**DATA BREACH CHECKLIST**

***Breach Prevention and Preparation***

* Obtain cyber liability insurance
* Establish relationships with external parties (*e.g.*, patient notification, call center services, credit monitoring, IT forensics and counsel)[[1]](#footnote-1)
* Identify **ALL** ePHI your organization creates, receives, maintains or transmits
* Conduct a risk analysis and develop a risk management plan
* Implement, and maintain documentation of, appropriate security measures (*e.g.*, encryption, firewalls and intrusion detection systems)
* Implement policies and procedures that address the requirements of the HIPAA Privacy, Security and Breach Notification Rules
* Create an incident response team and define team member role and responsibilities
* Create and test an incident response plan
* Train workforce members on how to identify and report security incidents

***Breach Response***

* Notify cyber insurance carrier
* Engage external parties (*e.g.*, patient notification, call center services, credit monitoring, IT forensics and counsel)
* Contain breach source, if necessary
* Consider notifying law enforcement
* Determine who and what was affected
* Notify necessary parties and agencies within applicable timeframes
* Sanction responsible workforce member(s), if applicable
* Document all mitigation steps taken
* Prepare for and respond to inquiries from government agencies

***Post-Breach***

* Update your risk analysis and risk management plan
* Revise policies and procedures, as necessary
* Retrain workforce members
* Evaluate incident response plan and revise as necessary

1. Your cyber insurance carrier may have preferred vendors. [↑](#footnote-ref-1)