| ACE-0000 | HIPAA Security Rule Compliance | • Justification for policies  
• ACE approach towards HIPAA compliance  
• Crosswalk of HIPAA Security Rule sections with existing VCU, VCUHS and Virginia Premier security policies |
| --- | --- | --- |
| ACE-0001 | Security Rule General Rules | • Mandate for compliance with HIPAA Security Rule  
• Implementation requirements |
| ACE-0002 | HIPAA Security Management Process | • Security management program overview  
• Standards for HIPAA compliance  
• Assignment of responsibilities |
| ACE-0003 | HIPAA Security Sanctions | • Human Resources sanction process  
• Communications of Sanction Policy to staff  
• Responsibilities for reporting policy violations |
| ACE-0004 | Assigned Security Responsibility | • Assignment of ACE Information Security Officer |
| ACE-0005 | Workforce Security | • Responsibilities of Resource Owners and Approvers  
• Access Management standards and controls |
| ACE-0006 | Information Access Management | • Access Authorization Process  
• Training requirements |
| ACE-0007 | Security Training & Awareness | • Training & Awareness requirements & responsibilities |
| ACE-0008 | Security Incident Procedures | • Requirements for Incident Reporting and Response |
| ACE-0009 | Contingency Plan | • Requirement for documented Contingency Plan  
• Business Impact Analysis  
• Outage communications |
| ACE-0010 | Evaluation | • Requirement for periodic or “for cause” audits for HIPAA compliance |
| ACE-0011 | Business Associate Contracts and Other Arrangements | • Description of Business Associate Agreement  
• Responsibility for development of BAA |
| ACE-0012 | Workstation Use | • Workstation definitions  
• ACE requirement for minimum workstation standards  
• Purchase review responsibility & process |
| ACE-0013 | Workstation Security | • Requirement for basic workstation security safeguards |
| ACE-0014 | Device & Media Controls | • Life Cycle Planning for systems  
• Inventory requirements  
• Standards for relocation or decommissioning of system  
• Re-use and destruction of removable media |
| ACE-0015 | Access Controls | • Controls for ensuring appropriate access to ePHI  
• Responsibilities for access management |
| ACE-0016 | Audit Controls | • Requirement for audit trails  
• Responsibility for implementing monitoring  
• Audit log review requirements |
| ACE-0017 | Integrity Controls | • Requirement to prevent improper alteration of records  
• Controls for ensuring “minimum necessary” access  
• Detection of inappropriate access or damage |
| ACE-0018 | Person or Entity Authentication | • Requirement for identification prior to authorization  
• Remote access authentication requirements |
| ACE-0019 | Policies & Procedures and Documentation Requirements | • Requirement for guidance documentation for HIPAA compliance |
| ACE-0020 | Network Firewall DMZ Transmission Security Measures | • Firewall implementation requirement  
• DMZ requirements |
| ACE-0021 | *** Retired *** | |
| ACE-0022 | Transmission Security | • Requirements for encryption of stored/transmitted data  
• Protocols blocked on networks  
• Periodic penetration testing guidelines  
• Wireless security control standards |
| ACE-0033 | Encryption and Decryption | • Use of approved encryption algorithms |