7.4.1 Guiding Principles

The implementation of the data security management function into an organization follows fifteen guiding principles:

1. Be a responsible trustee of data about all parties. They own the data. Understand and respect the privacy and confidentiality needs of all stakeholders, be they clients, patients, students, citizens, suppliers, or business partners.
2. Understand and comply with all pertinent regulations and guidelines.
3. Data-to-process and data-to-role relationship (CRUD–Create, Read, Update, Delete) matrices help map data access needs and guide definition of data security role groups, parameters, and permissions.
4. Definition of data security requirements and data security policy is a collaborative effort involving IT security administrators, data stewards, internal and external audit teams, and the legal department. The data governance council should review and approve high-level data security policy.
5. Identify detailed application security requirements in the analysis phase of every systems development project.
6. Classify all enterprise data and information products against a simple confidentiality classification schema.
7. Every user account should have a password set by the user following a set of password complexity guidelines, and expiring every 45 to 60 days.
8. Create role groups; define privileges by role; and grant privileges to users by assigning them to the appropriate role group. Whenever possible, assign each user to only one role group.
9. Some level of management must formally request, track, and approve all initial authorizations and subsequent changes to user and group authorizations.
10. To avoid data integrity issues with security access information, centrally manage user identity data and group membership data.
11. Use relational database views to restrict access to sensitive columns and / or specific rows.
12. Strictly limit and carefully consider every use of shared or service user accounts.
13. Monitor data access to certain information actively, and take periodic snapshots of data access activity to understand trends and compare against standards criteria.

14. Periodically conduct objective, independent, data security audits to verify regulatory compliance and standards conformance, and to analyze the effectiveness and maturity of data security policy and practice.

15. In an outsourced environment, be sure to clearly define the roles and responsibilities for data security, and understand the "chain of custody" for data across organizations and roles.

7.4.2 Process Summary

The process summary for the data security management function is shown in Table 7.1. The deliverables, responsible roles, approving roles, and contributing roles are shown for each activity in the data security management function. The Table is also shown in Appendix A9.

Activities	Deliverables	Responsible Roles	Approving Roles	Contributing Roles
5.1 Understand Data Security Needs and Regulatory Requirements (P)	Data Security Requirements and Regulations	Data Stewards, DM Executive, Security Administrators	Data Governance Council	Data Stewards, Legal Department, IT Security
5.2 Define Data Security Policy (P)	Data Security Policy	Data Stewards, DM Executive, Security Administrators	Data Governance Council	Data Stewards, Legal Department, IT Security
5.3 Define Data Security Standards (P)	Data Security Standards	Data Stewards, DM Executive, Security Administrators	Data Governance Council	Data Stewards, Legal Department, IT Security
5.4 Define Data Security Controls and Procedures (D)	Data Security Controls and Procedures	Security Administrators	DM Executive	Data Stewards, IT Security
5.5 Manage Users, Passwords and Group Membership (C)	User Accounts, Passwords, Role Groups	Security Administrators, DBAs	Management	Data Producers, Data Consumers, Help Desk
5.6 Manage Data Access Views and Permissions (C)	Data Access Views Data Resource Permissions	Security Administrators, DBAs	Management	Data Producers, Data Consumers, Software Developers, Management, Help Desk