

Table 1**Percentage Reporting Each Level of Security Compliance**

Security standard	Frequency of response* (as a percentage of all responses)				
	1	2	3	4	5
Policies/procedures for obtaining required business associate agreements	4	7	11	22	55
A security manager responsible for implementing and maintaining the requirements of the Security Rule	6	5	14	27	48
Policies/procedures for physical safeguards to limit access to electronic information systems with facility access controls, workstation use and security, and device and media controls	3	6	14	44	32
Policies/procedures for technical safeguards to provide access control, audit controls, integrity, person or entity authentication, and transmission security	4	9	17	47	22
Policies/procedures for information access management (authorizing access to electronic protected health information [EPHI] consistent with requirements)	2	10	24	38	23
Policies/procedures for work force security (ensuring all members have appropriate access to EPHI and preventing access to EPHI to those who should not have it)	4	8	24	38	25
Policies/procedures for addressing security incidents (a response and reporting plan)	5	13	25	29	28
A contingency plan for responding to an emergency or other occurrence of damage (such as a data backup plan, a disaster recovery plan, and an emergency mode operation plan)	6	11	26	36	21
A security management process including risk analysis, risk management, sanction policies, and review of IS activities	6	12	28	36	18
Program for security awareness and training for hospital personnel (including protection from malicious software and monitoring log-in attempts and password management)	9	15	23	30	23
Policies/procedures for performing a periodic technical and non-technical evaluation of security practices governed by security rule	10	13	28	29	19

* 1 being least compliant, 5 being most compliant