Guidance for using text, email, and video communication in practices devoted to reproductive medicine

Technology and Practice Committees of the American Society for Reproductive Medicine

American Society for Reproductive Medicine, Birmingham, Alabama

The prevalence and ease of electronic communication, specifically email through patient portals associated with electronic medical records or via traditional enterprise email clients (e.g., Outlook) and video, have resulted in increased use for rapid communication between practitioners and their patients. Concerns regarding patient privacy and compliance with the regulations of the Health Insurance Portability and Accountability Act (HIPAA) remain a barrier to routine incorporation of electronic communication into practice. Furthermore, capital investment, implementation, and maintenance costs may provide additional barriers. These long-standing concerns have been heightened and tested by the COVID-19 pandemic. Best-practice guidelines for the secure and safe use of electronic communication with reproductive care patients are provided. (Fertil Steril® 2021;115:1156–8. ©2021 by American Society for Reproductive Medicine.)

Discuss: You can discuss this article with its authors and other readers at **https://www.fertstertdialog.com/posts/32313**

The COVID-19 pandemic forced a change in the way medical practices interact with their patients. For the safety of patients and providers, the American Society for Reproductive Medicine (ASRM) COVID-19 task force strongly encouraged the use of telehealth in lieu of in-person visits [1]. For some practices, this was an entirely new experience whereas, for others, it meant a shift to a methodology that they had already been using. Telehealth encompasses multiple modalities including video conferencing, audio/phone conferencing, secure messaging within an electronic health record system, email over the open internet, and electronic means of signing consent forms. Patients find electronic media to be an efficient means of communicating with clinicians. In addition, electronic media enhances communication for medical practices, including the benefits of increased responsiveness and enhanced patient satisfaction. However, there are some pitfalls that should be considered. This document focuses on the use of email communication, portals embedded in electronic medical records, telemedicine, and other common types of video communication between providers and patients.

WHAT SHOULD I CONSIDER WHEN COMMUNICATING WITH MY PATIENTS BY EMAIL?

Transmission of previous medical records and test results: Patients often express frustration with provider-to-provider transmission of previous medical records. When paper charts prevailed, requests for medical records meant having an employee of the practice stand with the chart at a copy machine to make a physical paper copy of the records, which would be mailed or faxed to the requesting entity. Now in the era of electronic health records, digital copies can be generated and sent by several means. It is not uncommon for patients to request and retain copies of their medical records and then choose to transmit them via email to a new practice or provider that they may visit.

Follow up to a visit*:* In contrast to a live interaction over a video link, telephone, or in-person where one or more questions can be posed and answered in real-time, email allows the transmission of a focused query to which a response can be given hours or days later. There are many uses and benefits to email communication either via an enterprise email server, such as Outlook, or through a patient portal. Some of the advantages and pitfalls of either type of communication are listed.

Potential Uses/Benefits

- Patient flexibility: Patients often wish to provide previous medical records or test results in advance of a telehealth or in-person visit.
- Provider flexibility: Electronic communication allows more flexibility and timeliness in the relay of information, such as test results, treatment planning, and answers to frequently asked questions (FAQs).

Received January 21, 2021; accepted January 26, 2021; published online April 3, 2021.
Reprint requests: American Society for Reproductive Medicine, 1209 Montgomery Highway, Birmingham, Alabama 35216 (E-mail: ASRM@asrm.org).

Fertility and Sterility® Vol. 115, No. 5, May 2021 0015-0282/$36.00

https://doi.org/10.1016/j.fertnstert.2021.01.046

- Enhanced communication: Patients can electronically ask questions that they may have forgotten to ask during their last live encounter. Physicians can elaborate on specific information that needs further clarification and offer another telehealth or an in-person visit to better serve the patient if the issue isn't resolved by the email exchange.
- Availability: Electronic correspondence can improve the perception of provider and staff availability.
- "Real-time" reporting: Standard reporting of results through templates may reduce the time needed to inform patients of test results.
- Decreased number of patient visits: Relaying treatment instructions and other communications electronically rather than in person can decrease the risk of disease transmission in locations where COVID-19 cases or other serious communicable diseases are prevalent, improve patient throughput, and lower patients' copays through fewer visits without compromising care.

Potential Pitfalls

- Unrealistic patient expectations: Patients who receive a rapid reply to a sent email during office hours on a weekday may falsely believe that their email will receive the same attention 24 hours a day, 7 days a week even if counseled to the contrary. Placing warnings for patients (in email or otherwise) that email communication should not be used for emergent/urgent communication should be considered.
- Assumption of a single point of communication: A patient may unrealistically believe that they can rely on a single individual with whom they correspond to have email access every day. The patient may fail to reach out to the practice through other means with a time-dependent problem because they believe that the one individual will always be available and be able to address all issues.
- Misunderstandings: Conveyance of information in an asynchronous electronic written form is not equivalent to a live discussion between a patient and a medical professional. Vital clues to an underlying problem are often picked up by health-care personnel only through dialogue and questioning.
- Gaps in team information: Email communication outside the patient record can create knowledge gaps among the care team about the patient's treatment. Not all interchanges may be captured in the medical record, leading to misunderstandings and gaps or errors in patient care. Consideration should be given to ensuring that such communications are copied to all relevant members of the care team and/or directly into patient charts.
- Burden on staff/physician: With no barrier to direct communication, a patient without any malintent may send a large number of brief emails to the provider's office with questions that could easily be addressed during a single follow-up visit. Multiplied across a busy practice, staff time can be consumed without constraints.
- Security/privacy: Information may be viewed by individuals other than the patient without the patient's permission.
- Reimbursement: Billing for time spent on email communication is problematic.

One of the concerns with personal email is that only a single password is needed to access sensitive health information. A patient portal can be a useful way to encrypt messaging securely, but may still not be much more secure than personal email. Practices need to work with their information technology (IT) division or outside IT companies/consultants to implement secure patient portals.

Given the prevalence and convenience of email on mobile devices, some institutions have authorizations/consent forms for patients (Email Authorization forms) that disclose the insecure nature of unencrypted email or text messages and issues with validation of identity. These forms are intended to obtain formal authorization from each patient for the use of unencrypted communication and can be presented to patients at their initial visits and should become part of the medical records. Patients should be reminded that commonly used email servers have been breached in the past. Thus, it is probably best to recognize that no electronic communication is completely secure ([2]). Despite changing perceptions of what is private, the Health Insurance Portability and Accountability Act (HIPAA) remains in effect.

Billing for time spent in electronic communication may be reasonable, but laws and policies governing this type of medical billing vary widely across practices, institutions, and states. Even if permitted in some states, this does not mean that insurers will necessarily reimburse for electronic communication. Email communication should not be used as a substitute for an initial consultation to establish the care of a patient. In addition, clinics should make patients aware of internal policies about the timeliness of response to patients' email inquiries.

Electronic communication with a patient is part of the digital record and may be discoverable in potential lawsuits. Professionalism standards apply to any form of online communication with patients, whether in email or a portal, just as they do for any patient encounter. As with medical documentation, patient emails should be written with the assumption that they could become public knowledge.

WHAT DO I NEED TO CONSIDER WHEN USING TELEMEDICINE/VIDEO TO COMMUNICATE WITH MY PATIENTS?

Video communication can be used to interview and consult with patients but requires a higher level of physician involvement than email. Although any video messaging service can be used to talk to patients, these services can have the same security challenges as email and may not be compliant with HIPAA regulations. Free video communication applications embedded in operating software for handheld devices, tablets, and computers were not designed for secure interactions with patients. Likewise, the use of free versions of applications that sell HIPAA-compliant video communication services can put a practice at risk.

For video-conferencing software to meet HIPAA compliance, the software must meet the following requirements:

- High-level encryption: Most commercially available videoconferencing solutions exceed federal requirements.
- Contract: A business associate agreement should exist between the handler, that is, the software company of the encrypted personal health information, and the clinic, to share liability should a data breach occur. If a business associate agreement does not exist and personal health information is being transmitted, then both parties violate federal law. This requirement is likely satisfied by the licensing agreement between the practice and provider of medical telehealth services.
- Audit trail: Video conference software must be able to document, in a time-based manner, the trail of users that accessed patient information.

For more information on whether particular videoconferencing tools are HIPAA-compliant, visit https://www.healthit.gov/topic/health-it-initiatives/telemedicine-and-telehealth.

For FAQs on telehealth and HIPAA during the COVID-19 pandemic visit https://www.hhs.gov/sites/default/files/telehealth-faqs-508.pdf

Platforms for telemedicine that are expressly crafted for health-care providers should be used to maximize the likelihood of compliance with HIPAA and other existing laws. Consideration should be given to state laws that regulate medical licensing, as most states require physicians to have a license in the state in which the patient is located. Reimbursement can be equivalent to in-person physician visits if the patient is located in a remote site and not restricted by payor status; however, laws regulating reimbursement of telemedicine vary by state.

The video communication should not be recorded without appropriate permissions and should occur on the covered entity's own server. Thus, the practice should control both sides of the communication– the server on the physician side and the computer on the client side. This requires a dedicated application system and precludes the use of many commercially available applications where an outside company controls the server.

If a practice communicates with a patient in a nonsecure fashion, then the practice places itself at risk of breaches of private patient data that could result in fines and potential litigation.

CONCLUSIONS

- Electronic communication can enhance the patient experience, but safeguards compliant with regulatory statutes and institutional policies should be implemented.
- Patient and provider education about what constitutes appropriate use of email, expectation management about whom to send an email to, and when to reasonably expect a response is critical.
- Communication by video conferencing can enhance access to care and provide a safe means of HIPAA-compliant interaction during the COVID-19 pandemic.

Acknowledgments: This report was developed under the direction of the Practice Committee of the American Society for Reproductive Medicine (ASRM) in collaboration with the ASRM Technology Committee as a service to its members and other practicing clinicians. Although this document reflects appropriate management of a problem encountered in the practice of reproductive medicine, it is not intended to be the only approved standard of practice or to dictate an exclusive course of treatment. Other plans of management may be appropriate, taking into account the needs of the individual patient, available resources, and institutional or clinical practice limitations. The Practice Committee, the Technology Committee, and the Board of Directors of ASRM have approved this report.

This document was reviewed by ASRM members and their input was considered in the preparation of the final document. The following members of the ASRM Practice Committee participated in the development of this document: Alan Penzias, M.D.; Ricardo Azziz, M.D., M.P.H., M.B.A.; Kristin Bendikson, M.D.; Samantha Butts, M.D., M.S.C.E.; Christos Coutifaris, M.D., Ph.D.; Tommaso Falcone, M.D.; Susan Gitlin, Ph.D.; Clarisa Gracia, M.D., M.S.C.E.; Micah Hill, D.O.; Karl Hansen, M.D., Ph.D.; Sangita Jindal, Ph.D.; Suleena Kalra, M.D., M.S.C.E.; Jennifer Mersereau, M.D.; Randall Odem, M.D.; Catherine Racowsky, Ph.D.; Robert Rebar, M.D.; Richard Reindollar, M.D.; Mitchell Rosen, M.D.; Jay Sandlow, M.D.; Peter Schlegel, M.D.; Chevis N. Shannon, Dr.P.H., M.P.H., M.B.A.; Anne Steiner, M.D., M.P.H.; Dale Stovall, M.D., Cigdem Tanrikut, M.D.; Michael Vernon, Ph.D., Belinda Yauger, M.D. The Practice Committee acknowledges the special contribution of Kenan Omurtag, M.D.; Michelle Cho, M.D.; Preston Perry, M.D.; and the ASRM Technology Committee in the preparation of this document. All Committee members disclosed commercial and financial relationships with manufacturers or distributors of goods or services used to treat patients. Members of the Committee who were found to have conflicts of interest based on the relationships disclosed did not participate in the discussion or development of this document.

REFERENCES

1. American Society for Reproductive Medicine. Patient management and clinical recommendations during the Coronavirus (COVID-19) pandemic. Available at: https://www.asrm.org/globalassets/asrm/asrm-content/news-and-publications/covid-19/covidtaskforce.pdf. Accessed March 22, 2021.
2. PEW Research Center. Americans' Attitudes About Privacy, Security and Surveillance. Available at: https://www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/. Accessed March 24, 2021.