iatricSystems™

Vendor Risk Assessment

5-step assessment to understand the risk with your 3rd party vendors

To better protect patient privacy, the HIPAA Omnibus Final Rule has changed the obligations and liabilities between hospitals and their business associates — the focus is now on the relationship, not just the written agreement. If one of your business associates violates PHI, you're both subject to huge fines.

It is essential to keep the processes and workflow between health organizations and their associates smooth and productive and, at the same time, understand the associated risk with their access to Protected Health Information (PHI).

This assessment will help you understand your overall risk with your 3rd party vendor relationships and agreements.

A guide to understanding your overall risk with your 3rd party vendors.

Understand Your Risk	Yes	No
1. Do you have an automated process for assigning risk that characterizes vendors in terms of data classification, history, and agreement terms?		
• **Data Classification** defines attributes associated with the data the vendor has access to — such as the sensitivity of the data, repositories, and breach history		
• **History** indicates the level of compliance with the HIPAA Security and Privacy Rules, in the areas of destruction of data, encryption, and risk management		
• **Terms** describe the document status of the agreement including PHI safeguards, notification of disclosures, termination after breach clause, and right to audit clause		
2. Can you prioritize your vendors in terms of risk?		
3. Can you determine which vendors require additional evaluation based on the assignment of risk? Do you have the ability to:		
• Access questionnaires and send questionnaires to specific vendors		
• Spot check the security controls defined on the questionnaire		
• Conduct a security assessment		
4. Do you have the ability to monitor progress and report findings and deficiencies for further investigation?		
5. Are you alerted when users associated with a terminated business associate agreement are identified as accessing PHI?		

5-step assessment to understand the risk with your 3rd party vendors

Continued

If you answered “NO” to some of these questions, your organization may be vulnerable to breaches from your business partners and face costly penalties. iatricSystems Partner Risk Manager™ can simplify the process of identifying, monitoring, and managing your business partners and contracts to create a culture of ensuring trust and protecting patient privacy.

With Partner Risk Manager, you can:

- Monitor the risk of third-party vendors and agreements, understand those that need to be updated
- Keep informed of the status of your third-party vendors through risk determination
- Accomplish screening, tracking and cross-department collaboration related to vendors and agreements
- Prepare for OCR audit with complete reporting to document BA oversight
- Simplify vendors’ compliance tasks to build better partnerships and a culture of compliance
- Automate workflow logic with customized pre-contract questionnaires
- Evaluate the use of PHI, volume and frequency of data, how data is stored, processed, transmitted, and destroyed and much more
- Generate system alerts when a user associated with a terminated agreement accesses PHI (Requires Security Audit Manager™)

Turn to iatricSystems with confidence.

Your purpose is delivering quality patient care. Ours is making sure that your challenge of adhering to patient data privacy regulations never interferes with that purpose. Contact us to ensure that your business partners are a positive addition to the patient care you provide and not a risk to your patients’ privacy.

For more information on Partner Risk Manager please contact us using the information below.

iatricSystems™

Ph: 978.805.4100 Fax: 978.805.4101 info@iatric.com security.iatric.com