HIPAA Omnibus Rule Modifications Compliance Checklist

For Covered Entities

☐ Update Notice of Privacy Practices and post on website
☐ Update Patient Authorization Form
☐ Update privacy policies, including the following:
  ☐ Uses and Disclosures of Patient Information to include reference to genetic information, sale of protected health information, restriction on disclosure of information to health plan if the service is paid in full by patient and disclosure of patients’ records deceased over a 50-year period
  ☐ Use and Disclosure of Protected Health Information for Marketing Activities
  ☐ Use and Disclosure of Protected Health Information for Fundraising Activities
☐ Implement a process for requests to disclose immunization records to schools as required by law
  ☐ Prepare Authorization Form for disclosure of immunization records to schools
☐ Implement a form for Patient Requests to Restrict Disclosure of Protected Health Information to a Health Plan
☐ Update Patient Record Request form to include the option of providing an electronic copy to patient
☐ Update list of business associates and amend Business Associate Agreements
☐ Update Breach Notification Compliance Plan
☐ Ensure there is a process for confirming that business associates have entered into written contracts with subcontractors and vendors and that the subcontractors’ policies and procedures are HIPAA compliant

For Business Associates

☐ Implement privacy policies:
  ☐ Uses and Disclosures of Patient Information
  ☐ Patient Access to Health Information
  ☐ Accounting of Disclosures
  ☐ Amendment of PHI
  ☐ Confidentiality and Non-disclosure Agreement
☐ Implement Security Policies. The following Security Policies are required by the Security Rule:
  ☐ Information Security Risk Analysis Policy
  ☐ Information Security Risk Management Policy
Information Security Disciplinary Action Policy
Information Security Audit Controls and System Activity Review Policy
Security Incident Response and Reporting Policy
Data Backup and Storage Policy
Disaster Recovery Plan Policy
Emergency Mode Operations Policy
Workstation Use Policy
Disposal Policy
Media Re-Use Policy
EPHI Movement Policy

- Assign information security responsibility to a Security Officer
- Implement a HIPAA Privacy and Security Awareness Training Program for all employees and document same
- Ensure written contracts are in place with all subcontractors or vendors, meaning any person to whom you delegate a function, activity, or service, other than in the capacity as a member of your workforce, who creates, receives, maintains or transmits protected health information that the subcontractor or vendor agrees to the same restrictions and conditions applicable to the access, use, and disclosure of PHI as the business associate
- Implement Breach Notification Compliance Plan

For Health Plans (excluding an issuer of a long-term care policy)

- Update Notice of Privacy Practices and post on website
- Ensure policies are in place restricting the use of genetic information for underwriting purposes

Miscellaneous

- Update patient authorization form for research study

The HIPAA Omnibus Modifications Compliance Checklist was prepared by Linn Foster Freedman, Leader of the Nixon Peabody Privacy & Data Protection Group and Chair HIPAA Compliance Team. For more information, contact Linn at lfreedman@nixonpeabody.com or 401-454-1108.
For additional resources, visit www.nixonpeabody.com/HIPAA_Omnibus_Rule