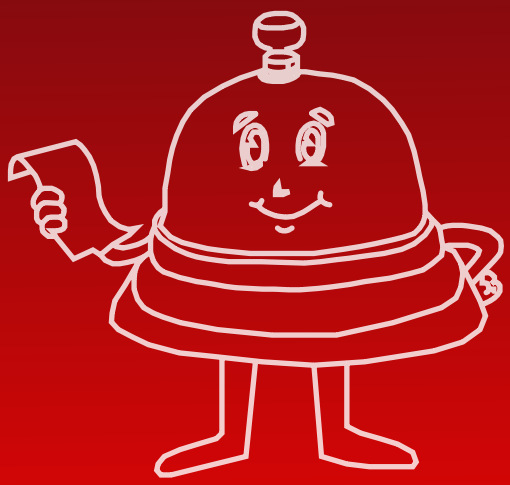
KLEAP

CYBERSECURITY

HIPAA Compliance Checklist



Brief Overview

This checklist is designed to give you a working clarity of what is required under HIPAA Compliance.

It maps every administrative, physical, and technical safeguard in the HIPAA Rules to the specific evidence required to demonstrate that each control is implemented.

For each control, it tells you what an auditor or regulator expects to see, so you are never in a position of having a policy on paper that cannot be backed by proof.

Use it to run an internal gap assessment, build your evidence library ahead of an audit, or validate that your compliance program reflects what is really happening in your organization.

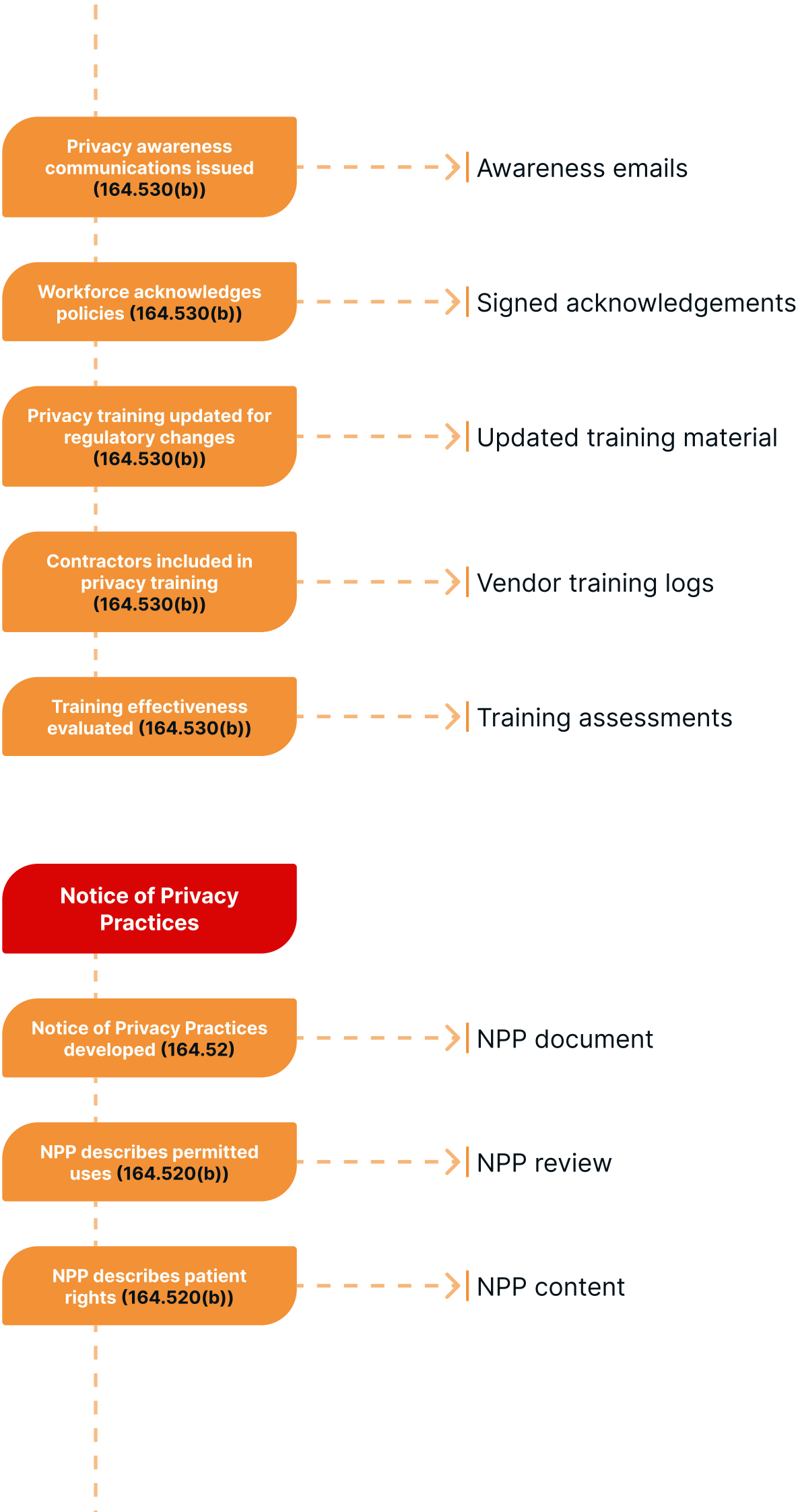
Table of Contents

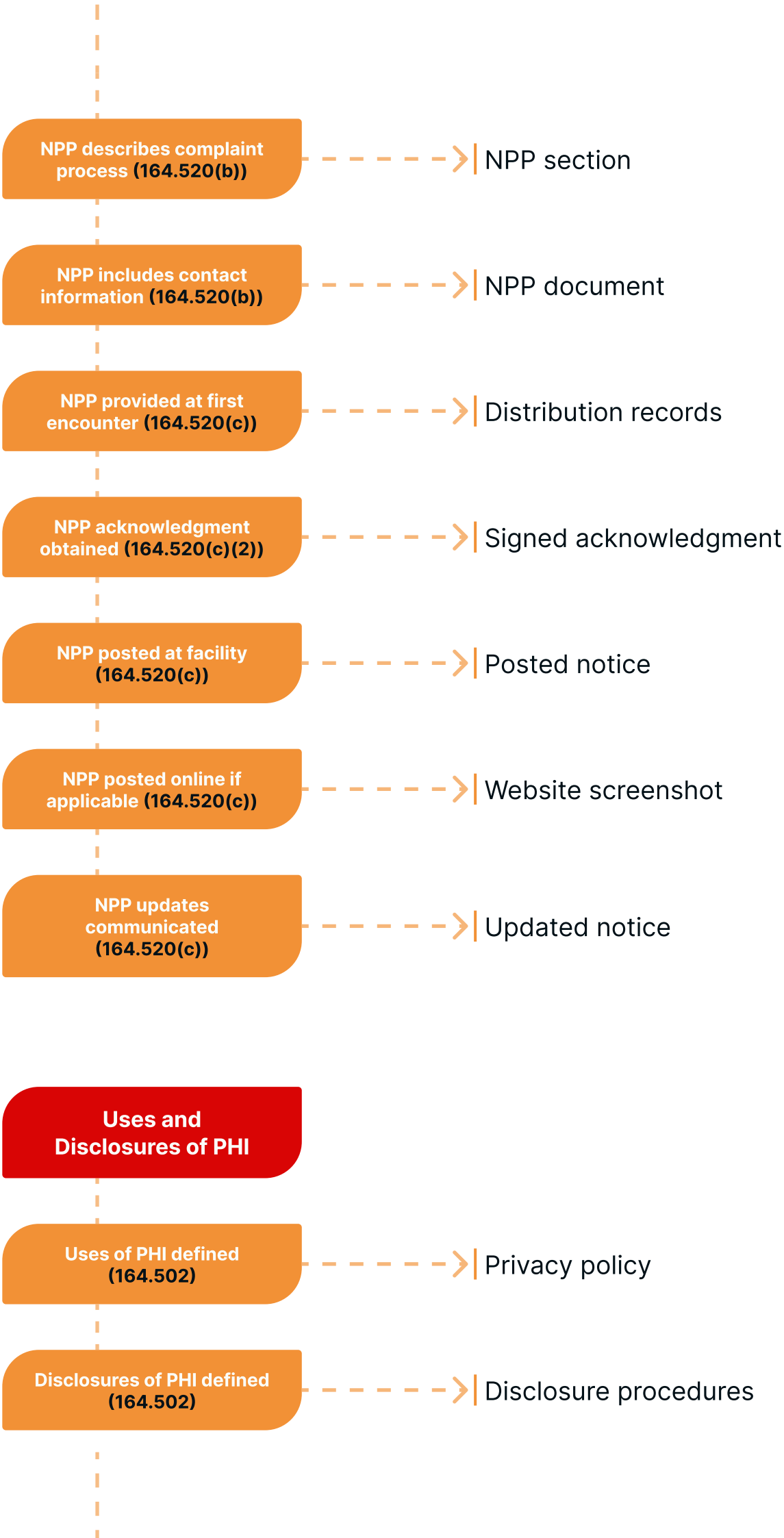
01

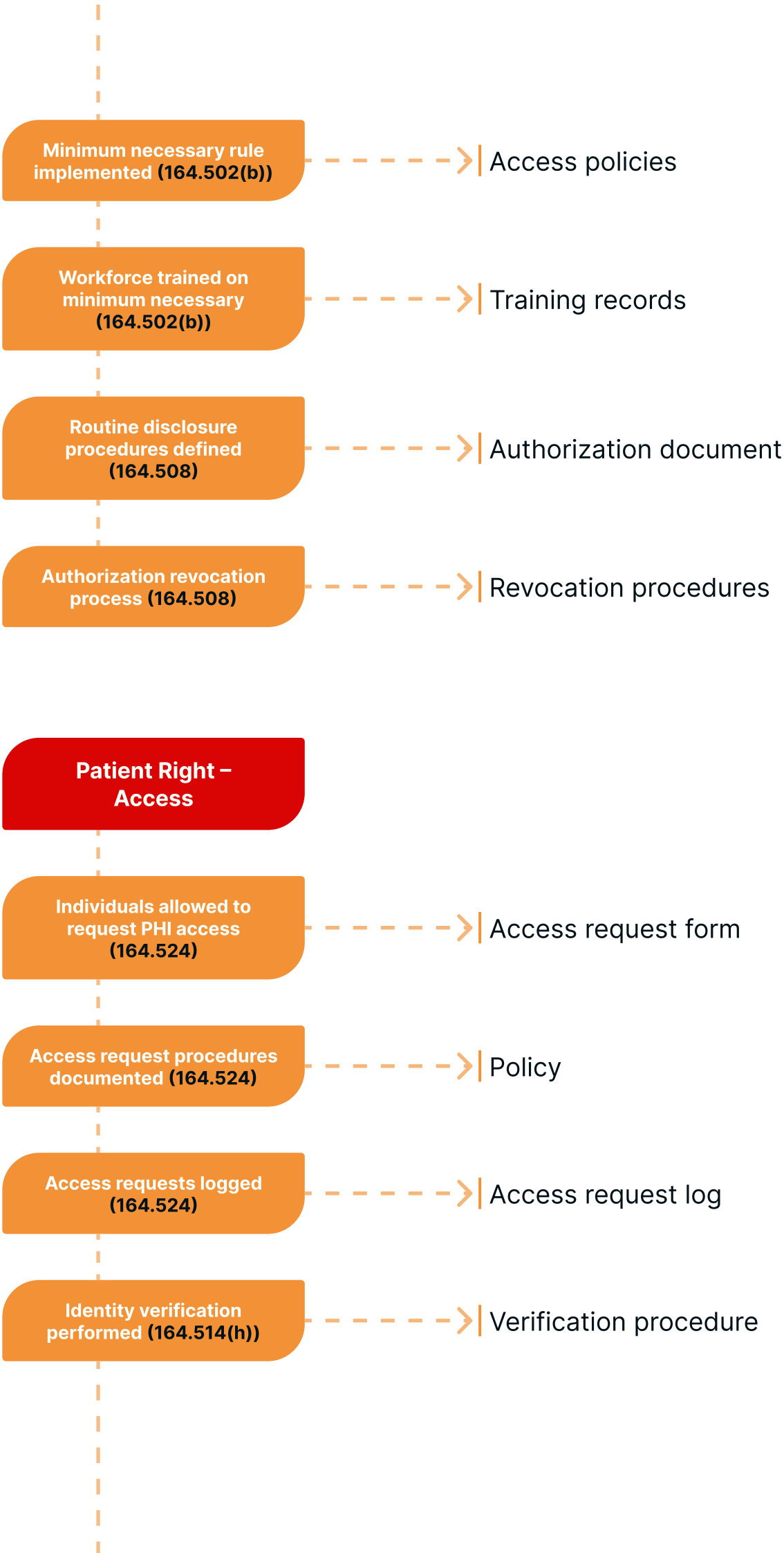
Privacy Rule Controls

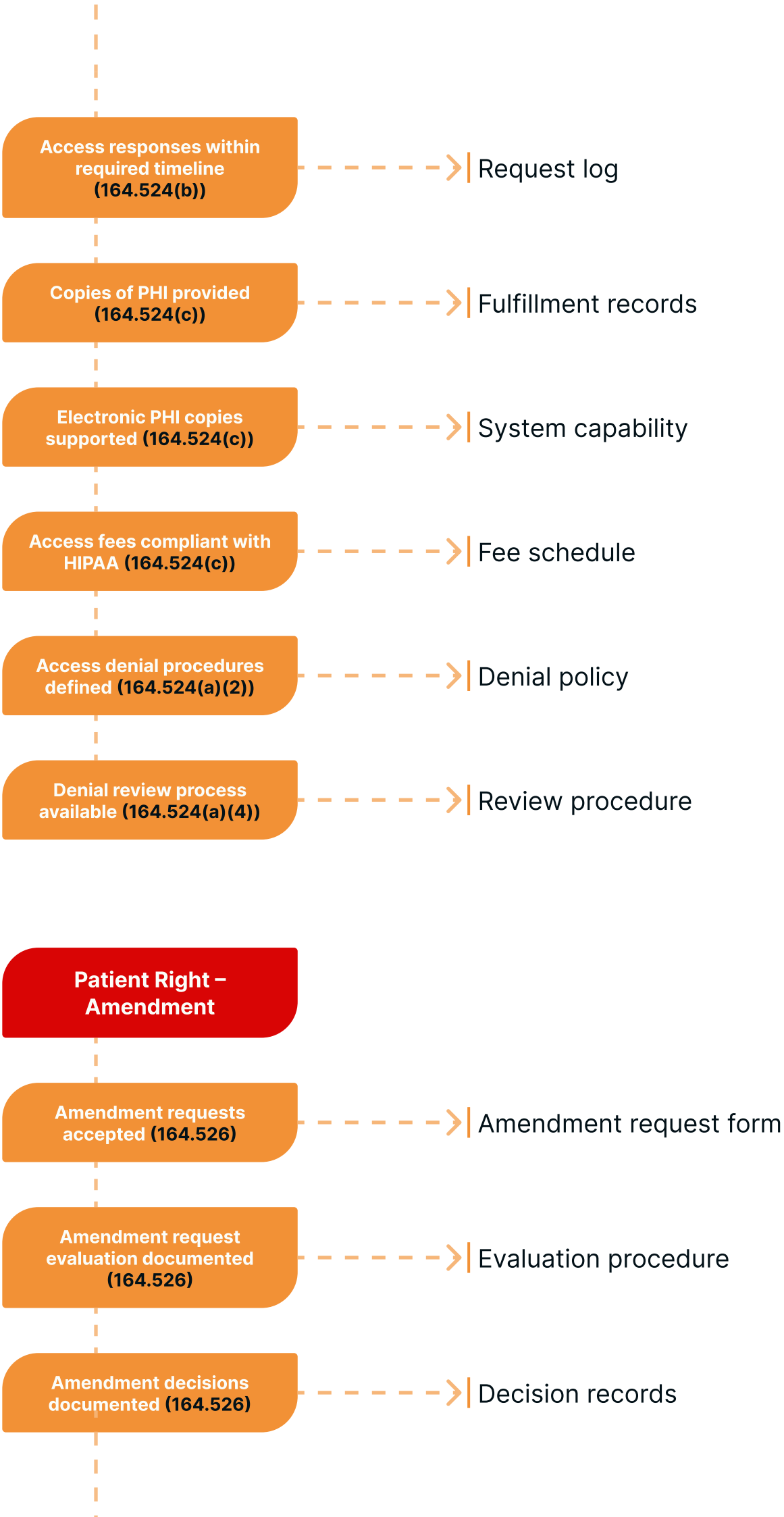
Governance & Policies	Evidence Required
Privacy Officer formally designated (164.530(a)(1))	Appointment letter, org chart
Privacy responsibilities defined (164.530(a)(1))	Job description
Privacy policies documented (164.530(i))	Privacy policy document
Privacy procedures documented (164.530(i))	Procedure documentation
Privacy policies approved by management (164.530(i))	Approval records
Privacy policy review process established (164.530(i))	Policy review schedule
Workforce required to comply with policies (164.530(b))	Employee handbook

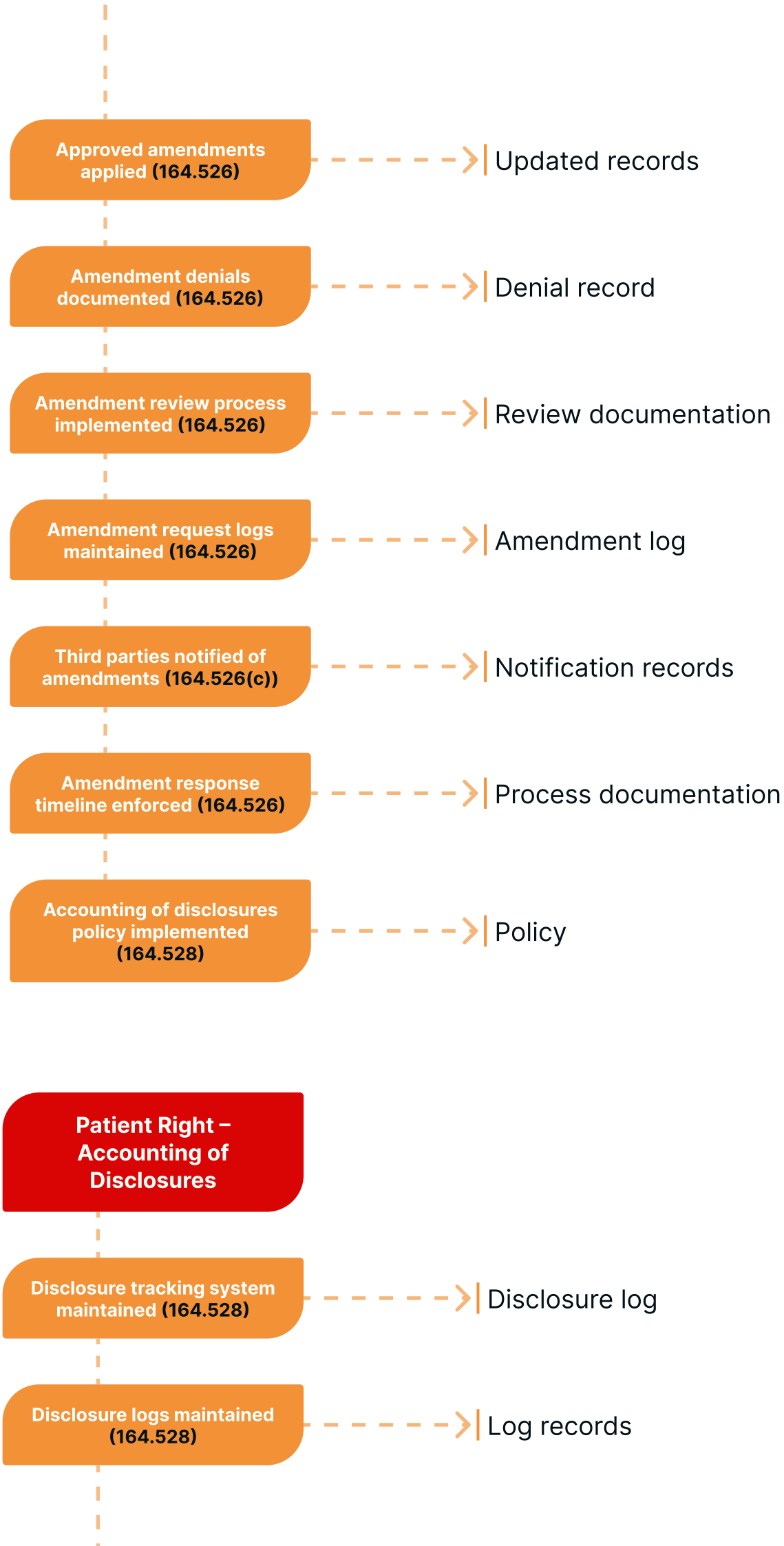

Sanctions policy defined (164.530(e))
Sanctions policy
Sanctions enforced (164.530(e))
Disciplinary records
Sanctions documented (164.530(e))
HR records
Privacy Training
Privacy training program implemented (164.530(b)(1))
Training plan
Workforce initial privacy training conducted (164.530(b)(1))
Training logs
Periodic privacy training conducted (164.530(b)(1))
Refresher training records
Privacy training materials documented (164.530(b))
Training presentations
Workforce training attendance tracked (164.530(b))
Attendance records

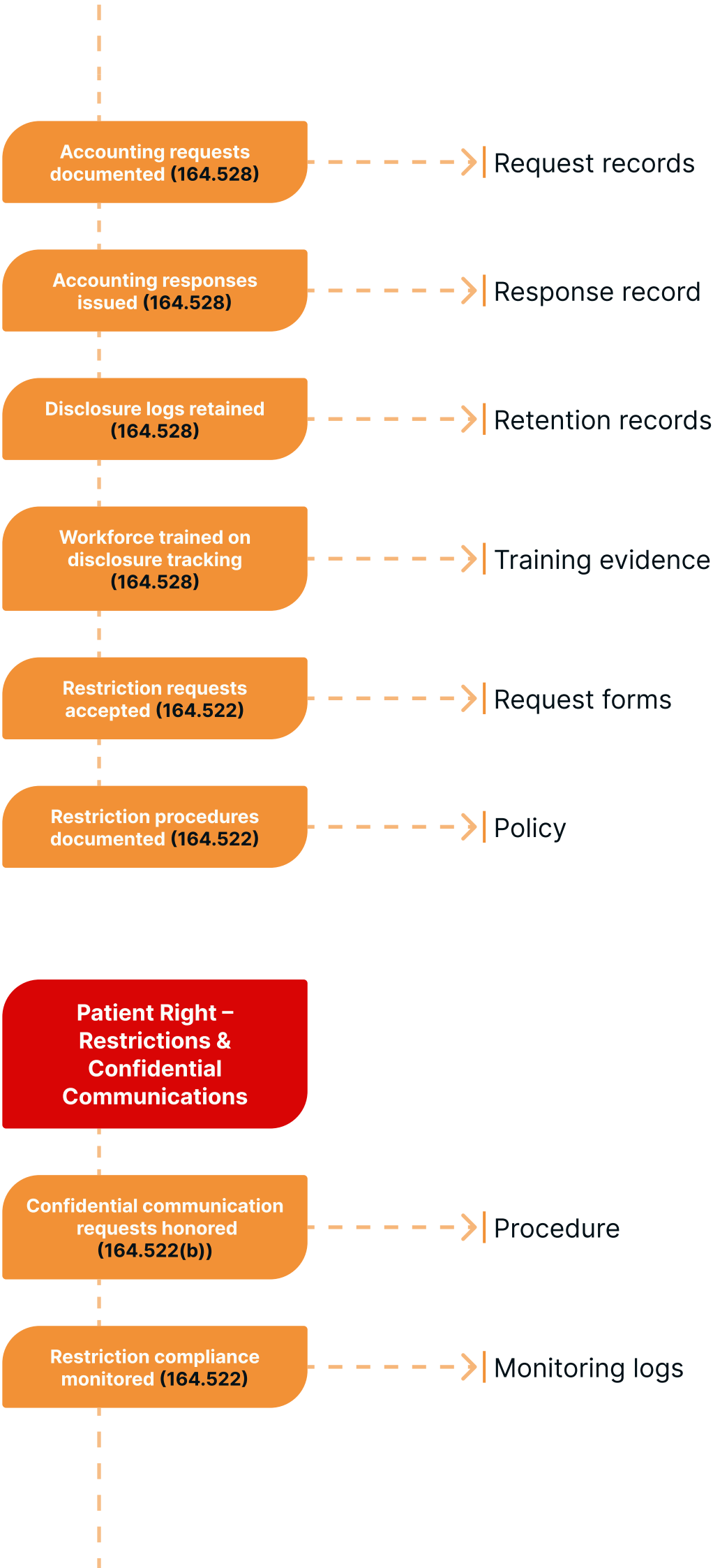

Privacy awareness communications issued (164.530(b))
Awareness emails
Workforce acknowledges policies (164.530(b))
Signed acknowledgements
Privacy training updated for regulatory changes (164.530(b))
Updated training material
Contractors included in privacy training (164.530(b))
Vendor training logs
Training effectiveness evaluated (164.530(b))
Training assessments
Notice of Privacy Practices
Notice of Privacy Practices developed (164.52)
NPP document
NPP describes permitted uses (164.520(b))
NPP review
NPP describes patient rights (164.520(b))
NPP content

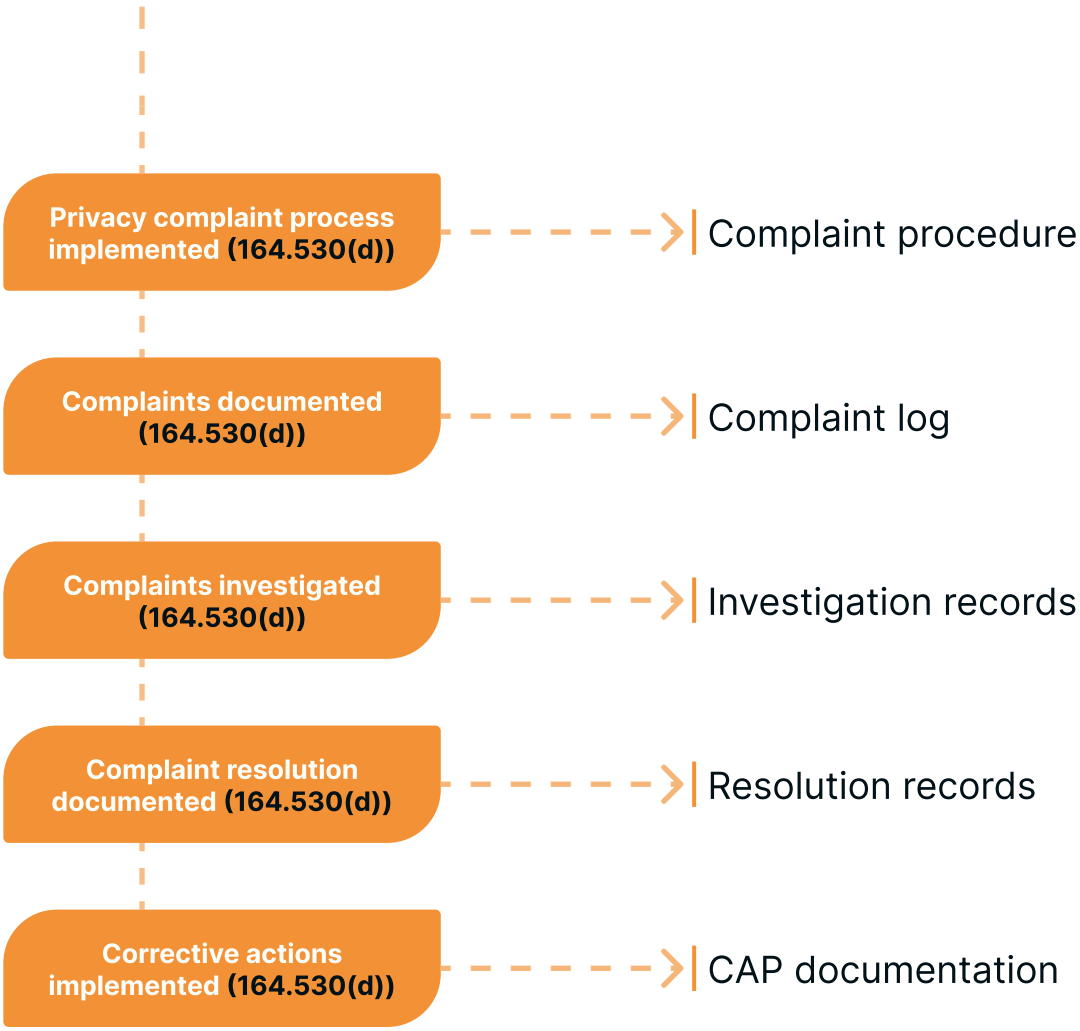

NPP describes complaint process (164.520(b))
NPP section
NPP includes contact information (164.520(b))
NPP document
NPP provided at first encounter (164.520(c))
Distribution records
NPP acknowledgment obtained (164.520(c)(2))
Signed acknowledgment
NPP posted at facility (164.520(c))
Posted notice
NPP posted online if applicable (164.520(c))
Website screenshot
NPP updates communicated (164.520(c))
Updated notice
Uses and Disclosures of PHI
Uses of PHI defined (164.502)
Privacy policy
Disclosures of PHI defined (164.502)
Disclosure procedures


Minimum necessary rule implemented (164.502(b))
Access policies
Workforce trained on minimum necessary (164.502(b))
Training records
Routine disclosure procedures defined (164.508)
Authorization document
Authorization revocation process (164.508)
Revocation procedures
Patient Right – Access
Individuals allowed to request PHI access (164.524)
Access request form
Access request procedures documented (164.524)
Policy
Access requests logged (164.524)
Access request log
Identity verification performed (164.514(h))
Verification procedure


Access responses within required timeline (164.524(b))
Request log
Copies of PHI provided (164.524(c))
Fulfillment records
Electronic PHI copies supported (164.524(c))
System capability
Access fees compliant with HIPAA (164.524(c))
Fee schedule
Access denial procedures defined (164.524(a)(2))
Denial policy
Denial review process available (164.524(a)(4))
Review procedure
Patient Right – Amendment
Amendment requests accepted (164.526)
Amendment request form
Amendment request evaluation documented (164.526)
Evaluation procedure
Amendment decisions documented (164.526)
Decision records


Approved amendments applied (164.526)
Updated records
Amendment denials documented (164.526)
Denial record
Amendment review process implemented (164.526)
Review documentation
Amendment request logs maintained (164.526)
Amendment log
Third parties notified of amendments (164.526(c))
Notification records
Amendment response timeline enforced (164.526)
Process documentation
Accounting of disclosures policy implemented (164.528)
Policy
Patient Right – Accounting of Disclosures
Disclosure tracking system maintained (164.528)
Disclosure log
Disclosure logs maintained (164.528)
Log records


Accounting requests documented (164.528)
Request records
Accounting responses issued (164.528)
Response record
Disclosure logs retained (164.528)
Retention records
Workforce trained on disclosure tracking (164.528)
Training evidence
Restriction requests accepted (164.522)
Request forms
Restriction procedures documented (164.522)
Policy
Patient Right – Restrictions & Confidential Communications
Confidential communication requests honored (164.522(b))
Procedure
Restriction compliance monitored (164.522)
Monitoring logs

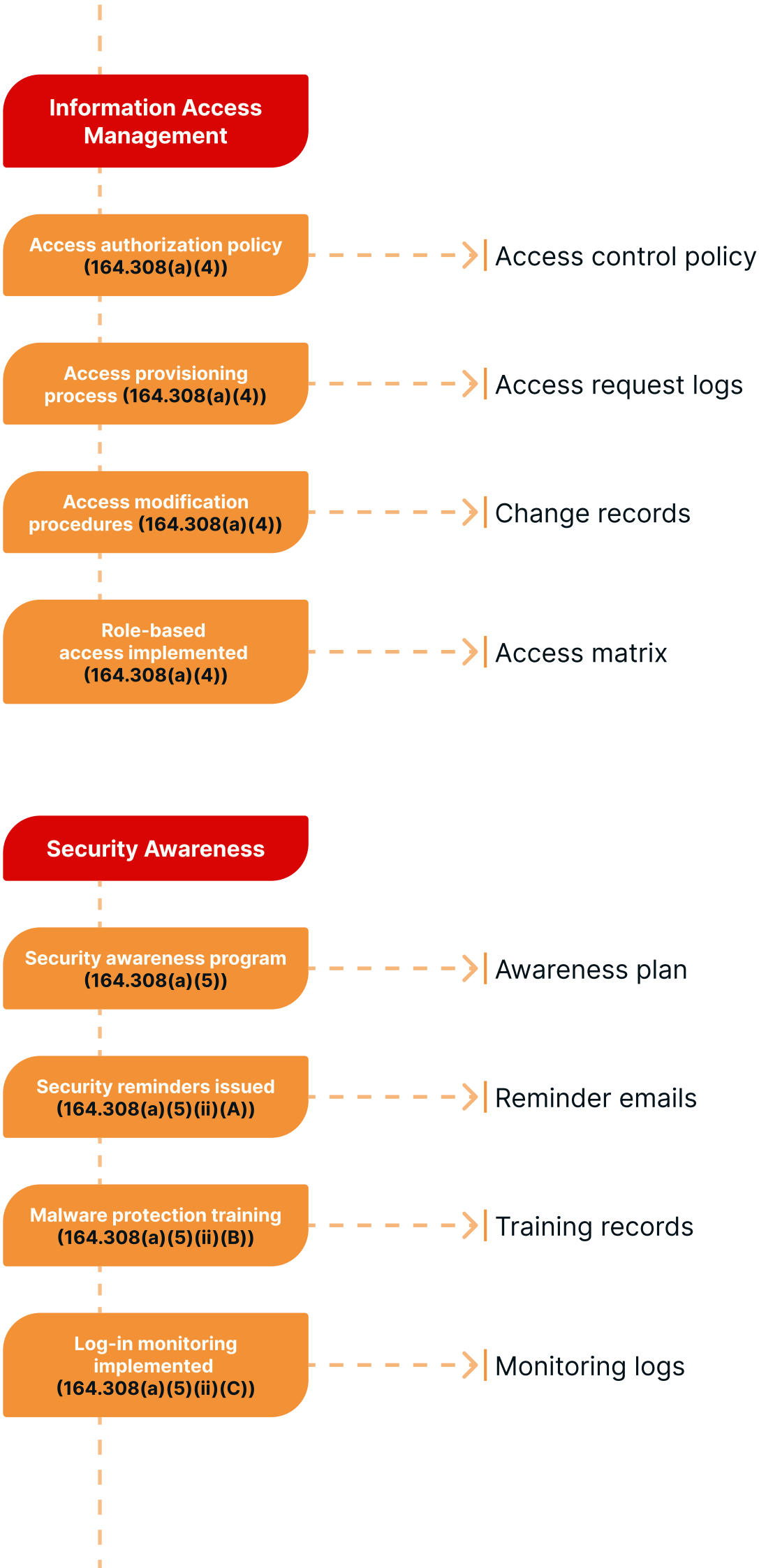

Privacy complaint process implemented (164.530(d))
Complaint procedure
Complaints documented (164.530(d))
Complaint log
Complaints investigated (164.530(d))
Investigation records
Complaint resolution documented (164.530(d))
Resolution records
Corrective actions implemented (164.530(d))
CAP documentation

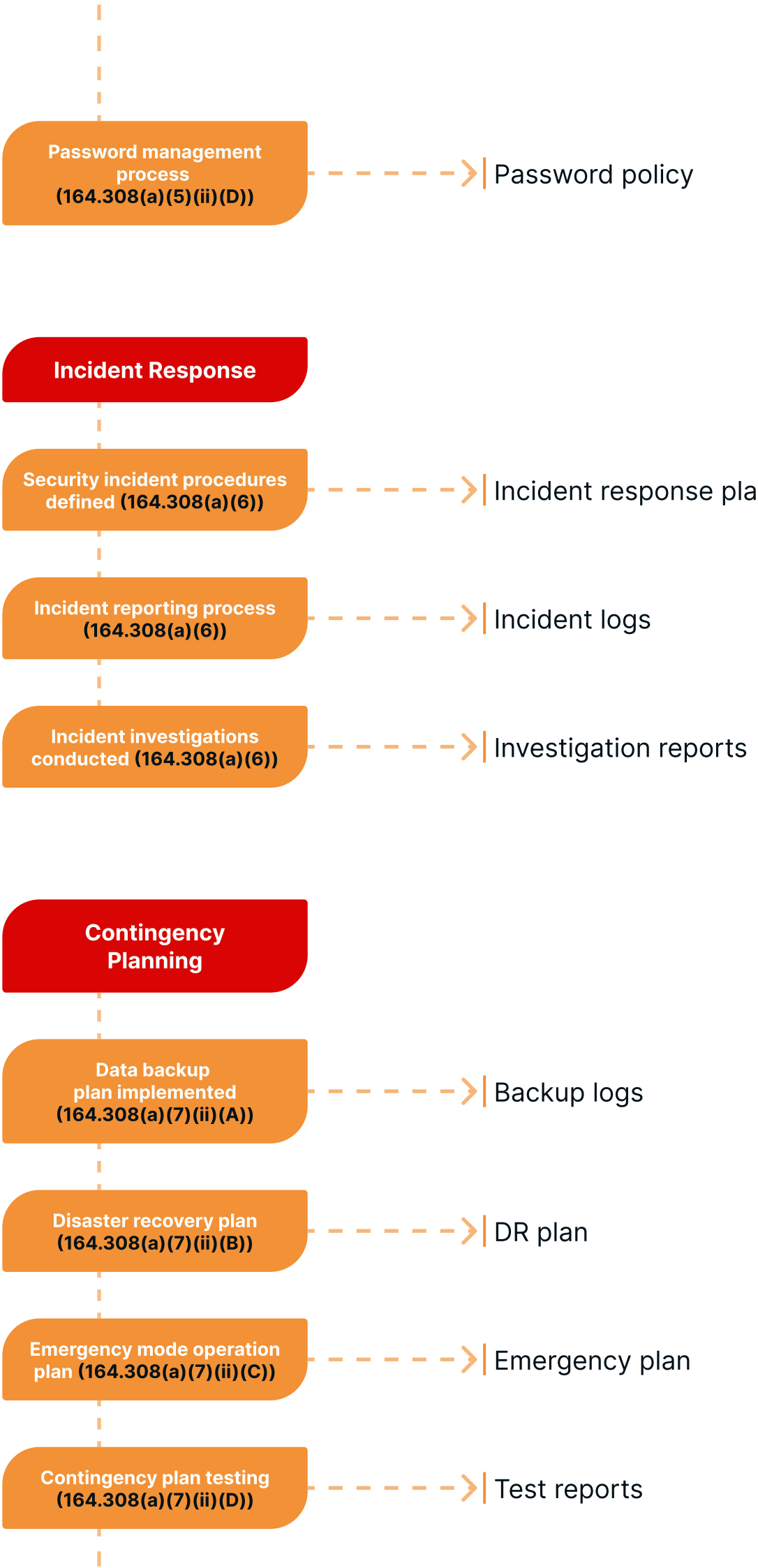
02

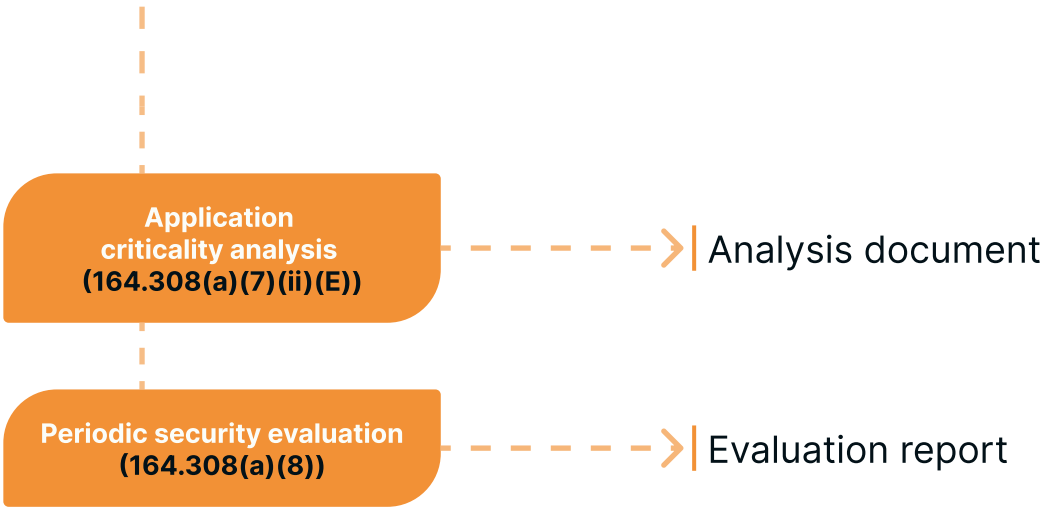
Security Rule Controls

	Evidence Required
Security Governance	
Security Officer designated (164.308(a)(2))	Appointment letter
Security responsibilities documented (164.308(a)(2))	Job description
Security policies documented (164.308)	Security policy
Security procedures documented (164.308)	Procedure documentation
Risk Management and Analysis	
Risk analysis performed (164.308(a)(1)(ii)(A))	Risk assessment report
Systems containing ePHI identified (164.308(a)(1))	Asset inventory


Threat identification conducted (164.308(a)(1))
Risk register
Vulnerabilities documented (164.308(a)(1))
Vulnerability reports
Risk levels calculated (164.308(a)(1))
Risk matrix
Risk mitigation plan developed (164.308(a)(1)(ii)(B))
Risk treatment plan
Sanction policy implemented (164.308(a)(1)(ii)(C))
Sanctions policy
Information system activity review (164.308(a)(1)(ii)(D))
Log review reports
Workforce Security
Workforce clearance procedures (164.308(a)(3)(ii)(B))
HR procedures
Workforce authorization procedures (164.308(a)(3)(ii)(A))
Access approval records
Workforce termination procedures (164.308(a)(3)(ii)(C))
Offboarding checklist

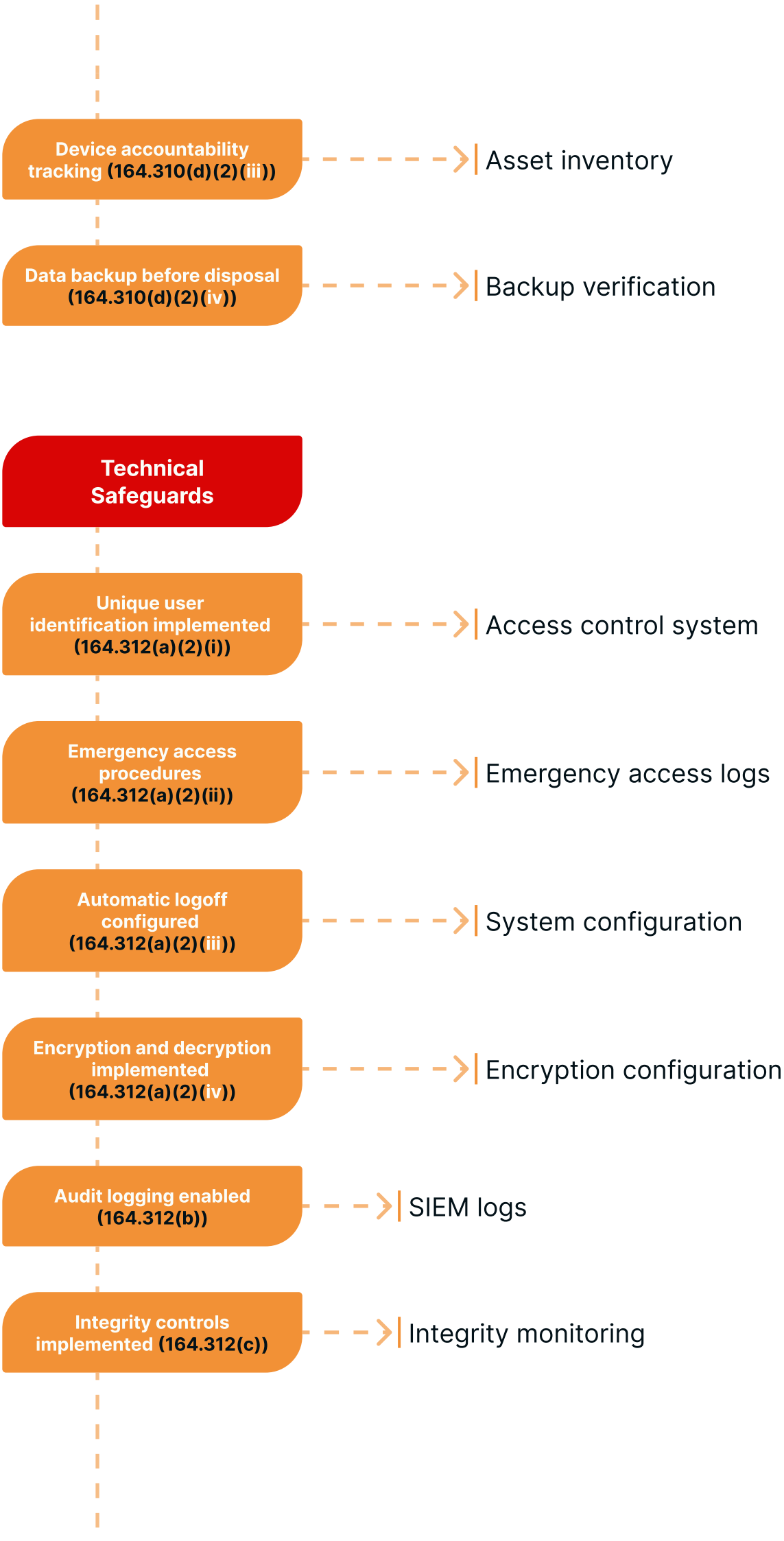

Information Access Management
Access authorization policy (164.308(a)(4))
Access control policy
Access provisioning process (164.308(a)(4))
Access request logs
Access modification procedures (164.308(a)(4))
Change records
Role-based access implemented (164.308(a)(4))
Access matrix
Security Awareness
Security awareness program (164.308(a)(5))
Awareness plan
Security reminders issued (164.308(a)(5)(ii)(A))
Reminder emails
Malware protection training (164.308(a)(5)(ii)(B))
Training records
Log-in monitoring implemented (164.308(a)(5)(ii)(C))
Monitoring logs

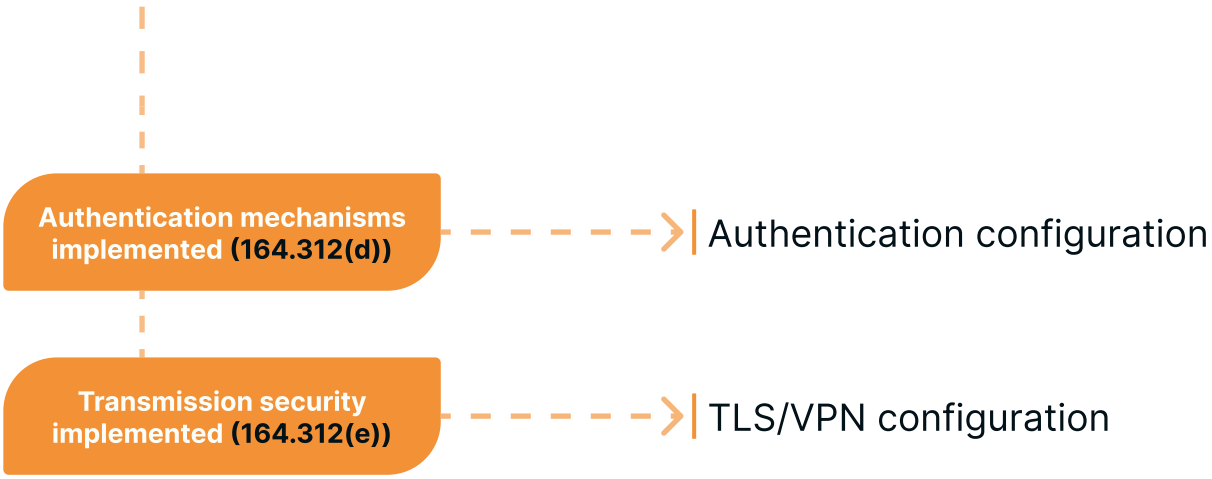

Password management process (164.308(a)(5)(ii)(D))
Password policy
Incident Response
Security incident procedures defined (164.308(a)(6))
Incident response plan
Incident reporting process (164.308(a)(6))
Incident logs
Incident investigations conducted (164.308(a)(6))
Investigation reports
Contingency Planning
Data backup plan implemented (164.308(a)(7)(ii)(A))
Backup logs
Disaster recovery plan (164.308(a)(7)(ii)(B))
DR plan
Emergency mode operation plan (164.308(a)(7)(ii)(C))
Emergency plan
Contingency plan testing (164.308(a)(7)(ii)(D))
Test reports


Application criticality analysis (164.308(a)(7)(ii)(E))
Analysis document
Periodic security evaluation (164.308(a)(8))
Evaluation report

03 Physical & Technical Safeguards

Physical Safeguards	Evidence Required
Facility access controls implemented (164.310(a))	Access logs
Facility security plan (164.310(a)(2))	Security plan
Visitor access validation (164.310(a)(2))	Visitor logs
Maintenance records maintained (164.310(a)(2))	Maintenance logs
Workstation use policy (164.310(b))	Workstation policy
Workstation security controls (164.310(c))	Configuration records
Media disposal procedures (164.310(d)(2)(i))	Disposal logs
Media reuse procedures (164.310(d)(2)(ii))	Reuse documentation

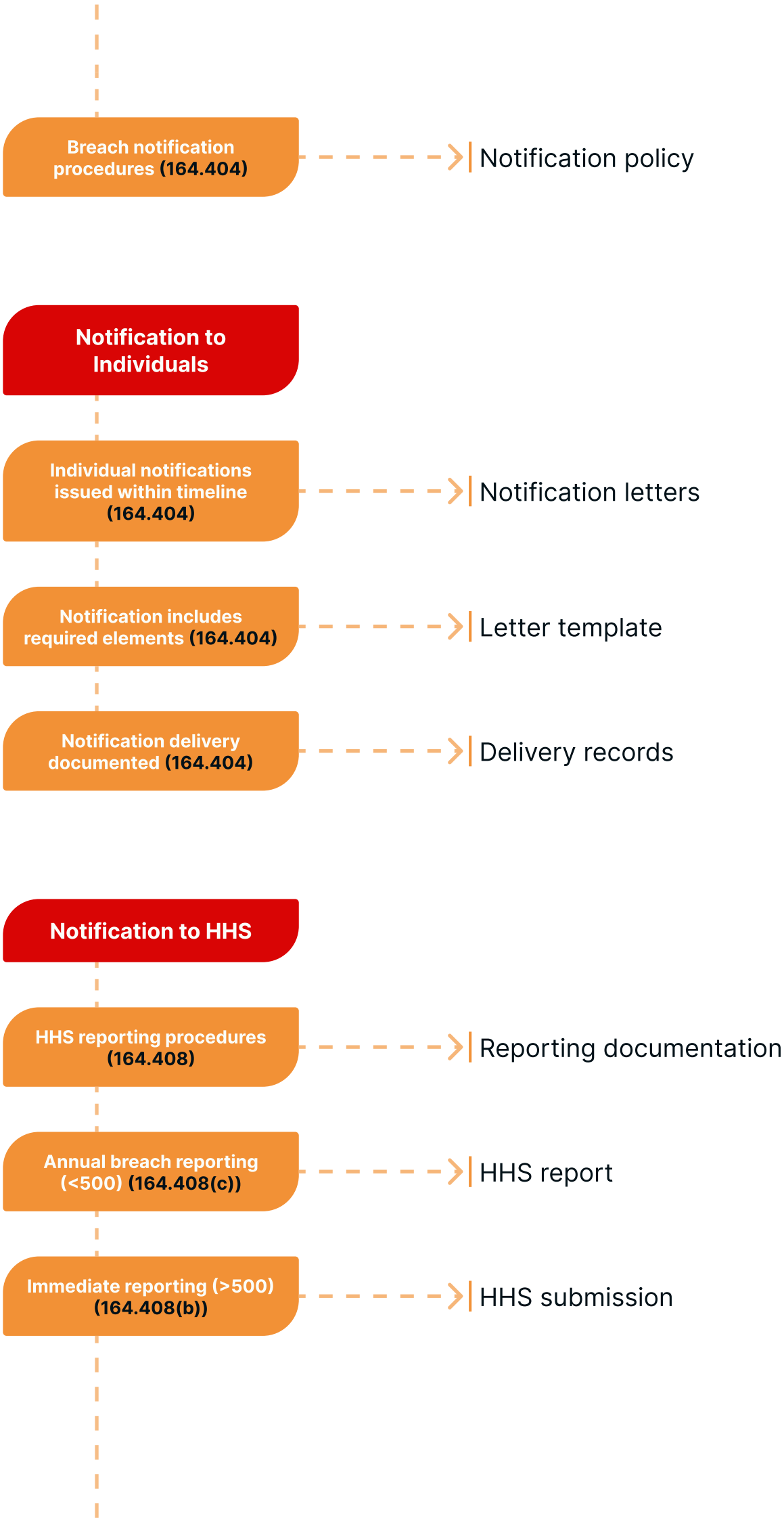

Device accountability tracking (164.310(d)(2)(iii))
Asset inventory
Data backup before disposal (164.310(d)(2)(iv))
Backup verification
Technical Safeguards
Unique user identification implemented (164.312(a)(2)(i))
Access control system
Emergency access procedures (164.312(a)(2)(ii))
Emergency access logs
Automatic logoff configured (164.312(a)(2)(iii))
System configuration
Encryption and decryption implemented (164.312(a)(2)(iv))
Encryption configuration
Audit logging enabled (164.312(b))
SIEM logs
Integrity controls implemented (164.312(c))
Integrity monitoring

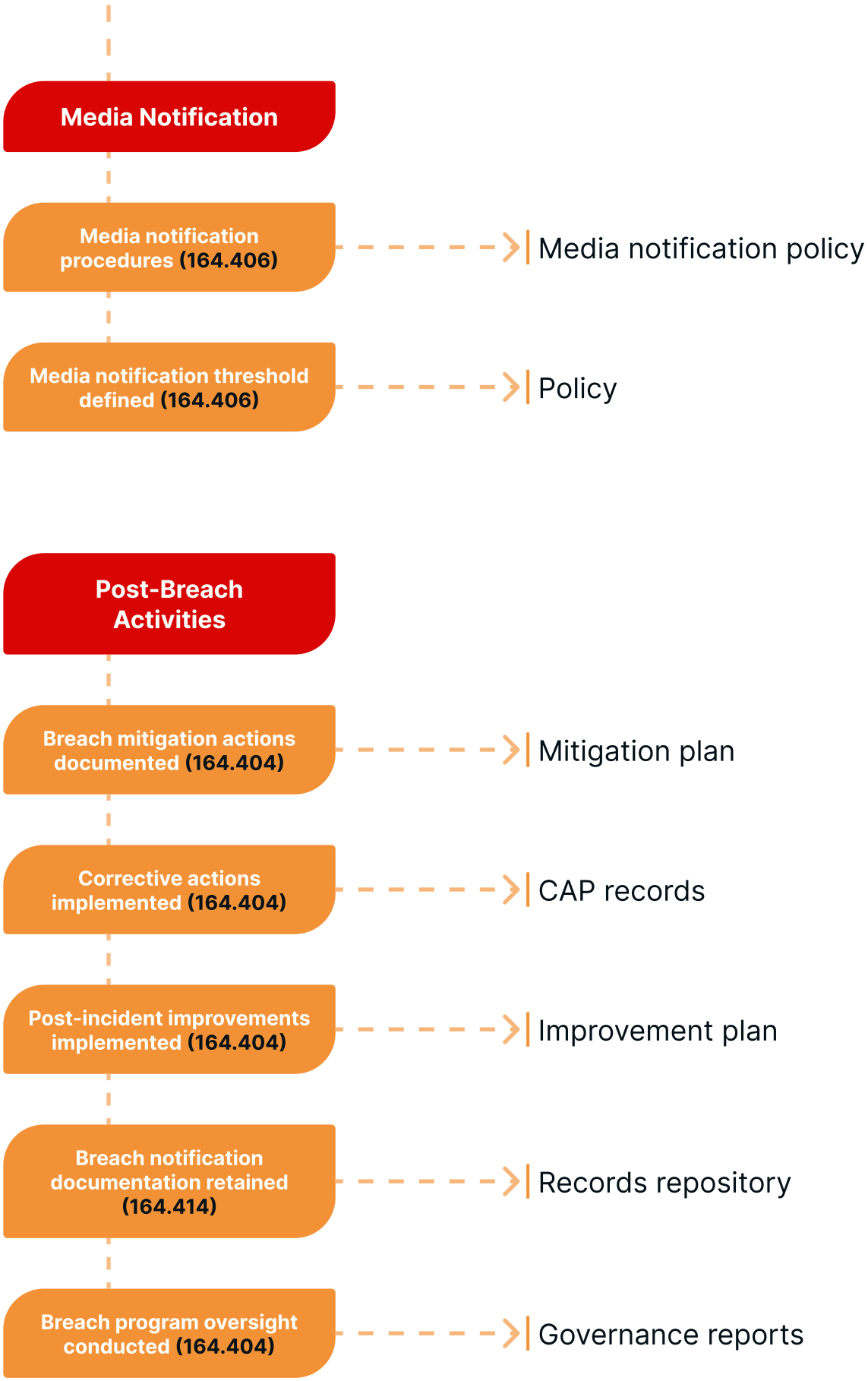

Authentication mechanisms implemented (164.312(d))
Authentication configuration
Transmission security implemented (164.312(e))
TLS/VPN configuration

04

Breach Notification Rule

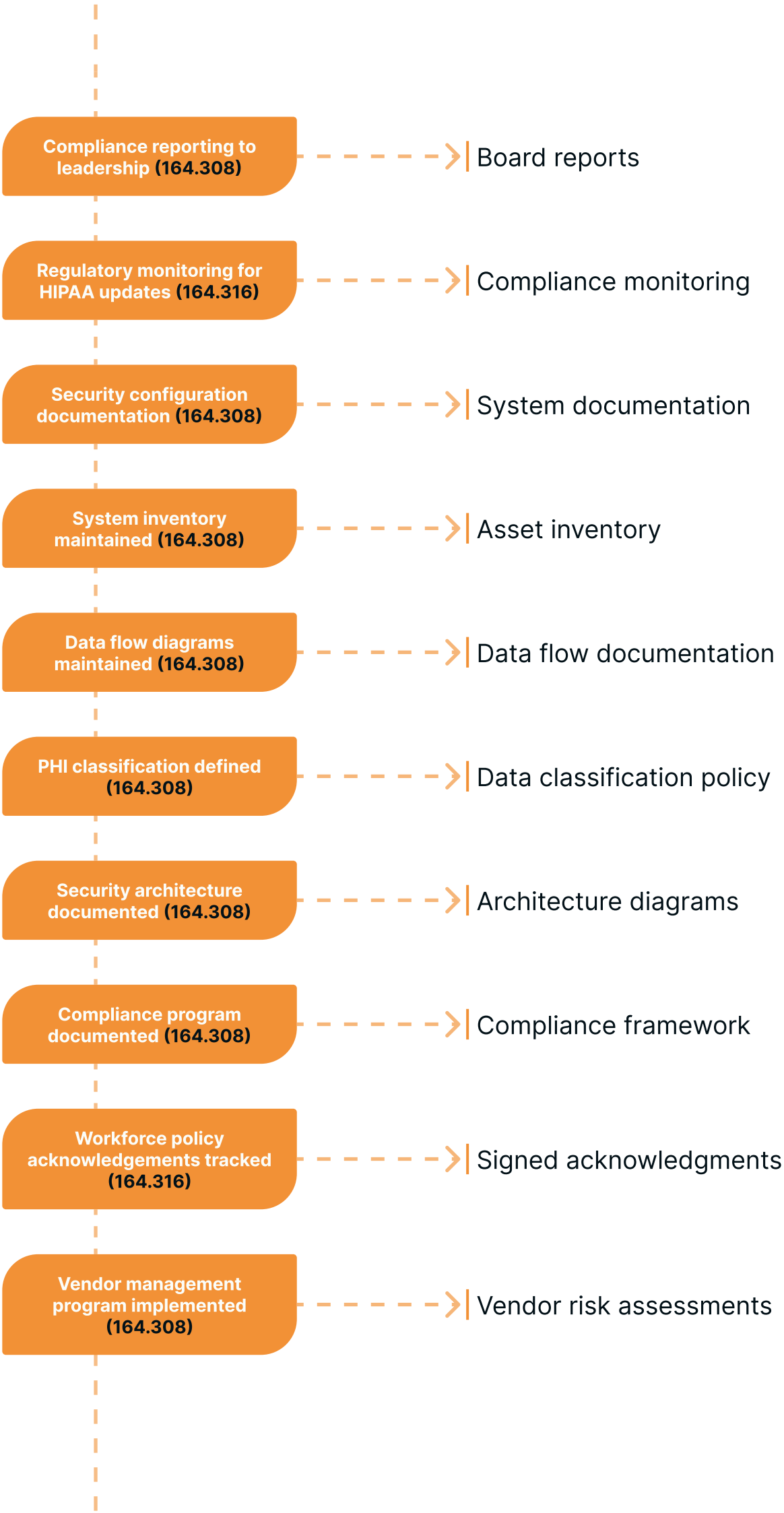
	Evidence Required
Breach Identification	
Breach definition documented (164.402)	Breach policy
Breach detection process implemented (164.402)	Monitoring logs
Workforce trained on breach identification (164.53)	Training records
Breach Risk Assessment and Documentation	
Breach risk assessment methodology (164.402)	Assessment framework
Breach investigation procedures (164.404)	Investigation reports
Breach incidents logged (164.404)	Incident register

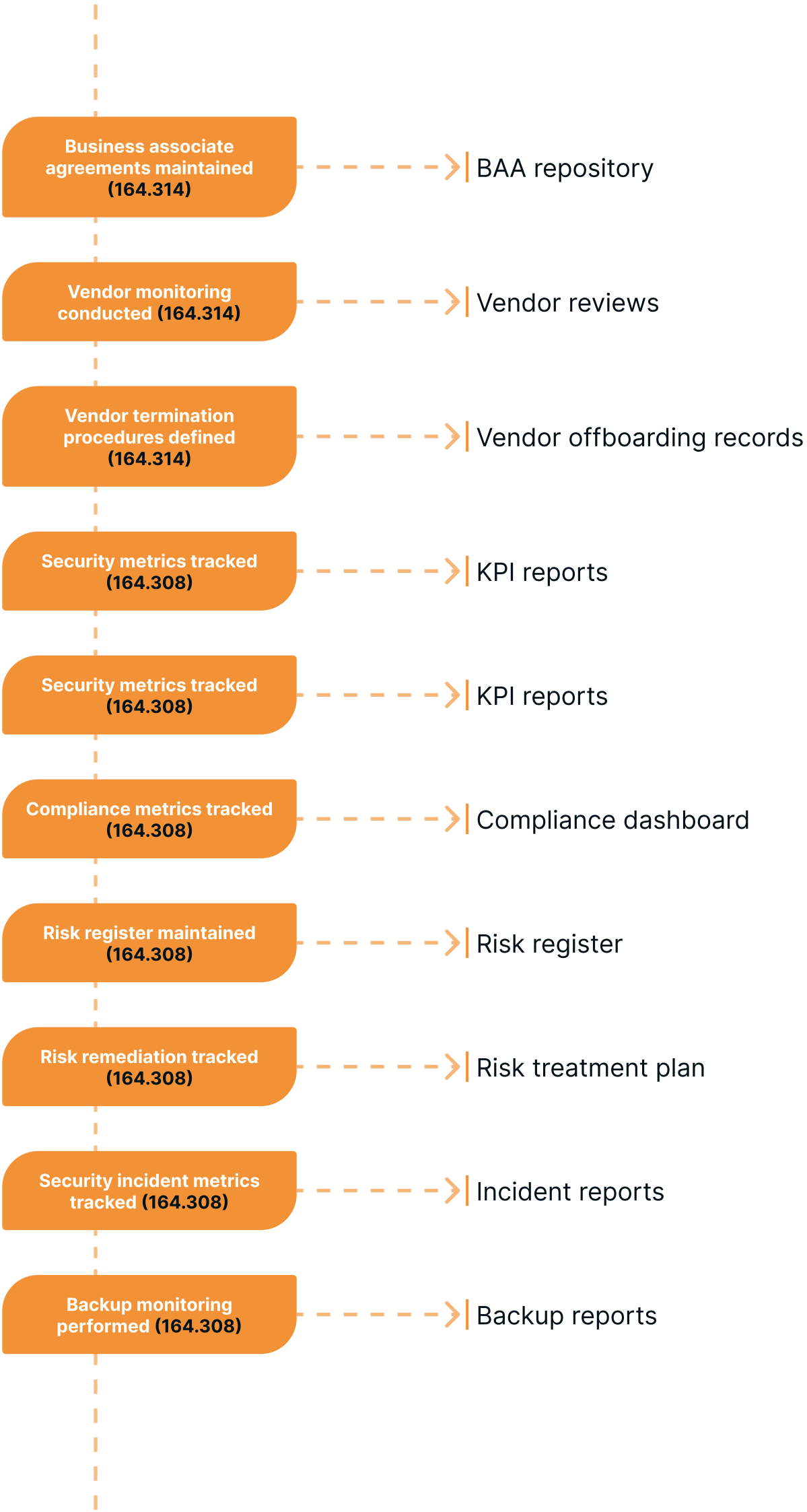

Breach notification procedures (164.404)
Notification policy
Notification to Individuals
Individual notifications issued within timeline (164.404)
Notification letters
Notification includes required elements (164.404)
Letter template
Notification delivery documented (164.404)
Delivery records
Notification to HHS
HHS reporting procedures (164.408)
Reporting documentation
Annual breach reporting (<500) (164.408(c))
HHS report
Immediate reporting (>500) (164.408(b))
HHS submission


Media Notification
Media notification procedures (164.406)
Media notification policy
Media notification threshold defined (164.406)
Policy
Post-Breach Activities
Breach mitigation actions documented (164.404)
Mitigation plan
Corrective actions implemented (164.404)
CAP records
Post-incident improvements implemented (164.404)
Improvement plan
Breach notification documentation retained (164.414)
Records repository
Breach program oversight conducted (164.404)
Governance reports

05 Documentation & Governance Controls

Governance and Documentation Maintenance and Monitoring	Evidence Required
HIPAA documentation retention policy (164.316)	Retention policy
Documentation retained ≥6 years (164.316(b))	Archive records
Policies accessible to workforce (164.316)	Policy portal
Policy updates communicated (164.316)	Communication records
Compliance monitoring program (164.308)	Monitoring reports
Internal HIPAA audits conducted (164.308)	Audit reports
Corrective action process defined (164.308)	CAP procedures


Compliance reporting to leadership (164.308)
Board reports
Regulatory monitoring for HIPAA updates (164.316)
Compliance monitoring
Security configuration documentation (164.308)
System documentation
System inventory maintained (164.308)
Asset inventory
Data flow diagrams maintained (164.308)
Data flow documentation
PHI classification defined (164.308)
Data classification policy
Security architecture documented (164.308)
Architecture diagrams
Compliance program documented (164.308)
Compliance framework
Workforce policy acknowledgements tracked (164.316)
Signed acknowledgments
Vendor management program implemented (164.308)
Vendor risk assessments


Business associate agreements maintained (164.314)
BAA repository
Vendor monitoring conducted (164.314)
Vendor reviews
Vendor termination procedures defined (164.314)
Vendor offboarding records
Security metrics tracked (164.308)
KPI reports
Security metrics tracked (164.308)
KPI reports
Compliance metrics tracked (164.308)
Compliance dashboard
Risk register maintained (164.308)
Risk register
Risk remediation tracked (164.308)
Risk treatment plan
Security incident metrics tracked (164.308)
Incident reports
Backup monitoring performed (164.308)
Backup reports

Disaster recovery tests documented (164.308)	DR test reports
Security awareness effectiveness measured (164.308)	Survey results
Data retention policies enforced (164.316)	Retention logs
System access logs retained (164.312)	Log archive
Encryption policies documented (164.312)	Encryption policy
Transmission security monitored (164.312)	Network monitoring logs
Authentication controls monitored (164.312)	Authentication logs
Security tool monitoring implemented (164.308)	SIEM reports
Compliance program review conducted annually (164.308)	Annual review report
Leadership oversight of HIPAA compliance (164.308)	Governance minutes
Continuous improvement of HIPAA program (164.308)	Improvement roadmap

KLEAP

CYBERSECURITY

https://kleapcybersecurity.com/

info@kleapcybersecurity.com

4111, Briargrove Circle, Raleigh,
North Carolina, 27607, USA