Cyber GRX

A Checklist for Third-Party Cyber Risk Management in Healthcare Organizations

Identify and mitigate cyber risk due to third parties while balancing the need to become more agile and protect electronic personal health information (EPHI). The following is what our solution engineers would advise if creating an effective TPCRM program from scratch.

1. Vendor Classification

The vendor class will tell you a lot about how to manage your relationship, not only how much scrutiny to apply during the pre-contract due-diligence phase but also throughout the duration of the vendor relationship.

- [ ] **Vendor Risk Tiering**

  Classify the exposure created by your vendors by assessing the likelihood and impact of a cyber event.

2. Begin the Assessment

After classifying vendors, you will know what the scope of the assessment should be.

- [ ] **Determine Assessment Scope & Necessary Questions**

  Each vendor tier will have a corresponding assessment scope – high risk vendors should be assessed via a questionnaire and a corresponding on-site evaluation, while lower risk vendors can be assessed with a lower level of rigor such as a questionnaire and desktop document validation.

- [ ] **Self-Assessment**

  Regardless of tier classification, each vendor should complete a self-assessment questionnaire. The questionnaire should only include relevant questions that show what level of risk a vendor will expose you to. Include well documented expectations and guidelines, as well as a deadline.

- [ ] **Validate Vendor Assertions**

  Examine evidence provided by your vendor that prove their controls are operating effectively, such as policies, procedures, audit results, etc.

- [ ] **Ongoing Monitoring**

  Continually update your data as changes in relationships with your vendors occur.

3. Issue-Based Scoring

A well-designed questionnaire should have a corresponding analysis component. Scoring a questionnaire can be difficult, but it's important to know issue status as it evolves – which is why we suggest issue-based scoring.

- [ ] **Create a Matrix**

  Relate your questions to negative answers to issue severity and mitigation strategies.

- [ ] **Track issues**

  Know the status of each issue at all times – this way, no exposure will go unaddressed.

- [ ] **Address Findings**

  Hold your vendors accountable for helping you close the issues that must be addressed. Ensure your program policies clearly lay out how the severity of the problem will affect its handling and that the process be repeatable. This will ensure consistency in your approach.

Building a strong TPCRM program is essential to the security of your organization and the sensitive data you collect. Each component will require constant fine tuning, especially while your program evolves in maturity and sophistication.

CyberGRX is on a mission to modernize third-party cyber risk management for the healthcare industry. The platform was created with the help of design partners such as Aetna for an emphasis on healthcare and healthcare-focused regulations. Built on the market's first third-party cyber risk exchange, our dynamic and scalable approach is innovating TPCRM for enterprises and third parties. Armed with fast and accurate data and a proven and innovative approach, CyberGRX customers make rapid, informed decisions and confidently engage with partners.

If you're looking for an innovative, dynamic approach, **schedule a demo** or read our **Vendor Risk Management Guide** to learn more.

Cyber GRX