Sample - Interview and Document Request for HIPAA Security Onsite Investigations and Compliance Reviews

1. Personnel that may be interviewed
   - President, CEO or Director
   - HIPAA Compliance Officer
   - Lead Systems Manager or Director
   - Systems Security Officer
   - Lead Network Engineer and/or individuals responsible for:
     - administration of systems which store, transmit, or access Electronic Protected Health Information (EPHI)
     - administration systems networks (wired and wireless)
     - monitoring of systems which store, transmit, or access EPHI
     - monitoring systems networks (if different from above)
   - Computer Hardware Specialist
   - Disaster Recovery Specialist or person in charge of data backup
   - Facility Access Control Coordinator (physical security)
   - Human Resources Representative
   - Director of Training
   - Incident Response Team Leader
   - Others as identified….

2. Documents and other information that may be requested for investigations/reviews
   a. Policies and Procedures and other Evidence that Address the Following:
      - Prevention, detection, containment, and correction of security violations
      - Employee background checks and confidentiality agreements
      - Establishing user access for new and existing employees
      - List of authentication methods used to identify users authorized to access EPHI
      - List of individuals and contractors with access to EPHI to include copies pertinent business associate agreements
      - List of software used to manage and control access to the Internet
      - Detecting, reporting, and responding to security incidents (if not in the security plan)
      - Physical security
      - Encryption and decryption of EPHI
      - Mechanisms to ensure integrity of data during transmission - including portable media transmission (i.e. laptops, cell phones, blackberries, thumb drives)
      - Monitoring systems use - authorized and unauthorized
      - Use of wireless networks
      - Granting, approving, and monitoring systems access (for example, by level, role, and job function)
      - Sanctions for workforce members in violation of policies and procedures governing EPHI access or use
      - Termination of systems access
• Session termination policies and procedures for inactive computer systems
• Policies and procedures for emergency access to electronic information systems
• Password management policies and procedures
• Secure workstation use (documentation of specific guidelines for each class of workstation (i.e., on site, laptop, and home system usage)
• Disposal of media and devices containing EPHI

b. Other Documents:
• Entity-wide Security Plan
• Risk Analysis (most recent)
• Risk Management Plan (addressing risks identified in the Risk Analysis)
• Security violation monitoring reports
• Vulnerability scanning plans
  o Results from most recent vulnerability scan
• Network penetration testing policy and procedure
  o Results from most recent network penetration test
• List of all user accounts with access to systems which store, transmit, or access EPHI (for active and terminated employees)
• Configuration standards to include patch management for systems which store, transmit, or access EPHI (including workstations)
• Encryption or equivalent measures implemented on systems that store, transmit, or access EPHI
• Organization chart to include staff members responsible for general HIPAA compliance to include the protection of EPHI
• Examples of training courses or communications delivered to staff members to ensure awareness and understanding of EPHI policies and procedures (security awareness training)
• Policies and procedures governing the use of virus protection software
• Data backup procedures
• Disaster recovery plan
• Disaster recovery test plans and results
• Analysis of information systems, applications, and data groups according to their criticality and sensitivity
• Inventory of all information systems to include network diagrams listing hardware and software used to store, transmit or maintain EPHI
• List of all Primary Domain Controllers (PDC) and servers
• Inventory log recording the owner and movement media and devices that contain EPHI