Codify
BY AAPC

# Health Information Compliance Alert

## Sample Policy: Take Your Patients' PHI Out of the Scrap Heap

Don't depend on your staff to make sound on-the-spot decisions about patient e-mails. Use the following e-mail retention policy sample, created by the SANS Institute in Bethesda, MD, as a guide to help you tease out the best practices for your office.

**PURPOSE:** This policy is intended to help employees determine what information sent or received by electronic mail (e-mail) should be retained and for how long.

**Note:** The information covered in these guidelines includes information that is either stored or shared via e-mail or instant messaging technologies. All employees should familiarize themselves with the e-mail retention procedures. Questions about the proper classification of a specific piece of information should be addressed to your manager. Questions about these guidelines should be addressed to the Information Technology (IT) department.

**SCOPE:** This policy is secondary to <COMPANY>'s policy on Freedom of Information and Business Record Keeping. Any message that contains information of that manner should be treated as outlined in the policy.

**PROCEDURE:** Administrative Correspondence. Includes clarification of established company policy and any legal issues such as intellectual property violations. If you copy (cc) the address when you send e-mail, retention will be administered by the IT department. Retention period = 4 years.

Fiscal Correspondence. Messages related to revenue and expense for the company. If you copy (cc) the address when you send e-mail, retention will be administered by the IT department. Retention period = 4 years.

Patient Correspondence. Messages that contain protected health information. The individual employee is responsible for retaining all patient correspondence by printing the e-mails and filing them in the correct patient chart. All patient e-mails must be deleted after the printed message is filed. Retention period = Determined by state guidelines, but no less than 6 years as mandated by HIPAA.

General Correspondence. Messages that relate to patient interaction and the operational decisions of the business. The individual employee is responsible for e-mail retention of General Correspondence. Retention period = 90 days.

Ephemeral Correspondence. Includes personal e-mail, requests for recommendations or review, e-mail related to product development, updates and status reports. These messages can be deleted immediately after they are read.

**ENCRYPTED COMMUNICATIONS:** Must be stored in a manner consistent with <COMPANY>'s information sensitivity policy, but in general, information should be stored in a decrypted format.

**E-MAIL RECOVERY FROM BACKUP MEDIA:** <COMPANY> will maintain backup tapes from the e-mail server. Tapes will be taken out of rotation and moved offsite once per quarter. No effort will be made to remove e-mail from the offsite backup tapes.

**ENFORCEMENT:** Any employee found to have violated this policy may be subject to disciplinary action up to and including termination of employment.