

## Survivor Business Associates and the Risks of Legacy ePHI

The covered entity-business associate relationship has become measurably more complex for both parties under HITECH. Both covered entities and business associates have exposure to HITECH's substantial new penalties and OCR's forthcoming random audits.

Perhaps no aspect of the business associate relationship is more difficult to navigate than the one between a covered entity and a "survivor" business associate; that is, a business associate who no longer provides the service that gave rise to the relationship but, upon termination of the service relationship, found it not feasible to return or destroy all PHI, including ePHI. In these survivor cases, the business associate relationship continues, critical protections must continue and ePHI should literally become "legacy data", frozen in place for a use or disclosure only for the purpose that made return or destruction not feasible.

Covered entities have no duty to monitor continuously a business associate, but they do have a duty to perform the terms of the business associate agreement. Problems arise when a business associate relationship is simply allowed to expire with no documentation ending the relationship, or confirming the return or destruction of PHI, or the post-termination use/disclosure limitations and continued protections. The greatest risk may be that upon termination of services, the business associate simply assumes that data with associated ePHI can continue to reside in its database and is erroneously considered by the business associate, as "its data" which the business associate can continue to use for a variety of purposes. If the business associate engages in a use or disclosure inconsistent with its infeasibility determination, that use or disclosure could be "unauthorized" under HITECH's criminal provisions, could violate 164.504(e) and, could subject the business associate to severe penalties under HITECH.

Covered entities and HITECH regulated business associates need to revisit their previously terminated business associate agreements. Here are some questions to ask and steps to consider.

1. Inventory all terminated or expired business associate agreements, especially those with ePHI.
2. Determine how the business associate relationship was discontinued. Is there documentation that substantiates the infeasibility of "return or destroy?" "Infeasible" should mean more than commercially inconvenient or disadvantageous to the business associate.
3. Do the external or internal conditions necessitating infeasibility for "return or destroy" continue to exist (e.g., the contract mandated period for an audit has expired)?
4. For those relationships with acknowledged post-termination continuing obligations (e.g., ePHI has been aggregated and data is hopelessly commingled), confirm that protections are in place and uses/disclosures are limited.
5. During the post-termination period, did the business associate report any unauthorized uses or disclosures or relevant security incidents?
6. Can the business associate demonstrate that there have been no improper uses or disclosures of the ePHI that are unrelated to the reasons for return or destruction was in-feasible?
7. Have the relevant information systems implicated by the infeasibility assessment changed? If so, should protections change? For example, if PHI has been digitized to ePHI, can it be encrypted to insure maximum use restriction?
8. For those business associate relationships without adequate documentation of termination, return or destruction and use/disclosure limitation, request assurances that appropriate steps were taken.
9. For relationships with acknowledged post-termination continuing obligations, request the addition of agreed upon breach notification procedures. Nothing in the breach notification rules suggest that they are inapplicable to legacy ePHI.
10. If the business associate has improperly used or disclosed legacy PHI on or after February 17, 2010, then both the business associate and the covered entity may need to undertake breach reporting compliance activities.

Proper termination of the covered entity-business associate relationship is a shared responsibility between the parties to the business associate agreement. Rarely does the relationship just go away quietly. Before legacy ePHI held by a survivor business associate turns up on a missing laptop, covered entities need to re-visit these relationships.

If you have any questions about the above E-Flash, or need assistance with HIPAA privacy, security or breach notification legal issues, please contact Edward F. Shay at (215) 587-1151 or [eshay@postschell.com](mailto:eshay@postschell.com).

**Disclaimer:** this E-Flash does not offer specific legal advice, nor does it create an attorney-client relationship. You should not reach any legal conclusions based on the information contained in this E-Flash without first seeking the advice of counsel.

© Copyright 2010 Post & Schell, P.C. All rights reserved  
"POST & SCHELL" and the Post & Schell Logo are registered trademarks of Post & Schell, P.C.  
[About Us](#) | [Our Attorneys](#) | [Practice Areas](#) | [Publications](#) | [Offices](#)