Workflow for Breach Notification

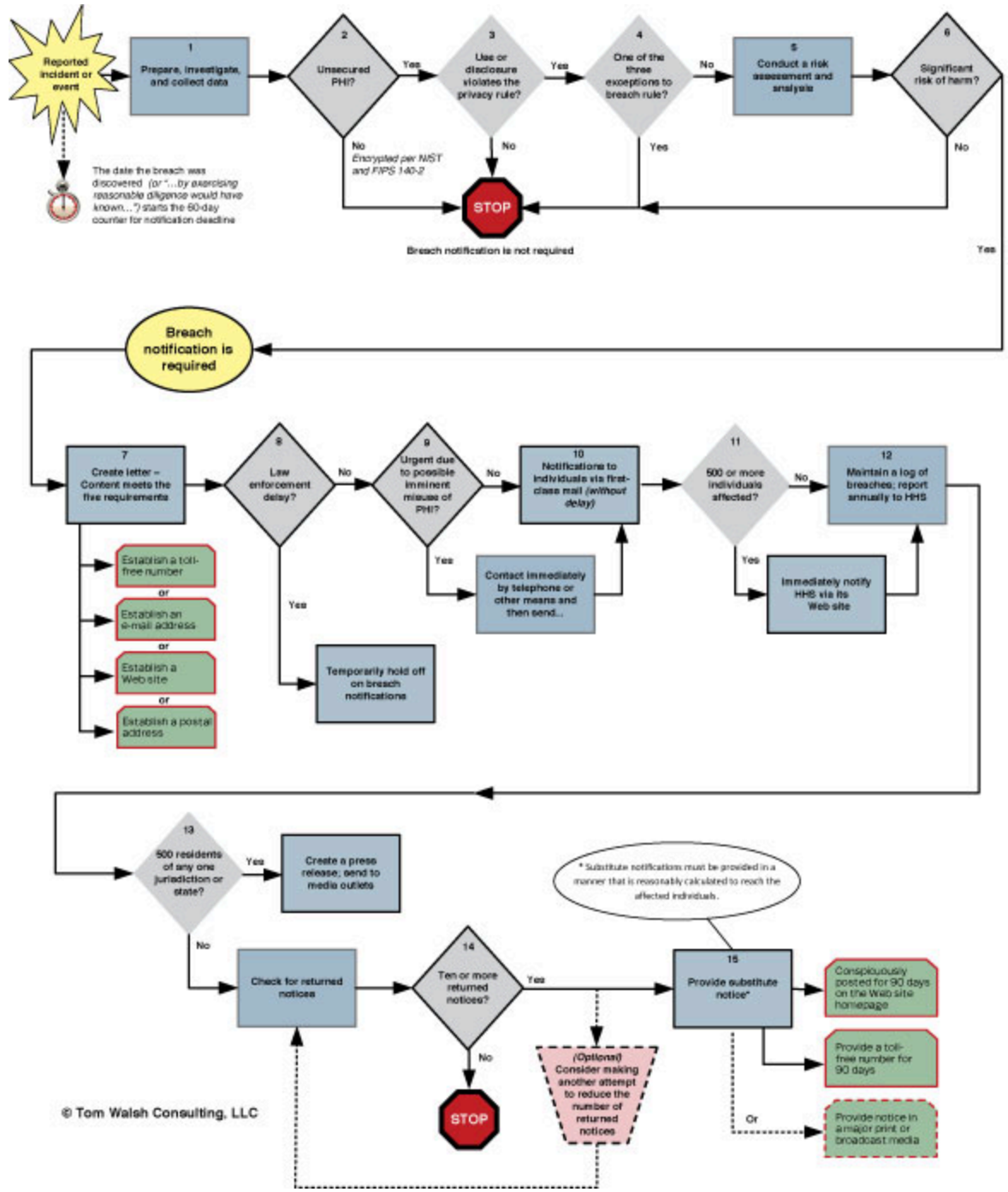
Save to myBoK

By Tom Walsh, CISSP

Federal regulations that took effect in September 2009 require HIPAA covered entities and their business associates to notify individuals if their protected health information (PHI) was accessed or disclosed in an unauthorized manner or by unauthorized individuals. Certain exemptions apply, such as incidents in which the PHI was encrypted or authorized staff accessed data accidentally.

The regulation was called for in the American Recovery and Reinvestment Act, and the Department of Health and Human Services (HHS) was tasked with promulgating the rule. HHS published an interim final rule in August 2009, and enforcement began in February. A final rule is still to come.

The regulation and its requirements run to 32 pages of description in the *Federal Register*. For purposes of planning and response, it is helpful to visualize the steps as a workflow like the one below.



1. Respond to reported incidents. Collect evidence and investigate. Capture the information necessary to file an annual report of breaches to HHS.
2. Determine if the incident involves unsecured PHI. If the PHI was encrypted and meets NIST guidelines and FIPS PUB 140-2, then a breach notification may not be required.
3. Determine if the use or disclosure of PHI violates the HIPAA privacy rule.
4. Determine if one of the three exceptions applies that would eliminate the breach notification requirement (i.e., unintentional access or inadvertent disclosure by and to authorized persons).
5. Perform a risk assessment to determine if there is a significant risk of harm to the individual. Document the risk assessment process, noting the factors that were considered and the decisions made.
6. Determine if there is significant risk or harm based upon the results of the risk assessment. Each organization bears the burden of demonstrating proof that the incident did not pose a significant risk of harm to the individual and that no breach has occurred.
7. Create a breach notification letter to the individuals whose information was used or disclosed in an unauthorized manner. Include required elements specified in the regulation (e.g., description of the event and the data involved).

8. Confirm whether the law enforcement agencies investigating the incident request that notification be delayed to prevent hindering their investigation.
9. Determine if the situation is urgent enough to require immediate notice by telephone or other means. (Direct written notice is still required.)
10. Send the breach notification letters via first-class mail without unreasonable delay and in no case no later than 60 calendar days after the breach was discovered.
11. If 500 or more individuals are affected by the breach, notify HHS via its online form without unreasonable delay and no later than 60 calendar days from discovery (http://transparency.cit.nih.gov/breach/index.cfm).
12. Record the incident in a log. All breaches involving fewer than 500 individuals must be reported to HHS annually.
13. If 500 or more individuals affected by the breach are within one jurisdiction or state, send a press release to major media outlets without unreasonable delay and no later than 60 calendar days from discovery.
14. If 10 or more notification letters are returned due to out-of-date or insufficient contact information, provide substitute notice (e.g., e-mail). Consider making additional attempts to reduce the number of returned notices and lessen the additional notification burden outlined in the next step.
15. If there are still 10 or more patients that have not been reached through mail or some other means, provide a substitute notice as required. The substitute notice must include all of the elements required for a notification letter in step 7.

Tom Walsh (twalshconsulting@aol.com) is president of Tom Walsh Consulting in Overland Park, KS.

Article citation:
Walsh, Tom. "Workflow for Breach Notification" *Journal of AHIMA* 81, no.4 (April 2010): 32-33.