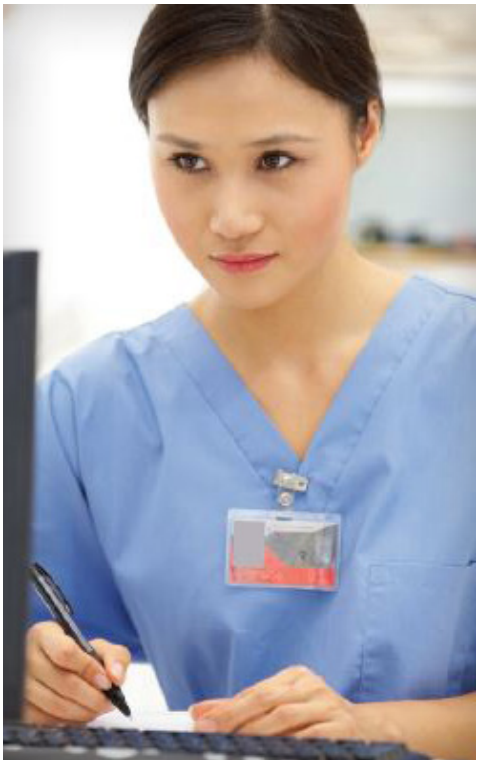
Simplifying HIPAA Compliance

ISO 27001

DQS MANAGEMENT SYSTEMS SOLUTIONS | 1500 MCCONNOR PARKWAY SUITE 400 | SCHAUMBURG, IL 60173 | 800-285-4476 | WWW.DQSUS.COM



Since the mid-1990s, HIPAA (Health Insurance Portability and Accountability Act) has been more than just a buzzword in and around organizations who routinely deal with health information.

Part of this unique legislation is the HIPAA Privacy Rule, which provides federal protections for personal health information. Requirements for HIPAA are defined in the Code of Federal Regulations (CFR) Title 45, Part 164.

They are divided into six categories:

1. *Security standard*
2. *Administrative safeguard*
3. *Physical safeguard*
4. *Technical safeguard*
5. *Organizational requirements*
6. *Policies, procedures, and documentation requirements*

ISO 27001 and HIPAA

ISO 27001 specifies a management system that is intended to organize and control information security, which is at the core of the HIPAA legislation. In fact, ISO 27001 addresses approximately 95% of the requirements of HIPAA. The framework of this standard provides flexibility to organizations to select the controls that are apply to their business.

They can also add new controls to the management system that are not defined in ISO 27001 to address the remaining 5% of HIPAA requirements focusing on the administrative safeguard. ISO 27001 provides a list of 114 controls and the guidelines on the implementation of the controls. As a result, it is much easier to implement ISO 27001 for organized and certifiable evidence of HIPAA compliance. Finally, there is no certification scheme available for HIPAA. Claims of compliance are based on self-assessment or assessments done by consultants. Credibility of these claims are often challenged, whereas ISO 27001 certificates are accredited by the American National Accreditation Board (ANAB).

An organization with an ISO 27001 certificate will have more credible evidence of HIPAA compliance.

The CFR 45 Part 164 only provides very brief descriptions of the requirements. Organizations are responsible for interpreting the requirements and identifying appropriate controls to satisfy the requirements. This has been a major challenge for organizations. The implementation of a management system according to ISO 27001 can help define and simplify processes in these compliance efforts.

ISO 27001 – Guideline for implementation of the controls