

Disposal Of Protected Health Information

Protected health information should be secured, monitored for age, and destroyed promptly to reduce potential privacy breach liabilities.

Breach of health privacy claims can arise from state law, as well as federal law. In order to reduce losses or mishandling of such PHI material, follow these guidelines and train your staff.

What This Means For Counties

Develop and follow a record retention and destruction policy that specifically addresses how such PHI should be stored, where, in what type of files or content, and who has access. Also specify when a record is old enough to destroy and how and how the destruction process must occur.

Have records destroyed regularly once the retention date has passed. Each record should have a retention expiration date. Destruction of records should be on a regular calendar of tasks to review the dates of PHI containing files and to destroy them under the policy.

Discard the records according to the methods chosen. Shredding, burning, pulping, or pulverizing paper records are possible, and for computer and electronic material, a total erasure or even destruction of magnetic storage components is possible—there are many methods. Whatever methods you choose, keep a record that you have consulted with a record destruction specialist to show reasonable compliance.

Train all record keeping employees and review compliance with record review and destruction as part of their evaluations. Having record custodians comply is as important as having your Privacy Officer know the rules that were broken.

For more information, contact CTSI at 303-861-0507.