Assured SPC

SECURITY + PRIVACY = COMPLIANCE

HIPAA Privacy and Security Documentation Requirements for Business Associates

I - PRIVACY

Safeguard	Safeguard Class	Requirement	Governing Reg.	Examples of Supporting Documentation
General	Business Associate	Organization is defined as a HIPAA Business Associate	§160.103(3)	Acknolwedgement that the organization is a classified as a Business Associate under HIPAA
Administrative	Business Associate	Uses and Disclosures, General	§164.502(e)	Sample Business Associate Agreement
		Uses and Disclosures, Organizational	§164.504(e)	Sample Business Associate Agreement
	Other Requirements	Minimum Necessary	§164.514	Sample Business Associate Agreement
		Training	§164.530(b)(1)	Evidence of HIPAA training for all relevent workforce members and HIPAA section of Employee Handbook

II - SECURITY

Safeguard	Safeguard Class	Requirement	Governing Reg.	Examples of Supporting Documentation
Administrative	Security Management	HIPAA Risk Analysis	§164.308(a)(1)	HIPAA Risk Analysis
		HIPAA Risk Management Plan	§164.308(a)(1)	HIPAA Risk Management Plan, based upon completed HIPAA Risk Analysis
		Sanction Policy	§164.308(a)(1)	Sanction Policy
		Information System Activity Review	§164.308(a)(1)	Audit logs or automated system activity reports
	Assigned Security Responsibility	Assigned Security Responsibility	§164.308(a)(2)	Specific Job Position Policy or Org Chart w/ clearly defined job definitions
	Workforce Security	Authorization and Supervision	§164.308(a)(3)	Evidence of process to approve access to PHI
		Workforce Clearance Procedure	§164.308(a)(3)	Evidence of process of which specific workforce roles and members receive access to PHI
		Termination Procedures	§164.308(a)(3)	HR Termination Procedures and Sanctions Policy
	Information Access Management	Isolated Health Care Clearinghouse Function	§164.308(a)(4)	Any policies and procedures related to security and information access IF the business processes PHI or PII and qualifies as a healthcare clearinghouse
		Access Authorization	§164.308(a)(4)	Evidence of process for granting access to PHI for cleared workforce members
		Access Establishment and Modification	§164.308(a)(4)	Evidence of access priviledgesto workforce members, including workforce change management
	Security Awareness and	Security Awareness and Training	§164.308(a)(5)	Evidence of security awareness training and testing
		Security Reminders	§164.308(a)(5)	Evidence of security reminders
		Protection from Malicious Software	§164.308(a)(5)	Security Plan, Penetration Test and Vulnerability Scan Report, Intrusion Detection System Log or Report
		Log-In Monitoring	§164.308(a)(5)	Evidence of log-in monitoring

Safeguard	Safeguard Class	Requirement	Governing Reg.	Examples of Supporting Documentation
Administrative, cont.		Password Management	§164.308(a)(5)	Evidence of password management
	Security Incident	Response and Reporting	§164.308(a)(6)	Incident Response Plan, including test results
	Contingency Plan	Data Backup Plan	§164.308(a)(7)	Data Backup/Restore Plan or Business Contingency Plan
		Disaster Recovery Plan	§164.308(a)(7)	Disaster Recovery Plan or Business Contingency Plan
		Emergency Mode Operation Plan	§164.308(a)(7)	Emergency Mode Operation Plan or Business Contingency Plan
		Testing and Revision Procedure	§164.308(a)(7)	Testing Plan and Test Results for Business Contingency Plan or individual plans
		Application and Data Criticality Analysis	§164.308(a)(7)	Security Plan or Data Classification Table and Business Continuity Plan
	Evaluation	Evaluation	§164.308(a)(8)	Evidence of ongoing security monitoring and evaluation, including Penetration Test and Vulnerability Scan Reports
	Business Associate	Business Associate Contracts and Other	§164.308(b)(1)	Sample Business Associate Agreement
Physical	Facility Access Controls	Contingency Operations	§164.310(a)(1)	Business Contingency Plan, including test results
		Facility Security Plan	§164.310(a)(1)	Security Plan
		Access Control and Validation	§164.310(a)(1)	Access Control Plan and Workforce Validation Procedures
		Maintenance Records	§164.310(a)(1)	Maintenance Logbook or Security Plan
	Workstation Use	Workstation Use	§164.310(b)	Workstation Acceptable Use Policy
	Workstation Security	Workstation Security	§164.310(c)	Workstation Security Policy or Security Plan
	Device and Media Controls	Disposal	§164.310(d)(1)	Media Re-use and Disposal Policy
		Media Reuse	§164.310(d)(1)	Media Re-use and Disposal Policy
		Accountability	§164.310(d)(1)	Media Control Policy, Media Log or Electronic Tracking Measures
		Data Backup and Storage	§164.310(d)(1)	Data Backup/Restore Plan
Technical	Access Control	Unique User Identification	§164.312(a)(1)	Evidence of unique user identification at system login
		Emergency Access Procedure	§164.312(a)(1)	Business Continuity Plan or evidence of procedures to access PHI during an emergency situation
		Automatic Logoff	§164.312(a)(1)	Evidence of automatic system logoff after reasonable period of inacvtivity
		Encryption and Decryption	§164.312(a)(1)	Security Plan or evidence of data encrpytion, at rest and in transit
	Audit Controls	Audit Controls	§164.312(b)	Audit Reports or Automated Activity Monitor
	Integrity	Mechnism to Authenticate PHI	§164.312(c)(1)	Security Plan or Data Integrity Policy, Penetration Test and Vulnerability Scan Report
	Person or Entity Authentication	Person or Entity Authentication	§164.312(d)	Security Plan or evidence of access control methods utilized for external resources
	Transmission Security	Integrity Controls	§164.312(e)(1)	Security Plan or other evidence that data is secure in transit
		Encryption	§164.312(e)(1)	Security Plan or other evidence that data is encrypted in transit
Organizational	Business Associate Contracts and Other	Business Associate Contracts and Other Arrangements	§164.314(a)(1)	Sample Business Associate Agreement and other agreements containing security and privacy requirements for PHI sent or received
	Requirements for Group	Requirements for Group Health Plans	§164.314(b)(1)	Not Applicable
	Policies and Procedures	Policies and Procedures	§164.316(a)	Evidence that "reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements" are met
	Documentation	Time Limit	§164.316(b)(i)	Evidence that policies and procedures required by 164.316(a) are retained for (6) years from date of creation

Safeguard	Safeguard Class	Requirement	Governing Reg.	Examples of Supporting Documentation
Organizational, cont.		Availability	§164.316(b)(ii)	Evidence that policies and procedures required by 164.316(a) are made available to all necessary workforce members
		Updates	§164.316(b)(iii)	Evidence that all HIPAA documentation is reviewed periodically and updated as needed, in response to environmental or operational changes affecting the security of ePHI

III - ADDITIONAL Information not required by CFR but may be requested by OCR during a formal Audit

Safeguard	Safeguard Class	Requirement	Governing Reg.	Examples of Supporting Documentation
Additional		Explanation of unimplemented addressable standards	N/A	HIPAA Remediation Task List
		Third-Party Vendor Management Policy	N/A	Evidence of third-party vendor management security requirements
		Software Development Life Cycle Plan	N/A	SDLC Plan or DevOps Security Plan
		Safe Software Test Plan	N/A	Evidence of sofware security testing (Dev only)