Sent on Behalf of

Partnering To Protect Patient Privacy

Target Audience - Qualified Vendors and Providers

Transmittal Date - 02/09/2026

AHCCCS wants to share an important reminder about protecting patient information in email communications. In recent months, AHCCCS has seen a noticeable increase in unsecure emails from providers, some of which are being sent directly to us without the proper safeguards in place.

In addition, AHCCCS has received a growing number of complaints from members and other providers regarding unsecure communications. These trends underscore the importance of following required privacy and security practices to protect sensitive health information.

AHCCCS understands how essential it is for providers to keep electronic communication secure and compliant. While HIPAA does not set specific rules for email itself, it does require safeguards that protect the privacy and security of protected health information (PHI) whenever it is shared electronically, email included.

Below are key practices that help ensure compliance and protect patient privacy.

Key HIPAA Email Requirements

Use encryption for any email containing PHI.

- Encryption prevents unauthorized access and is a required technical safeguard under the HIPAA Security Rule.

Verify recipient identity before sending PHI.

- Double-check email addresses and use systems that support secure authentication or multifactor authentication.

Follow the “minimum necessary” standard.

- Only include the PHI needed for the purpose of the communication.

Ensure staff are trained on secure email practices.

- Training should cover encryption, identity verification, access controls, and proper handling of PHI.

Apply appropriate access controls.

- Use unique user IDs, role-based access, automatic logoff, and strong authentication methods.

Monitor and audit email activity.

- Regular reviews help detect unauthorized access or inappropriate use of PHI.

Maintain clear policies and procedures.

- Policies should address encryption, identity verification, data minimization, training, monitoring, reporting incidents, and disposal of PHI.

Obtain patient consent when emailing PHI to them.

- While not explicitly required, it is best practice to inform patients of risks and document their preferences.

Dispose of emails containing PHI securely.

- Delete PHI using approved secure disposal processes, and ensure vendors follow compliant deletion practices as well.

Why This Matters

Implementing these practices helps protect patient privacy, reduce organizational risk, and maintain compliance with HIPAA requirements for electronic communication.

If you believe that any organization or individual covered under HIPAA Privacy or Security Rules ("covered entity") has violated a patient's health information privacy rights or has otherwise failed to follow HIPAA Privacy or Security requirements, you may file a complaint directly with the Office for Civil Rights (OCR).

For instructions on how to submit a complaint, visit OCR's complaint submission page.