provider.

14. **Do you have a question?**

    If you have additional questions, please call patient portal support at 123-456-7890 or contact us by e-mail at portal@ABCHealthcarePortal.com.