Health Information Compliance Alert

CLIP 'N' SAVE: USE THIS TOOL TO ENSURE CORRECT DOCUMENTATION

Hold on to this information or kiss your security compliance goodbye

If you can't rattle off all the various data the security rule requires you to save, you aren't alone--but failure to keep the correct information could torpedo your compliance program.

Action plan: Create a list of all pieces of information you must keep in your records. Use this list, created by **Mark Eggleston**, HIPAA program manager for Health Partners of Philadelphia, in conjuction with Bricker & Eckler health care consulting practice, as a guide to get you started:

(1) All HIPAA-related policies and procedures
(2) Sanctions imposed against non-compliant workforce members
(3) All contracts and addenda to existing contracts with business associates and limited data set users, as well as amendments, renewals, revisions and terminations
(4) Access control decisions or other documentation meeting minimum necessary standard
(5) Security official selection
(6) Risk Assessment and risk management (including, but not limited to, vulnerability analysis, gap analysis, applications and data criticality analysis and rationale for security decisions).
(7) Record of audit activity or assessment that shows date, review findings and initials of reviewer
(8) Record of security reminders
(9) Disaster recovery plan/business continuity plan
(10) Change management/facility repairs logs where related to security
(11) Accountability logs for movement of hardware, media and responsible personnel
(12) Record of all evaluations
(13) Incident response plan

Disclaimer: Additional documentation requirements are applicable to Group Health Plans.

Editor's note: For more information, or to access a list of the privacy rule's documentation requirements, visit Bricker & Eckler's Web site at www.bricker.org.

CPT® 2023 American Medical Association. All rights reserved.