HIPAA/HITECH Checklist

The HIPAA/HITECH Privacy and Security Rules provide a valuable framework for protecting participants' and beneficiaries' data. Fulfilling your obligation to protect this information is important because of increased attacks on entities with valuable information as well as because of increased enforcement activity by regulatory agencies, through complaints, breach reports and random audits.

The consequences of failing to comply with the rules and regulations of HIPAA/HITECH can be severe for your organization. There is a tiered penalty structure for civil monetary penalties, based on intent behind the violation. Penalties and resolution agreements can result in payment of millions of dollars per year for breach of one or more standards.

☐ 1 HIPAA Security/HITECH risk assessment within the last three years

- ✓ Perform a HIPAA/HITECH risk assessment at least every two to three years — or whenever your IT environment has a significant change that could affect the security of ePHI, such as a new server or adoption of new mobile devices.
- ✓ Make sure the risk assessment reviews the application standards/implementation specifications; includes factual findings; determines the risk to ePHI and makes recommendations for addressing issues identified. And then address those issues! It's good to know your vulnerabilities — it's even better to minimize them.

☐ 2 Up-to-date policies, procedures and business associate agreements

- ✓ Develop policies and procedures that comply with the Security Rule, are reasonable and appropriate for your organization's size and capabilities and address bring-your-own-device policies.
- ✓ Establish Privacy Rule policies that ensure PHI is protected and can continue to be used by the plan for treatment, payment and healthcare operations purposes.
- ✓ Publish a Notice of Privacy Policies and Procedures and provide it to new enrollees upon enrollment. Thereafter, notify participants at least once every three years of the notice's availability and how to obtain it.
- ✓ Designate privacy officials for both privacy and security.
- ✓ Ensure business associate agreements are in place with all vendors, keeping in mind that the Department of Health and Human Services (HHS) now considers hosting and storage vendors, as well as cloud services, to be business associates.
- ✓ Enforce these policies and procedures! They do no good if they're simply pieces of paper.

☐ 3 Ongoing staff training

- ✓ Conduct and document high-quality privacy and security awareness and training and retraining program for all staff, as required by the Privacy and Security Rules.
- ✓ Include HIPAA training in the onboarding process; provide refreshers at least annually that keep pace with evolving and increasingly complex cybersecurity threats and send security reminders at least quarterly.
- ✓ Promote a strong cybersecurity culture, so everyone in your organization understands the value of the information your organization is entrusted with, as well as the ramifications for participants and beneficiaries if that data and information is compromised.

Segal

4 Processes in place to detect and report HITECH breaches

- ✓ Ensure a process is in place to examine security incidents and determine whether they constitute a reportable breach.
- ✓ Be prepared to provide notice of a breach of unsecured PHI without unreasonable delay, and to address breaches by your business associates.
- ✓ Send the notice to impacted individuals, the media (in certain instances) and HHS within 60 days after discovery of the breach.

5 Monitoring business associates

- ✓ Have contracts with your business associates in place to uphold HIPAA privacy and security standards and keep PHI confidential.
- ✓ Make sure your business associates are aware that they have a direct statutory duty under HITECH to:
  - Comply with the privacy-related obligations in their HIPAA business associate agreements
  - Report a breach of unsecured PHI to the covered entity
  - Enter into sub-business associate agreements with their subcontractors and agents, which are also considered business associates
- ✓ Keep in mind that business associates are now directly subject to audits by HHS and to HIPAA's civil monetary and criminal penalties

6 System access control and activity review

- ✓ Watch out for these HIPAA access control red flags:
  - Inadequate encryption policies and procedures
  - Insufficient access control and activity review
  - Poor mobile device and laptop policies and control
  - Lack of IT governance — standards, inventory control, basic security procedures (i.e., patching and administrative lockdown)
  - Inadequate disaster recovery procedures
  - Incomplete IT policies and procedures
  - Lack of advanced monitoring techniques — intrusion detection system/intrusion prevention system, log correlation and data-loss prevention
- ✓ Assess any new technologies according to the HIPAA Security/HITECH rules. Examples include cloud migration, mobile and portable storage devices, protection against malicious software, security information and event management tools, text and instant messaging, transactional websites and benefit administration systems.

We can help you manage your HIPAA privacy and security issues with confidence.

Melanie Walker, JD
SVP, National Compliance Practice Leader
mwalker@segalco.com
303.241.5880

Michael Stoyanovich, CDPSE
VP and Senior Consultant
mstoyanovich@segalco.com
248.910.2637

Segal