Health Information Compliance Alert

Prepare Yourself: What Auditors Will Look For

Focus your efforts on these hot areas.

Although the HIPAA audit protocols are an invaluable tool for any organization needing to prepare for an audit, the protocols aren't particularly easy to wade through. According to **Ober Kaler** Attorneys at Law's Healthcare Information Technology and Privacy Blog, here are the highlights of what auditors are focusing on from the HIPAA audit protocol:

- **Risk Assessment** — Auditors will want to see that you're performing risk assessments to determine potential harm from a breach. You must maintain detailed records of your risk assessment, "as well as the reasoning behind a decision to take or not take notification or mitigation steps," Ober Kaler instructed.
- **Breach Response** — "Responding to breaches should not be a 'one-off' process," Ober Kaler said. You should maintain a breach response process and have on-hand certain form letters or other notification materials.
- **Impermissible Uses/Disclosures** — You should maintain a detailed file on all impermissible uses or disclosures of protected health information (PHI), including breaches. Keep a file even on those incidents in which, "following a risk assessment, a determination was made not to notify the subject individual(s)," Ober Kaler noted.
- **Breach Notification** — Your breach preparation materials should include detailed steps on how to notify an individual of a breach if the person's contact information is out of date or lost. You should also have a policy on how to notify the media in the event of a large breach that requires media notice. Your Business Associate Agreements (BAAs) must also contain breach notification language.
- **Deceased Individuals** — You should have policies on handling the PHI of deceased individuals and addressing personal representatives. You must also maintain a policy on delaying breach notifications in response to law enforcement needs.
- **Whistleblower Disclosures** — You must have a process to determine whether a disclosure is from a potential whistleblower, including the non-retaliation requirement.
- **NPP** — Review and update your Notice of Privacy Practices (NPP) frequently to reflect changing practices in your organization. New staff training should always follow NPP changes, Ober Kaler added.
- **Plan Sponsors** — For group health plans, you should review plan sponsor documents carefully to confirm that the PHI use and disclosure by the plan sponsor is properly limited.
- **Multiple Covered Functions** — If your organization has multiple covered functions, you should maintain formal documentation that restricts PHI use or disclosure within your organization to only the purpose related to the appropriate function being performed.
- **Consent Vs. Authorization** — Ensure that your staff members understand the difference between consent and authorization, as well as when each type of assent is appropriate or required.
- **Sensitive Areas** — The audit protocols address each of these areas extensively: interactions with law enforcement; psychiatric notes; and uses and disclosures for research — specifically documentation regarding interactions with Internal Review Boards (IRBs).
- **'Relevant' Information Disclosure** — Make sure your policies and training regarding disclosures to patients' friends and family (including other individuals involved in a patient's care) are up to snuff. Auditors will also want to see that you're taking precautions to disclose only the "relevant" information in these situations.
- **Disaster Relief** — You should have a policy regarding disclosing information to aid in disaster relief efforts.
- **Individuals' Objections** — Maintain records "regarding any individual's objections to specific uses or disclosures of PHI," Ober Kaler stated. Also review your training in this area "to ensure that workforce members are trained to respond to such objections appropriately."
- **Public Health Disclosures** — You should have a policy on making disclosures for public health purposes, and you should maintain records of all such disclosures.
- **Abuse/Neglect Victims** — Maintain a policy regarding victims of abuse and neglect.

- **Specialized Government Functions** — "Notably, with regard to disclosures for specialized government functions, the audit protocols appear to suggest that it is the covered entity's responsibility to make a determination regarding the lawfulness or appropriateness of the request," Ober Kaler wrote.
- **Termination** — You must maintain policies and procedures on terminating a staff member's access to PHI after terminating a employment or a contractual relationship, for example.
- **Identity Verification** — Auditors will look for policies on verifying the identity of a requestor of PHI. "Entities should also maintain documentation regarding how specific requestors' identities are confirmed," Ober Kaler said.
- **Accounting of Disclosures** — Ensure you're maintaining documentation on all accounting of disclosures requests, including the responses you provided to a request.
- **Electronic PHI Safeguards** — Be prepared to defend your administrative, technical and physical safeguards for electronic PHI (ePHI). "Auditors are asked to determine whether the safeguards in place are 'appropriate,' although the regulatory requirements provide only that safeguards must be 'reasonable,'" Ober Kaler noted.
- **Damage/Injury Mitigation** — You must maintain policies and procedures on mitigating any damage or injury from improper use or disclosure of PHI.