Coverys Risk Management

Ambulatory Care Manual

Communication: Electronic

What's the Risk?

Electronic communication is a modern-day phenomenon that relies on computer and internet technology to transmit digital information such as text, sound, and images over high-speed networks via electronic devices. Computer and mobile device technology has advanced significantly over the years to the point where our society now relies on the conveniences these devices offer. As of June 2019, 96% of American adults had a cellphone, while 81% had a smartphone.[1]

Today's high-speed internet and electronic devices make it possible for consumers and healthcare practitioners to access programs and apps on both stationary and mobile devices and to communicate via email, text, and social media. Clinical apps and software enable healthcare practitioners to research, review, and document clinical information; electronically order treatments and medications; and communicate with patients and other practitioners, both inside and outside of healthcare and office practice settings. Electronic patient portals enable patients to communicate with practitioners, access online health information to make informed decisions about their care, and share their clinical information with multiple healthcare practitioners and personal caregivers.

While computer technology, electronic devices, and software offer convenience, easy access to information, and flexibility, healthcare practitioners must be aware of the potential for risks, which include:

- Security or privacy breaches related to transmission of protected health information (PHI) over unsecured or unencrypted devices.
- Identity theft.
- Personal information theft (PHI, financial, demographic details, etc.).
- Equipment or software failure interrupting access to health information and the software used to review, document, and transmit health information.
- Communication delays and interruptions caused by:
    - Equipment failure and connectivity issues.
    - Insufficient power sources.
    - Unreliable or lost internet or Wi-Fi signals.
- Distractions in the clinical setting and during patient care.
- Public messages on social media that expose patient complaints and grievances, inappropriate communications, or PHI.

This document is a work product of Coverys' Risk Management Department. This information is intended to provide general guidelines for risk management. It is not intended and should not be construed as legal or medical advice. Your organization should add to and modify this tool to address the compliance standards and regulations applicable in your state or organization.

The links included in this document are being provided as a convenience and for informational purposes only; they are not intended and should not be construed as legal or medical advice. Coverys Risk Management bears no responsibility for the accuracy, legality or content of the external site or for that of subsequent links. Contact the external site for answers to questions regarding its content.

Updated: October 2020

COVERYS

- Threats to data security and integrity caused by hackers, viruses, or malware.
- Lost or stolen data and PHI stored on mobile devices such as laptops, tablets, and cellphones/smartphones.
- Inappropriate use of portals for communicating urgent/emergent clinical information.

When Is This Risk an Issue?

The following highlights various risk issues associated with electronic communications.

Basic Requirements for Electronic Communication

Electronic communication relies on several factors, including device type, power source, and signal used to transmit the communication. All electronic devices must have a reliable power source or charge in order to operate. Successful connectivity and transmission of a call or message completely depend upon an adequate internet or Wi-Fi signal. Weak or interrupted Wi-Fi and internet signals can contribute to failed or disconnected calls and the inability to transmit emails or text messages in a timely manner. Mobile devices rely on an electrical charge in order to operate and can shut down whenever the battery is drained, unexpectedly interrupting urgent communications and creating the potential for harm.

Internet Access

Internet connections are required when emailing and communicating via patient portal. These connections can become vulnerable if the proper security settings are not in place. Use of unencrypted or private email accounts can contribute to security and privacy risks.[2] While HIPAA does not prohibit the use of unsecured, unencrypted email when communicating patient information, using unsecured or unencrypted email can create the potential for breaches.

Furthermore, the internet can be a vehicle for phishing emails or scams. It is important to educate staff to recognize suspicious emails or phishing attempts that could potentially infect a computer or mobile device with malware if a user unknowingly clicks on an infected link or attachment within the email. Using secure, encrypted email reduces the risk of a breach.

Unlimited internet access also makes it possible for staff to access personal email accounts and unsecure sites. Aside from security risks, open internet access can create distractions. Establishing a policy or permissions for limited internet access may be helpful to minimize personal email and internet usage during office hours.

Electronic Devices and Data

Computers, mobile devices, and other means of electronic messaging introduce a wide range of communication opportunities, but also pose significant risks. These risks include security, confidentiality, and timeliness concerns. According to the National Cybersecurity Center of

Excellence (NCCOE) and the National Institute for Standards and Technology (NSIT) within the Department of Commerce, healthcare practitioners increasingly use mobile devices to receive, store, process, and transmit patient clinical information, and many practitioners are using mobile devices for healthcare delivery before they have implemented safeguards for privacy and security. Compromised mobile devices enable hackers to access the healthcare organization's network. In addition, untrusted networks may use a man-in-the-middle strategy to obtain credentials to access an enterprise's network, and interacting with other systems increases a healthcare worker's risk of compromising routine operations.[3]

While mobile electronic devices offer a wider range of communication options, they are not always appropriate for PHI. Both the Centers for Medicare & Medicaid Services and The Joint Commission advise against using texting for transmitting orders and only allow texting of patient information if supported by a secure platform. Mobile devices used for social media, instant messaging, and texting can also pose significant risks for breaches in confidentiality and can create situations that violate patient rights. The Joint Commission strongly urges all organizations to draft a social media abuse policy and train employees accordingly. Additionally, mobile devices are not usually preloaded with antivirus software or malware protection, leaving them at risk for viruses and intrusions that can compromise security and result in data theft and loss. For further information, please see ***HIPAA Privacy*** and ***HIPAA Security***.

Two Types of Electronic Communication

When using electronic devices, communication can be synchronous or asynchronous. Synchronous communication occurs in real time and supports mobile face-to-face and cellphone communications, telecommunication devices for the deaf (TDD), and video conferencing. Synchronous communication may be used for high-stakes, time-sensitive interactions that require action or decision-making. Synchronous communication may also be useful in situations requiring supervision or clarification, or when handling urgent matters.

Asynchronous communication is sometimes referred to as "store and forward." It includes delayable forms of electronic communication such as texts, email, voicemail, and portal messages. Asynchronous communication is useful for simple messages that are not time-sensitive, but should never be used for emergent, urgent, or complex communications.

Various risks are also associated with the following forms of electronic communication.

Communicating by Email With Patients

According to the HIPAA Privacy Rule, 45 C.F.R. Section 164.522, patients have the right to request and have a healthcare practitioner communicate with them by email. Email can be useful to facilitate communication between a practitioner and patient under the right circumstances. All methods of communication, whether electronic, virtual, telephonic, or face-to-face, should be appropriate to the patient's clinical need and the information being conveyed.

This document is a work product of Coverys' Risk Management Department. This information is intended to provide general guidelines for risk management. It is not intended and should not be construed as legal or medical advice. Your organization should add to and modify this tool to address the compliance standards and regulations applicable in your state or organization.

The links included in this document are being provided as a convenience and for informational purposes only; they are not intended and should not be construed as legal or medical advice. Coverys Risk Management bears no responsibility for the accuracy, legality or content of the external site or for that of subsequent links. Contact the external site for answers to questions regarding its content.

Communication: Electronic

When email is used, special concerns about privacy and confidentiality must be considered, particularly when communicating sensitive information. When physicians engage in electronic communication, they hold the same ethical responsibilities to patients as they do during other clinical encounters.

Oftentimes, patients’ personal email accounts are not encrypted or secure. Patients may be unaware of potential risks associated with using unencrypted email. Additionally, some states require patient consent to use or disclose health information, including information transmitted by email. Email is also available via patient portals and allows practitioners and patients to communicate securely. However, because email is asynchronous, communicating via the portal can potentially create life-threatening delays if patients use the portal to report urgent or emergent information. Instructing patients to communicate urgent clinical concerns directly to the office by phone rather than email can deter inappropriate portal use.

Communicating by Email With Practitioners

Aside from communicating with patients, practitioners may also communicate with other healthcare practitioners regarding patient care and treatment and may use email to transmit electronic PHI (ePHI).

Email as Documentation

Whether the email was sent to or received from a patient or another practitioner, care-related email communication is a record of care. Maintaining this documentation in the medical record demonstrates continuity of care and the rationale for treatment recommendations. Email communication documentation that is incomplete or missing can negatively affect patient care. Email communications related to patient care should be filed in the medical record. Additionally, email retention rules must be followed since email communications are considered part of the patient record.

Texting

Mobile devices introduce a wide range of communication opportunities, but also pose significant risks, including:

- Security breaches.
- Confidentiality breaches.
- Timeliness concerns.

Mobile devices are not always appropriate for PHI. Texting on a mobile device or a social media and instant messaging platform can pose significant risks of confidentiality breaches. For further information, please see ***HIPAA Privacy*** and ***HIPAA Security***.

This document is a work product of Coverys’ Risk Management Department. This information is intended to provide general guidelines for risk management. It is not intended and should not be construed as legal or medical advice. Your organization should add to and modify this tool to address the compliance standards and regulations applicable in your state or organization.

The links included in this document are being provided as a convenience and for informational purposes only; they are not intended and should not be construed as legal or medical advice. Coverys Risk Management bears no responsibility for the accuracy, legality or content of the external site or for that of subsequent links. Contact the external site for answers to questions regarding its content.

Communication: Electronic

Faxing

Faxing can be a good way to share information, as long as the sender takes care to ensure that the information reaches the intended recipient. While some patients may have fax machines or computers that allow fax transmission to or from their homes, faxing is generally used to transmit information between offices and business associates. Additionally, dialing an incorrect fax number could result in information reaching an unintended recipient. Including a fax cover sheet with instructions to contact the practice if the fax was received in error can be protective and help determine if a breach occurred.

Alternately, most fax machines can generate records of successfully sent documents, including page counts, date, and time, and can also help signal if not all pages were sent. Typically, it is helpful when sending faxes to have a name and phone number for the intended recipient to ensure the fax was received in its entirety. This helps guard against delays and minimizes the chances for incomplete faxing and missing information that might be needed to coordinate care.

Faxing is subject to the same HIPAA requirements that apply to all other information exchanges (oral, paper, and electronic) between covered entities. For more information on permitted uses and disclosures for healthcare operations between covered entities, please see Permitted Uses and Disclosures: Exchange for Health Care Operations, 45 Code of Federal Regulations (CFR) 164.506(c)(4).[4]

Communicating Information on Practice Websites

Given the exposure provided through the internet, many medical office practices create websites as part of their business operations. Websites attract new patients, describe services, and provide access to educational information about relevant health-related topics. They also allow practices to post locations and hours of operation, introduce the practitioners, list professional credentials, as well as provide any professional recognition or certifications granted to the practice. Some websites provide interactive links for scheduling appointments, making payments, and providing access to patient portals.

Websites require continual monitoring and upkeep to ensure security and to maintain accurate and current content. False or inaccurate information can lead to allegations of false advertising or to regulatory challenges. Accepting a free website in exchange for referring patients, prescribing a pharmaceutical company's medications or products, or granting other similar favors is discouraged as this could represent a conflict of interest and violate other corporate compliance rules. Some practices may use their website to sell health-related products and services. Additionally, a website offering purchase or payment options will require processing of financial transactions and shipping information. Financial transactions, including credit card information, are at risk of being hacked.

This document is a work product of Coverys' Risk Management Department. This information is intended to provide general guidelines for risk management. It is not intended and should not be construed as legal or medical advice. Your organization should add to and modify this tool to address the compliance standards and regulations applicable in your state or organization.

The links included in this document are being provided as a convenience and for informational purposes only; they are not intended and should not be construed as legal or medical advice. Coverys Risk Management bears no responsibility for the accuracy, legality or content of the external site or for that of subsequent links. Contact the external site for answers to questions regarding its content.

Website content and activities may be regulated by a number of federal agencies, including the Federal Trade Commission (advertising in general) and the Food and Drug Administration (advertising related to regulated medical devices/products). Individual states may also have applicable regulations, particularly when practices use their website to sell health-related products and services. Finally, if the website collects patient information such as appointment requests, pre-visit health questionnaires, or medical history forms, it is essential that this be done in a secure manner that is consistent with HIPAA security requirements. Please see ***HIPAA Security*** for additional information.

Messaging Through Patient Portals

Portals allow the practice to more closely monitor patients at risk because of personal or family history, chronic illness, recurrent symptoms, or other factors. Patients value the sense of partnership created with practitioners when they can access their health information and have the ability to confirm or check information relayed during the clinical encounter.[5] They become more engaged in their care.

Having patients communicate any clinical concerns directly to the office by phone rather than the portal can deter inappropriate portal use. Establishing compatible expectations for practitioners and patients regarding communication and information sharing via the portal ensures patient safety. Providing patient education materials and defining safe portal use can help mitigate risks.

When using the portal to communicate test results, a new diagnosis, or a care plan change, it is important to remember that patients may not receive messages on a timely basis. Simply offering a patient portal will not ensure that patients will use it. According to the Office of the National Coordinator for Health Information Technology (ONC), a portal must be engaging and user-friendly in addition to supporting patient-centered outcomes. The portal must also be integrated with clinical encounters so the care team can use it to convey information, communicate with patients, and support self-care and decision-making.[6]

A portal user agreement is an essential component of implementing a portal. Patients have the right to accept or refuse to access information and communicate via a portal and generally must register to use it. While a patient portal has many benefits, it also includes associated risks, such as privacy and security breaches, inappropriate patient use, delays, and the possibility of the patient and/or practitioner developing unrealistic expectations. Furthermore, portal communication is asynchronous and therefore inappropriate for emergent or urgent information. Many of these risks can be mitigated through education, implementation of a secure portal, and effective policies and procedures. Additionally, patient portals must comply with HIPAA Security rules. See ***HIPAA Security*** for more information.

Communicating via Social Media

Physician practices often use social media to gain a presence and keep their name in the public eye. In theory, social media offers the practice an opportunity to advertise and gain exposure, but the benefits of social media for both physicians and patients must be weighed carefully. For instance, if a medical practice has a Facebook page or uses Twitter or another social media platform to communicate with patients and nonpatients, it is important for the practice to maintain the same professional and ethical standards in social media comments and responses that it would use with any other form of communication.

The Federation of State Medical Boards notes that physicians have been reported to licensing authorities for unprofessional interactions via social media and for online communications such as inappropriate contact with patients, inappropriate prescribing, misrepresentation of credentials, and unsubstantiated clinical outcomes resulting in serious disciplinary actions.[7] The growing concerns about physician social media use and the potential for compromised patient identity based on posted comments underscore the need for physician practices to have social media policies.

Other risks associated with social media use include violations of staff privacy, publicly voiced employee grievances, damage to the practice's reputation, legal or regulatory violations, public disagreements, bullying, and complaints. Social media platforms can also serve as a venue for current and former employees, patients, or family members to voice complaints or post negative comments about the practice, its staff, and patients.[8]

For more information on handling negative social media posts, see ***Patient Relations***.

How Can I Reduce Risk?

It is incumbent upon practitioners to implement systems that will ensure, to the fullest extent possible, easily accessible communication and secure, confidential patient information.

Adhere to Basic Requirements	
Start with basic requirements	• Connect all devices and related equipment to an appropriate and reliable power source for continuous function and operation. • Consider installing a backup power source to ensure continuous operation during power outages. • Inspect hardwired connections to ensure they are intact and operational. • Connect wireless equipment to a secure Wi-Fi network and ensure that all electronic devices

This document is a work product of Coverys' Risk Management Department. This information is intended to provide general guidelines for risk management. It is not intended and should not be construed as legal or medical advice. Your organization should add to and modify this tool to address the compliance standards and regulations applicable in your state or organization.

The links included in this document are being provided as a convenience and for informational purposes only; they are not intended and should not be construed as legal or medical advice. Coverys Risk Management bears no responsibility for the accuracy, legality or content of the external site or for that of subsequent links. Contact the external site for answers to questions regarding its content.

Adhere to Basic Requirements

designated for wireless use can successfully access a signal.

- Educate staff on all new software programs installed.
- Ensure all devices and equipment function and operate properly.

Follow relevant policies and procedures

- Develop policies and procedures that define safe and appropriate use of electronic devices for secure and private communication.
- Ensure policies and procedures define acceptable use of work-related and personal electronic devices.

Ensure Safe Use of Electronic Devices

Develop a policy and procedures for mobile device use

- Ensure a backup power source is available to minimize service interruptions and maintain access to electronic information if power outages occur.
- Develop a policy addressing safe mobile device use by practitioners and staff members that covers at least the following:
  - Periodic risk assessments of mobile device use, including whether personal mobile devices are being used to exchange ePHI and whether proper authentication, encryption, and physical protections are in place to secure the exchange of ePHI.
  - Encryption and security breach protocols for mobile devices.
  - Encryption installation to protect ePHI stored or sent by mobile devices.
  - Security software protocols and installation schedules for regular updates.
  - Unique passwords or biometric authentication to verify the person using the mobile device is authorized to access ePHI.
  - Limits on file-sharing applications.
  - Preapproved mobile applications.
  - Wi-Fi security rules.

This document is a work product of Coverys' Risk Management Department. This information is intended to provide general guidelines for risk management. It is not intended and should not be construed as legal or medical advice. Your organization should add to and modify this tool to address the compliance standards and regulations applicable in your state or organization.

The links included in this document are being provided as a convenience and for informational purposes only; they are not intended and should not be construed as legal or medical advice. Coverys Risk Management bears no responsibility for the accuracy, legality or content of the external site or for that of subsequent links. Contact the external site for answers to questions regarding its content.

Updated: October 2020

COVERYS

Ensure Safe Use of Electronic Devices

- Define appropriate and safe use of mobile devices by clinicians and staff and provide education about relevant policies and procedures.
- Train clinicians and staff on how to safely access and share ePHI using mobile devices.

Ensure device safety and security

- Install firewalls to block unauthorized access.
- Install security software to protect against malicious applications, viruses, spyware, and malware-based attacks.
- Use radio frequency identification (RFID) tags on mobile devices to help locate a lost or stolen mobile device.
- Install and use remote shutdown tools to prevent data breaches when devices are lost or stolen.
- Disable or uninstall file sharing applications.
- Research and approve mobile applications before downloading.
- Ensure clinicians and staff understand risks of data breaches, HIPAA violations, and fines.
- Do not save unencrypted PHI on smartphones, tablets, or laptops.
- When smartphone access to the EMR is permitted:
  - Ensure mobile devices are fully encrypted through a virtual private network (VPN).
  - Ensure no PHI is downloaded and stored on the smartphone (for example, view-only access).
  - Do not use unencrypted texts or emails to exchange PHI, including digital images.
- Regularly update operating systems, anti-malware, and firewall applications on all mobile devices.
- Install GPS tracking software on all mobile devices. Include the ability to disable (also known as “lock” or “brick”) the device remotely if it is lost.

Educate clinicians and staff on safe mobile device use

- Provide training to all clinicians and staff who use mobile devices. Training should address:
  - Relevant policies and procedures.
  - IT security protocols.

This document is a work product of Coverys’ Risk Management Department. This information is intended to provide general guidelines for risk management. It is not intended and should not be construed as legal or medical advice. Your organization should add to and modify this tool to address the compliance standards and regulations applicable in your state or organization.

The links included in this document are being provided as a convenience and for informational purposes only; they are not intended and should not be construed as legal or medical advice. Coverys Risk Management bears no responsibility for the accuracy, legality or content of the external site or for that of subsequent links. Contact the external site for answers to questions regarding its content.

Ensure Safe Use of Electronic Devices

  - Safe mobile device use.

Dispose of devices appropriately

- Clean all saved data from the device by initiating a factory or “hard” reset. Consult the user manual for instructions. Contact the service provider for other options.
- After resetting or wiping the phone, check call logs, voicemails, emails, text messages, downloads, folders, browser search history, and photo albums to ensure removal of all personal information.
- Delete all downloaded applications.
- Remove the SIM card or any additional storage cards.

Consider Communication Delays

Understand the two types of electronic communication

- Ensure staff understands the difference between synchronous and asynchronous communication.
  - Synchronous communication occurs in real time and is appropriate for urgent and time-sensitive interactions that require action or decision-making.
  - Synchronous communication may also be useful for supervision.
  - Asynchronous communication is delayable and includes texting, email, voicemail, and portal messages.
  - Asynchronous communication should never be used for emergent, urgent, or complex communications.

‘m not

Use Caution When Accessing or Communicating via the Internet

Do not practice distracted medicine

- Set limits for using devices during patient care activities. For example, do not accept emails or texts during patient examination or while documenting orders.
- Consider implementing device-free zones, such as examination rooms, treatment suites, and medication preparation areas.
- Consider identifying zones for device use that is unrelated to work, such as a break room.

This document is a work product of Coverys’ Risk Management Department. This information is intended to provide general guidelines for risk management. It is not intended and should not be construed as legal or medical advice. Your organization should add to and modify this tool to address the compliance standards and regulations applicable in your state or organization.

The links included in this document are being provided as a convenience and for informational purposes only; they are not intended and should not be construed as legal or medical advice. Coverys Risk Management bears no responsibility for the accuracy, legality or content of the external site or for that of subsequent links. Contact the external site for answers to questions regarding its content.

Updated: October 2020

Use Caution When Accessing or Communicating via the Internet

- Consider separate devices for work and personal use. When using one device for both, ensure that work-related email is separate from personal email.

Use technology etiquette

- Inform patients when using a device for care-related purposes, and explain why and what you are doing.

Use Caution With Unencrypted Email

Develop a written policy and procedures

- Develop a policy and procedures before using email in professional practice. Ensure the policy includes, at a minimum, the following elements:
  - Parameters for use.
  - Prohibited uses.
  - Response times.
  - Confidentiality.
  - Patient permission to communicate by email.
  - Emergencies.
  - Documentation of emails sent/received.
  - Inclusion of emails in patient care records.
  - Email retention process.
- Share electronic and hard copies of policies and procedures with all patients who use email to communicate with the practice.
  - Ensure that emails forwarded outside the practice to parties with established business associate agreements or parties entitled to patient information under the Treatment, Payment, and Operations (TPO) clause comply with HIPAA requirements.
- Use encryption and mark emails “confidential” to decrease the possibility of a breach.

Educate staff members

- Educate all staff members about the unencrypted email policy and procedures.
- Monitor staff email use to ensure strict adherence.

Define parameters for use

- Explain that email may be used for scheduling appointments, requesting prescriptions and refills, asking insurance or simple non-urgent questions, and communicating routine follow-up information,

Use Caution With Unencrypted Email

	such as home blood pressure readings or glucose test results. ○ Explain that email should NOT be used for emergencies, time-sensitive information, medically sensitive information, and complicated care-related issues. ○ Prohibit forwarding patient emails outside the practice.
Obtain permission from patients to communicate by email	• Obtain the patient’s written permission to communicate by email. File the original signed permission form in the patient record and give the patient a copy. • See ***Permission to Use Email SAMPLE***
Use encryption to maintain confidentiality	• Develop and implement encryption systems if using email to communicate PHI, including email sent via an open network or the internet. • Include automated disclaimers on each email regarding information confidentiality and appropriate measures to take in case an email is received in error. • Transmit personal health information via a secure network.
Include email confidentiality requirements in privacy and security policies	• Address email use in privacy and security policies. Ensure relevant policies include: ○ How health information will be handled. ○ For what purposes it will be disclosed. ○ What security systems exist or need to be implemented to protect against unauthorized disclosures.
Define standard response time	• Establish a response time frame and inform patients when to expect responses during and after hours and when practitioners are on vacation.
Monitor, review, and respond to emails	• Monitor email on a regular basis. • Establish a schedule for office email review (e.g., hourly, once or twice daily, etc.). • Respond according to the time frames established in your policy.

This document is a work product of Coverys’ Risk Management Department. This information is intended to provide general guidelines for risk management. It is not intended and should not be construed as legal or medical advice. Your organization should add to and modify this tool to address the compliance standards and regulations applicable in your state or organization.

The links included in this document are being provided as a convenience and for informational purposes only; they are not intended and should not be construed as legal or medical advice. Coverys Risk Management bears no responsibility for the accuracy, legality or content of the external site or for that of subsequent links. Contact the external site for answers to questions regarding its content.

Use Caution With Unencrypted Email	
Develop a vacation coverage policy for email management	• Develop an email policy for vacation coverage that defines who will read and triage emails. Ensure the covering practitioner can access the emails. • Inform patients when practitioners are on vacation.
Add a disclaimer statement	• Consider adding a standard disclaimer statement to the end of all emails. Include the practice’s contact information and language indicating that information provided via email is not meant as a substitute for medical care or advice. • Provide instructions on measures to take when an email is sent or received in error.
Create an email retention policy	• Develop and adhere to an email retention policy that establishes time frames for retaining and deleting emails. • Recognize that emails are considered electronically stored information and are discoverable in legal proceedings. • Maintain email communication in the medical record for the same retention period as the medical record.
Maintain email as part of the medical record	• Consider any patient care-related email to be a part of the legal medical record. Include all email communications in the medical record to provide a complete record of patient care. • File email in the patient’s medical record and maintain them in the same way that all other health-related communications are stored.
Ensure Safe Texting	
Develop a policy and procedures for mobile device use	• Ensure a backup power source is available to minimize service interruptions and maintain access to electronic information if power outages occur. • Develop a policy addressing safe use of mobile devices by practitioners and staff members that covers at least the following: ○ Periodic risk assessments of mobile device use, including whether personal mobile devices are being used to exchange ePHI and whether proper authentication, encryption, and physical

Ensure Safe Texting	
	protections are in place to secure the exchange of ePHI. ○ Encryption and security breach protocols for mobile devices. ○ Encryption installation to protect ePHI stored or sent by mobile devices. ○ Security software protocols and installation schedules for regular updates. ○ Unique passwords or biometric authentication to verify the person using the mobile device is authorized to access the ePHI. ○ Limits on file-sharing applications. ○ Preapproved mobile applications. ○ Wi-Fi security rules. • Define appropriate and safe use of mobile devices by clinicians and staff and provide education about relevant policies and procedures. • Train clinicians and staff on how to safely access and share ePHI using mobile devices.
Take steps to protect information privacy	• Ensure devices are secure: ○ Provide password protection. ○ Fully encrypt through a VPN. • Avoid downloading and storing PHI on a smartphone (for example, view-only access). • Do not permit others, including family members, to use devices. • When using devices in a public location, take steps to prevent others from viewing the screen when entering passwords and viewing patient-related information. • If using a mobile device to text protected health or personal information, make sure the device is encrypted.
Use caution when texting	• Avoid using text messages for transmitting PHI; text messages are unencrypted and unsuitable for ePHI.

This document is a work product of Coverys' Risk Management Department. This information is intended to provide general guidelines for risk management. It is not intended and should not be construed as legal or medical advice. Your organization should add to and modify this tool to address the compliance standards and regulations applicable in your state or organization.

The links included in this document are being provided as a convenience and for informational purposes only; they are not intended and should not be construed as legal or medical advice. Coverys Risk Management bears no responsibility for the accuracy, legality or content of the external site or for that of subsequent links. Contact the external site for answers to questions regarding its content.

Ensure Safe Texting	
	• Shut off Bluetooth and wireless when not in use and beware of public wireless systems; encrypt PHI transmitted over public Wi-Fi. • Ask for acknowledgment of receipt when sending text messages. • Keep in mind that text messaging can be asynchronous and not appropriate for urgent or emergent communication. • Use caution when taking and texting images. Use approved applications that link to an EMR such as VisualDx to capture care-related images. • Ensure images do not contain or constitute an identifier (e.g., a full-face photograph, name, or unique identifier). • Enter texted treatment recommendations into the patient medical record.
Educate clinicians and staff on safe mobile device use	• Provide training to all clinicians and staff who use mobile devices. Training should address: ○ Relevant policies and procedures. ○ IT security protocols. ○ Safe mobile device use.
Do not practice distracted medicine	• Set limits for using devices during patient care activities. For example, do not accept personal texts or phone calls during patient examination or while documenting orders. • Consider implementing device-free zones, such as examination rooms, treatment suites, and medication preparation areas. • Consider identifying zones for device use that is unrelated to work, such as a break room.
Use technology etiquette	• Inform patients when using a device for care-related purposes, and explain why and what you are doing.

This document is a work product of Coverys' Risk Management Department. This information is intended to provide general guidelines for risk management. It is not intended and should not be construed as legal or medical advice. Your organization should add to and modify this tool to address the compliance standards and regulations applicable in your state or organization.

The links included in this document are being provided as a convenience and for informational purposes only; they are not intended and should not be construed as legal or medical advice. Coverys Risk Management bears no responsibility for the accuracy, legality or content of the external site or for that of subsequent links. Contact the external site for answers to questions regarding its content.

Use Caution With Fax Machines

Develop and implement a policy and procedures for faxing

- Develop a policy and procedures that provide clear direction to staff members for faxing medical information and PHI. Address the following elements in the policy:
  - Define situations requiring fax use.
  - Specify in the policy what PHI should not be faxed (e.g., highly sensitive records, such as psychotherapy, sexually transmitted diseases, and/or substance abuse).
  - Place fax machines that transmit and receive PHI in a private area to avoid inadvertent PHI disclosure.
  - Obtain patient authorization before faxing information, if indicated. (Authorization for faxing is not required under HIPAA's TPO clause.)
  - Include a process for ensuring preprogrammed numbers are accurate in fax machines, EMRs, and computer systems used to fax records. Validate preprogramed numbers on a regular basis.
  - "Appoint someone to be responsible for fax machines to ensure pre-programmed numbers are **regularly audited** to check that the number is indeed current and accurate, and that automatic polling and delayed transmission are turned off."[9]
  - Ensure that faxed information is going to the proper party.
  - Educate personnel who use the fax machine.
  - Report misdirected fax documents and any confidentiality breaches to the designated privacy officer.

Ensure faxes are sent and received securely

- Place the fax machine in a secure location.
- Avoid sending faxes to general locations, such as a mailroom.
- Verify the fax number and request the recipient to stand by the fax machine when necessary before faxing the information.

This document is a work product of Coverys' Risk Management Department. This information is intended to provide general guidelines for risk management. It is not intended and should not be construed as legal or medical advice. Your organization should add to and modify this tool to address the compliance standards and regulations applicable in your state or organization.

The links included in this document are being provided as a convenience and for informational purposes only; they are not intended and should not be construed as legal or medical advice. Coverys Risk Management bears no responsibility for the accuracy, legality or content of the external site or for that of subsequent links. Contact the external site for answers to questions regarding its content.

Use Caution With Fax Machines

Use care with preprogrammed numbers

- Preprogram frequently used fax numbers.
- Decrease the likelihood of sending a fax to an unintended recipient by confirming the accuracy of preprogrammed fax numbers at least every six months.

Confirm “need to know”

- Prevent breaches of confidential information by confirming the requestor’s “need to know.” For example, require a patient’s signed authorization to release PHI when the requested information will be used outside of treatment, payment, or operations.

Confirm receipt

- Request that the recipient acknowledge receipt of the fax transmission.

Include a confidentiality statement on the fax cover sheet

- Use a fax cover sheet to help mitigate the risk associated with misrouted faxes.
- Include language that advises unintended recipients that the information is confidential and should be returned to the sender or destroyed. For example:

  > “The information contained in this facsimile transmission is intended for use only by the addressee indicated above. The information is confidential and legally privileged. If you are not the intended recipient, please be advised that any disclosure, copying, distribution, or use of the contents of this information is strictly prohibited. Please notify [insert contact person] at [insert number] that you have received a fax in error and wish to arrange for return or destruction of the documents. Your cooperation is appreciated.”

Use caution with sensitive information

- Do not fax sensitive PHI that requires additional privacy protections, such as HIV, sexually transmitted diseases, substance abuse treatment, and psychotherapy notes.
- Use caution with other information that may be considered sensitive but is not subject to additional privacy protections.

Use Practice Website Effectively

Determine the purpose

- Define the practice website’s purpose. For example:

Use Practice Website Effectively

  - To provide information about the practice (e.g., office hours, locations, practitioner profiles, credentials, awards, etc.).
  - To provide patient education.
  - To attract new business.
  - To promote patient portal use and provide a portal link for scheduling appointments and accessing records, secure email communication, and payment options.

Establish guidelines

- Consider developing and posting guidelines defining how patients and the public can access and utilize the website.

Choose language carefully

- Avoid overpromising or making false claims to reduce the risk of regulatory noncompliance. Website content may be regulated by a number of federal agencies, including the Federal Trade Commission (advertising in general) and the Food and Drug Administration (advertising related to regulated medical devices).
- Comply with applicable state regulations.
- Use objective language; make sure to support any claims made about products or services and to comply with applicable regulations.
- Take care NOT to advertise on the website in such a way that it establishes standards of care.
- Clearly identify physicians and advanced practice professionals.
- Post an administrative email address for general inquiries.

Use a disclaimer

- Prominently post a disclaimer on the website's educational page(s) advising both patients and nonpatients that:
  - The website is intended to provide general healthcare information and is not medical advice.
  - The website is not intended to take the place of an office encounter.
  - Links to external sites do not necessarily represent the practice's endorsement of products, treatments, or philosophies.

Use Practice Website Effectively

Take precautions with advertising	• Avoid overstating capabilities, making promises, or offering products or services that do not comply with federal and state regulations. • Use objective language, and make sure that any claims made about products or services are accurate. • Do not advertise in such a way that appears to establish standards of care. • Accurately depict practitioners' credentials. • Disclose affiliations with commercial or other entities. • Use caution when advertising third-party products or services. Obtain written consent before displaying images of third-party products or services on the website. • Consult an attorney to establish fees and contracts when the practice chooses to advertise for drug companies or other businesses. • Ensure any business that advertises on the practice website operates at a high standard of professional ethics. • Prohibit public display of patient images or PHI.
Maintain the website	• Establish a website maintenance schedule. • Ensure all information is current and accurate. • Update any changes, including: ○ Services, treatments, and therapies offered. ○ Practitioner staffing and credentials. ○ Locations. ○ Hours. ○ Contact information.
Take care when accepting free websites	• Obtain legal advice before entering into an arrangement for free website services.

Ensure Safe Portal Use

Decide how and when to develop a patient portal	• Conduct thorough research on the use of portals. Visit practices that have successfully implemented a portal and ask them what works and what doesn't.

This document is a work product of Coverys' Risk Management Department. This information is intended to provide general guidelines for risk management. It is not intended and should not be construed as legal or medical advice. Your organization should add to and modify this tool to address the compliance standards and regulations applicable in your state or organization.

The links included in this document are being provided as a convenience and for informational purposes only; they are not intended and should not be construed as legal or medical advice. Coverys Risk Management bears no responsibility for the accuracy, legality or content of the external site or for that of subsequent links. Contact the external site for answers to questions regarding its content.

Updated: October 2020

Ensure Safe Portal Use

- Consult your EMR system vendor, which may be able to provide information.
- Determine if you will permit patients to upload information for inclusion in their record, how they will upload the information, and what types of information you will accept.
- Consult state laws pertaining to healthcare for minors to determine if they can consent for care on their own and if the practice can sequester health information related to that care from the portal to prevent parental access.
- Consider the following related to minors when designing the portal:
    - For patients 12 and under, parents can have primary access to the portal; a child's level of access should be guided by discussion with the family.
    - For patients between the ages of 13 and 18 who may be able to consent to some services such as birth control without parental involvement, define parental access by the ability to restrict sensitive information. If it is not possible to sequester sensitive information from parental review, it may be necessary to terminate parental access, or, if agreed upon in advance, do not upload that information to the portal.
    - For patients 18 and older, terminate parental access to the portal, unless there are special circumstances (e.g., the patient is not competent to consent to care) or the patient agrees to permit parental access and signs written authorization.[10]
- Determine whether and when to limit or completely restrict parental access to the portal.
- Consider implementing a testing phase based on role-based access to the portal (patients, practitioners, and staff members).
- Consider reviewing HealthIT.gov's resource How to Optimize Patient Portals for Patient Engagement and Meet Meaningful Use Requirements.

This document is a work product of Coverys' Risk Management Department. This information is intended to provide general guidelines for risk management. It is not intended and should not be construed as legal or medical advice. Your organization should add to and modify this tool to address the compliance standards and regulations applicable in your state or organization.

The links included in this document are being provided as a convenience and for informational purposes only; they are not intended and should not be construed as legal or medical advice. Coverys Risk Management bears no responsibility for the accuracy, legality or content of the external site or for that of subsequent links. Contact the external site for answers to questions regarding its content.

Ensure Safe Portal Use

Develop a portal policy and procedures

- Ensure the patient portal policy and procedures address the following:
  - Privacy and security.
  - Username and password.
  - Security risk assessment, including frequency.
  - Criteria and monitoring for appropriate usage.
  - Data backup.
- Parameters for portal use.
- Response time.
- Prohibited usage for sensitive, time-sensitive, emergent, or urgent matters.
- Guidelines for prescription refill requests.
- Permissions to access minors' information.
- Portal user agreement.
- Patient education on portal use.
- Notification to provider when patients review diagnostic results.
- Define urgent and emergent matters and consider including a bolded pop-up message that instructs portal users to call 911 for emergencies.
-

Develop and implement a portal user agreement

- Ensure the portal user agreement addresses the following:
  - How the office practice will use the portal and what patients may expect.
  - Acceptable and unacceptable portal use.
  - Prohibiting portal use for sensitive, time-sensitive, urgent, or emergent matters.
  - Types of information that patients can upload to the portal.
  - How to request a prescription refill.
  - How to schedule appointments.
- Use the agreement as a teaching tool and a document of the patient's willingness to use the portal.

This document is a work product of Coverys' Risk Management Department. This information is intended to provide general guidelines for risk management. It is not intended and should not be construed as legal or medical advice. Your organization should add to and modify this tool to address the compliance standards and regulations applicable in your state or organization.

The links included in this document are being provided as a convenience and for informational purposes only; they are not intended and should not be construed as legal or medical advice. Coverys Risk Management bears no responsibility for the accuracy, legality or content of the external site or for that of subsequent links. Contact the external site for answers to questions regarding its content.

Ensure Safe Portal Use	
	• Give the patient a signed copy of the agreement. • Maintain a copy of the portal user agreement in the patient record.
Reduce the risk of privacy breaches on the portal	• Require each user to register with a unique username and password. • Instruct users to not share their username or password with others. • Instruct users against posting sensitive patient information (e.g., treatment pertaining to mental health, sexually transmitted diseases, or substance use disorder).
Educate patients on acceptable portal use	• Post a statement on the entry page and/or the messaging window stating that the portal is not continuously monitored and must not be used for emergent or urgent situations. • Instruct portal users to call 911 in the event of a medical emergency and the office for all non-urgent/emergent care-related questions. • Consider developing patient education materials defining acceptable portal use. ○ Explain how patients will communicate through the portal. ○ Establish what patients should expect for a response time. ○ Demonstrate acceptable and unacceptable communication types. ○ Provide examples of acceptable use (e.g., request an appointment, review previously communicated lab results, immunizations, etc.). ○ Provide examples of unacceptable use (e.g., sensitive or time-sensitive matters such as abnormal diagnostic results, urgent or emergent matters, reporting signs or symptoms, etc.). ○ Stress the importance of communicating any urgent and emergent clinical concerns directly to the office by phone rather than the portal.

This document is a work product of Coverys' Risk Management Department. This information is intended to provide general guidelines for risk management. It is not intended and should not be construed as legal or medical advice. Your organization should add to and modify this tool to address the compliance standards and regulations applicable in your state or organization.

The links included in this document are being provided as a convenience and for informational purposes only; they are not intended and should not be construed as legal or medical advice. Coverys Risk Management bears no responsibility for the accuracy, legality or content of the external site or for that of subsequent links. Contact the external site for answers to questions regarding its content.

Ensure Safe Portal Use

Monitor the patient portal for inappropriate use

- Ask patients to sign for education to accept and document their understanding of the portal's purpose as well as inappropriate and appropriate portal use.
- Consider assigning a clinician to check the portal throughout each day for appointments scheduled that might qualify as an emergency and respond accordingly.

Use Best Practices for Social Media

Develop a social media policy and procedures

- Develop and implement a written policy and procedures that address social media use by practitioners and staff members. Ensure the policy includes:
  - The reasons for using social media, the target audience, and the expected outcome.
  - A social media code of conduct that addresses the terms of use for practitioners and staff members.
  - The expectations regarding the practice's social media site, as well as the use of external social media platforms to discuss practice-related or patient care matters.
- Review and update existing patient communication and confidentiality policies to address social media use, as appropriate.
- Polices should address maintaining the same professional and ethical standards in social media comments and responses that the practice would use with any other form of communication.
- Consider the Centers for Disease Control and Prevention's (CDC) Social Media Tools, Guidelines & Best Practices[11] for additional resources.

Delegate responsibility for managing social media

- Assign responsibility for developing, reviewing, and posting content on internal and external social media sites.
- Define who is responsible for responding to requests and content posted by others about the practice on social media.

This document is a work product of Coverys' Risk Management Department. This information is intended to provide general guidelines for risk management. It is not intended and should not be construed as legal or medical advice. Your organization should add to and modify this tool to address the compliance standards and regulations applicable in your state or organization.

The links included in this document are being provided as a convenience and for informational purposes only; they are not intended and should not be construed as legal or medical advice. Coverys Risk Management bears no responsibility for the accuracy, legality or content of the external site or for that of subsequent links. Contact the external site for answers to questions regarding its content.

Use Best Practices for Social Media	
	• Clearly define the authority limits of the person or persons assigned this responsibility. • Define terms under which a responsible individual or group can review and respond to comments, complaints, and inappropriate content posted on the group's social media site(s) and external social media platforms. • Document actions taken in response to social media content and comply with appropriate laws and regulatory requirements.
Monitor social media posts	• Regularly monitor social media posts by and about the practice on the group's social media site(s) and external platforms for potentially libelous and copyrighted material, PHI breaches, inappropriate content, cyberbullying, stalking, and viral postings that result in media attention. Consider conducting a risk analysis for exposures.
Define how the practice responds to social media posts	• Establish a process for designated staff to review and respond to social media posts that include potentially libelous and copyrighted material, PHI breaches, inappropriate content, cyberbullying, stalking, and viral postings that result in media attention.
Provide staff education on social media use	• Educate staff members to not respond to complaints and inappropriate social media posts, but instead to escalate these communications to the attention of individuals who are delegated to handle and respond to them.[12] • Include a formal mechanism for staff members to report inappropriate postings and/or use of the site and its content. • Remind staff that online posts, tweets, or blogs can never be completely deleted.

Additional Coverys Resources:

- HIPAA Privacy
- HIPAA Security
- Patient Relations

This document is a work product of Coverys' Risk Management Department. This information is intended to provide general guidelines for risk management. It is not intended and should not be construed as legal or medical advice. Your organization should add to and modify this tool to address the compliance standards and regulations applicable in your state or organization.

The links included in this document are being provided as a convenience and for informational purposes only; they are not intended and should not be construed as legal or medical advice. Coverys Risk Management bears no responsibility for the accuracy, legality or content of the external site or for that of subsequent links. Contact the external site for answers to questions regarding its content.

Updated: October 2020

- ***Permission to Use Email SAMPLE***

References:

1. Pew Research Center. Mobile fact sheet. https://www.pewinternet.org/fact-sheet/mobile/. Published June 12, 2019. Accessed August 8, 2019.
2. Office for Civil Rights. Does the HIPAA privacy rule permit health care providers to use e-mail to discuss health issues and treatment with their patients? U.S. Department of Health & Human Services website. https://www.hhs.gov/hipaa/for-professionals/faq/570/does-hipaa-permit-health-care-providers-to-use-email-to-discuss-health-issues-with-patients/index.html#:~:text=Further%2C%20while%20the%20Privacy%20Rule,through%20the%20unencrypted%20e%2Dmail. Created December 15, 2008. Last reviewed July 26, 2013. Accessed October 20, 2020.
3. O'Brien G, Lesser N, Pleasant B, et al. *Securing Electronic Health Records on Mobile Devices, Volume B: Approach, Architecture, and Security Characteristics.* National Institute of Standards and Technology. Special Publication 1800-1B, CODEN: NSPUE2. https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-ehr-nist-sp1800-1b.pdf. Published July 2018. Accessed October 8, 2019.
4. *Permitted Uses and Disclosures: Exchange for Health Care Operations.* The Office of the National Coordinator for Health Information Technology, US Department of Health and Human Services Office for Civil Rights. 45 Code of Federal Regulations (CFR) 164.506(c)(4). https://www.healthit.gov/sites/default/files/playbook/pdf/exchange-health-care-ops.pdf. Published January 2016. Accessed July 17, 2020.
5. Patient portal increases communication between patients and providers. The Office of the National Coordinator for Health Information Technology website. https://www.healthit.gov/case-study/patient-portal-increases-communication-between-patients-and-providers. Last reviewed February 7, 2018. Accessed October 20, 2020.
6. Increase patient participation in their care. The Office of the National Coordinator for Health Information Technology website. https://www.healthit.gov/topic/health-it-and-health-information-exchange-basics/increase-patient-participation-their-care. Last reviewed September 26, 2018. Accessed October 20, 2020.
7. FSMB Ethics and Professionalism Committee. Social media and electronic communications. Federation of State Medical Boards website. http://www.fsmb.org/siteassets/advocacy/policies/social-media-and-electronic-communications.pdf. Published April 2019. Accessed July 17, 2020.
8. ECRI Institute. Social Media in Healthcare, Ambulatory Care Risk, Quality, & Safety Guidance, https://www.ecri.org/search-results/member-preview/pprm/pages/st6/ Published April 18, 2017. Accessed July 17, 2020.

This document is a work product of Coverys’ Risk Management Department. This information is intended to provide general guidelines for risk management. It is not intended and should not be construed as legal or medical advice. Your organization should add to and modify this tool to address the compliance standards and regulations applicable in your state or organization.

The links included in this document are being provided as a convenience and for informational purposes only; they are not intended and should not be construed as legal or medical advice. Coverys Risk Management bears no responsibility for the accuracy, legality or content of the external site or for that of subsequent links. Contact the external site for answers to questions regarding its content.

9. Cobb M. Fax Machine security: creating a corporate faxing policy. *Computer Weekly*. November 17, 2010. https://www.computerweekly.com/tip/Fax-machine-security-Creating-a-corporate-faxing-policy. Accessed September 25, 2020.
10. Goldschmidt M. Patient portals: privacy for minors. Healthcare Info Security website. https://www.healthcareinfosecurity.com/patient-portals-privacy-for-minors-a-6495. Published February 11, 2014. Accessed July 17, 2020.
11. Centers for Disease Control and Prevention. CDC social media tools, guidelines & best practices. https://www.cdc.gov/socialmedia/tools/guidelines/index.html. Last reviewed December 27, 2019. Accessed July 17, 2020.
12. ECRI. Ask ECRI: patient complaints on social media, the HIPAA privacy rule, and providers. https://www.ecri.org/components/PPRM/Pages/AskECRI080217.aspx. Published August 2, 2017. Accessed July 17, 2020.

This document is a work product of Coverys' Risk Management Department. This information is intended to provide general guidelines for risk management. It is not intended and should not be construed as legal or medical advice. Your organization should add to and modify this tool to address the compliance standards and regulations applicable in your state or organization.

The links included in this document are being provided as a convenience and for informational purposes only; they are not intended and should not be construed as legal or medical advice. Coverys Risk Management bears no responsibility for the accuracy, legality or content of the external site or for that of subsequent links. Contact the external site for answers to questions regarding its content.