Health Information Compliance Alert

HIPAA Compliance: Heed Expert Tips To Craft Effective HIPAA Policies & Procedures

Make sure you cover these 7 big changes under the new rules.

If you're like most covered entities (CEs), you're probably still in the midst of updating your policies and procedures (P&Ps) to comply with the new HIPAA Omnibus Final Rule. Here are some essential tips to perfect your HIPAA P&Ps and make your revisions a little easier.

And according to a recent presentation by the **Malvern Group Incorporated** of Malvern, PA, you should create or revise your P&Ps when you have:

- **Regulation Changes:** Federal, state, accreditation, industry standards.
- **Organization Changes:** Acquisitions, divestitures, reorganizations.
- **Environmental Changes:** Technology use (portable media, employee-owned devices), threat landscape (social media).
- **Operational Changes:** Services (registries, HIE), outsourcing, technology (architecture, EHR, cloud storage).
- **Procedure Failures:** Difficulty in implementing procedure(s) to carry out policy; lack of policy that would have required the procedure.
- **Policy Reviews:** Gaps in addressing regulations/requirement or technology changes; material errors in content.
- **Implementation Organization Change:** Change in policy implementation organization, such as HIPAA, NIST, or ISO.

Make These Updates to Your P&Ps

Of course, the passing of the HIPAA Omnibus rule has generated significant regulation changes, which means you need to update your P&Ps now. According to **Jim Sheldon-Dean**, founder and director of compliance services for **Lewis Creek Systems, LLC**, your P&Ps must reflect the following seven major changes under the HIPAA Omnibus regulations:

1. New individual rights of access;
2. New individual rights to request restrictions;
3. Change in the way to determine whether you must report a breach;
4. New restrictions on disclosures for marketing and sale of protected health information (PHI), and changes to rules for use of PHI for fundraising;
5. New restrictions on use of genetic information by health plans;
6. Expansion of rules to business associates (BAs); and
7. New rule that PHI is not protected 50 years after an individual's death.

Additionally, Sheldon-Dean points out that you must also include the following revisions to your Notice of Privacy Practices (NPP):

- New right of access to electronic PHI (ePHI);
- New right of restriction of disclosures;
- New right to be notified in the event of a breach;
- Changes to marketing restrictions;
- Changes to fundraising restrictions; and

- Genetic Information Nondiscrimination Act (GINA) notice for health plan NPPs.

Understand the P&P Basics

So as you're revising and creating your P&Ps based on the new HIPAA Omnibus regulation, fine-tune your process by getting back to the P&P basics.

Remember: The policy is the "what" and the procedures are the "how," according to the Malvern Group. The policy describes the intended effects of the rule(s), along with your organization's other business needs. The procedures, on the other hand, are the documented steps and responsibilities for accomplishing the policy, including action lists and flow charts.

Policy and procedure are the Yin and Yang, the Malvern Group stated. You must develop them together, and the policy must be implementable, while the procedure must support one or more policies.

What to do: For each statement or directive contained in a regulation, you would first determine what the required effect must be this is what you must address in your policy, the Malvern Group explained. Then you must determine the parts, if any, of the regulation's statements that direct how your organization should accomplish the requirement this is what you must address in your procedures.

Include These Key Elements in Your Policies

Best bet: You should follow a basic format for each of your organization's HIPAA policies. For instance, each policy should include a title block with dates and versions, as well as essential signatures of the policy writers, entity-level procedure owner, and senior management, the Malvern Group said. And a good rule is to limit each policy to three pages maximum.

Essential: Additionally, according to the Malvern Group, each policy should contain seven vital elements:

ü **Purpose** What the policy will accomplish for your organization.

ü **Scope** To what organizational level(s) or department(s) the policy applies, such as the entire organization, specific sites, or particular units.

ü **Policy Statements** Express what you must do to comply, including federal, state, and organizational requirements.

ü **Review Requirements** How often and in what circumstances your organization must review the policy, including both calendar-based (i.e., annually) and event-driven (i.e., regulation changes) reviews.

ü **Enforcement** Identify what organization is responsible for enforcing compliance with the policy.

ü **Assigned Responsibilities** This should include who is responsible for policy content revision and implementation of procedures.

ü **Related Regulations & Policies** Include references to any related federal and state regulations, as well as related organization policies.

Follow 6 Steps to Create/Revise P&Ps

Finally, make sure that every new or revised policy undergoes the same general process, from the draft stage all the way through to distributing the new or revised policy to employees. The Malvern Group sets out the following steps:

1. Draft/revise the policy.
2. Verify that the policy provides enough detail for implementation.
3. Draft the entity-level procedure(s) related to the policy.
4. Verify that the entity-level procedure(s) meets the policy requirements.

5. Obtain senior management approval of the policy and procedures.
6. Make the policy and procedures available for all who need it.