

Health Information Compliance Alert

Make Your Job Easier With This Breach-Notification Decision Tree

Information 'retention' can affect your notification duties.

How can you know for sure when you need to make a breach notification in the event of a potential breach of protected health information (PHI)? Use this breach-notification decision tree, provided by Jim Sheldon-Dean, founder and director of compliance services for Lewis Creek Systems, LLC in Charlotte, VT.

1. Was there acquisition, access, use, or disclosure of PHI in violation of the Privacy Rule?

- a. NO:** Not a breach; Document the incident and the determination of "not a breach".
- b. YES:** Go to Step 2.

2. Was the information secured according to **U.S. Department of Health and Human Services** (HHS) guidance, or destroyed?

- a. YES:** Not a reportable breach; stop here. Document the incident and determination of "not a reportable breach."
- b. NO:** Go on to Step 3.

3. Was the potential breach internal to your organization AND unintentional, in good faith, with no further use, or inadvertent and within the job scope?

- a. YES:** Not a breach; stop here. Document the incident and determination of "not a breach."
- b. NO:** Go on to Step 4.

4. Can the breached information be retained in any way?

- a. NO:** Not a breach; stop here. Document the incident and determination of "not a breach."
- b. YES:** If the breached information may be retained in some way, you have a breach. Go on to Step 5.

5. Perform a risk assessment. Is there a "low probability of compromise?"

- a. YES:** If there is a low probability of compromise, the breach is not reportable; stop here. Document the incident and determination of "not a reportable breach."
- b. NO:** If there is not a low probability of compromise, you **MUST** report the breach.

Remember: If you have a small breach (affecting fewer than 500 individuals), you must report the breach to those individuals within 60 days, Sheldon-Dean says. You must also report the breach to HHS no later than 60 days after the end of the year.

If you have a large breach (affecting 500 individuals or more), you need to report the breach to the individuals affected and to HHS within 60 days, Sheldon-Dean explains. But you must also notify major media outlets of the breach when it affects more than 500 individuals in a given jurisdiction.