

Risk Prevention/Management Advice to Hospitals Regarding Document-Sharing Technology

Hospitals, multi-hospital systems, and integrated healthcare delivery systems are increasingly utilizing data-sharing technology to communicate with, and share documents among, their officers and directors.

For example, some healthcare business enterprises use online services to upload documents to a "secure" Internet web site for Board members' review prior to Board meetings, in lieu of sending out such documents via e-mail or in paper form. Healthcare business enterprises using such services need to be aware of many potential security and privacy risks inherent in transmitting, uploading and storing sensitive, confidential or even proprietary information via the Internet.

Communications to a hospital Board may include:

- Confidential information regarding the hospital's operations or personnel;
- Data on non-public commercial and financial affairs of the hospital;
- Legally privileged information regarding law suits on behalf of or against the hospital; and
- Confidential and privileged peer review materials, including protected health information (PHI, as defined under HIPAA) of the hospital's patients.

Prior to acquiring or using such data-sharing technology, healthcare business enterprises should make sure that the software is secure and that both the enterprise and the service provider use appropriate physical and technical security safeguards to protect personal and otherwise protected information. There is no one fail-safe approach to implementation and operation of data-sharing technology, and such technology should be customized to fit the enterprise's needs and requirements. However, at minimum, preliminary precautions should include:

- Knowing exactly what information is being distributed, via what channels (*e.g.*, whether it is contained on a laptop, another portable device or on the network);
- Avoiding access, storage, sharing, or use (including downloading, printing, or e-mailing) of information from or via unsecured home office computers or other mobile devices;
- As much as possible, limiting the unencrypted sensitive data being transmitted;
- Avoiding use of actual personal or confidential data in testing of the software;
- Implementing access control checks, including restricting access to essential personnel only;
- Using intrusion detection technology or procedures to quickly detect any unauthorized access; and
- Training and educating all relevant personnel and all persons with access to such information regarding the enterprise's data privacy protection policies and procedures.

In order to protect your healthcare business enterprise, your Legal and IT teams should negotiate an agreement with the service provider which, at minimum, includes the following provisions:

- A warranty from the service provider that their product is safe, secure, and complies with all applicable privacy and security standards;
- A requirement for the software provider to comply with your institutional privacy and security policies, as well as all applicable laws and regulations;
- An explicit prohibition for the service provider to use, communicate, divulge, exploit, duplicate, distribute, publish, reproduce, transfer, dispose of, recreate, modify, or create derivative works based upon or

otherwise reveal or make available to any third party, directly or indirectly, for any purpose, except as provided in such contract; and

- Indemnification, remedies, limitation of liability, and other provisions protecting your business enterprise for any damages resulting from a data breach or loss, in instances where such breach or loss are caused by the purchased software or the service provider.

Finally, the agreement with the service provider should include a Business Associate Agreement (BAA, as defined under HIPAA); however, please keep in mind that the BAA should acknowledge the changes mandated by the recent [American Recovery and Reinvestment Act of 2009](#), as well as numerous new regulations to be promulgated by the Secretary of Health and Human Services under this Act.

For additional information, please feel free to contact Steven J. Fox at SJFox@PostSchell.com (202-661-6940), Ed Shay at EShay@PostSchell.com (215-587-1151), or Vadim Schick at VSchick@PostSchell.com (202-661-6945).

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 2009 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](#)