COUNCIL ON CYBERSECURITY
LE CONSEIL DE LA CYBERSÉCURITÉ

Top 20 Security Controls (Updated)

Crosswalk to the 42 HIPAA Security Controls

Council Control #	Council on CyberSecurity Control	HIPAA Citation	HIPAA Control
1	Inventory of Authorized and Unauthorized Devices		None, although some OCR enforcement actions suggest they might expect an inventory as part of the Risk Analysis, 164.308(a)(1)(ii)(A).
2	Inventory of Authorized and Unauthorized Software		None
3	Secure Configurations for Hardware, Software on Laptops, Workstations, Servers		None
4	Continuous Vulnerability Assessment and Remediation	164.308(a)(8)	Evaluation. (Periodic Technical and nontechnical evaluation . . .)
5	Malware Defense	164.308(a)(5)(ii)(B)	Protection from Malicious Software
6	Wireless Access Control		None
7	Application Software Security		None
8	Data Recovery Capability	164.308(a)(7)(i)	Contingency Plan, including Data Backup Plan and Disaster Recovery Plan
9	Security Skills Assessment, Appropriate Training to Fill Gaps	164.308(a)(5)(ii)(A)	Security Reminders
10	Secure Configuration of Devices such as Firewalls, Routers, and Switches		None
11	Limitation and Control of Network Ports, Protocols and Services		None
12	Controlled Use of Administrative Privileges		None
13	Boundary Defense		None, although one OCR enforcement action cited the lack of a properly configured firewall and no monitoring of its log as specified with 164.308(a)(1)(ii)(D) “Information system Activity Review”
14	Maintenance, Monitoring and Analysis of Audit Logs	164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(C) 164.312(b)	Information System Activity Review Log-in Monitoring Audit Controls
15	Controlled Access Based on Need to Know	164.502(b)	Minimum Necessary
16	Account Monitoring and Control	164.308(a)(4)(ii)(B) 164.308(a)(4)(ii)(C)	Access Authorization Access Establishment and Modification
17	Data Protection	164.310(d)	Device and Media Controls – Disposal, Media-Re-Use
18	Incident Response Capability---	164.308(a)(6)	Security Incident Procedures
19	Secure Network Engineering		None
20	Penetration Tests and Red Team Exercises	164.308(a)(8)	Evaluation. (Periodic Technical and nontechnical evaluation . . .)None

Crosswalk created by Eagle Consulting Partners, Inc.
NOTE: Controls are not equivalent!

Published on 3-05-2014 | www.EagleConsultingPartners.com