The Sedona Conference Commentary On Privacy and Information Security: Principles and Guidelines for Lawyers, Law Firms, and other Legal Service Providers (November 2015)

Advances in technology, communications, data storage, and transmission have produced immeasurable societal benefits. However, they have also created unforeseen risks to individual privacy and the security of information that lawyers gather and hold while representing their clients, whether in litigation, in business transactions, or through personal counseling. Personal identities, privacy, confidential client information, work product, and even attorney-client communications have never been more vulnerable to unauthorized disclosures, breaches, loss, or theft than they are today. Yet, the responsibility of all legal service providers to protect such information has not changed. The applicable standards of conduct do not depend on the size or resources of the professional who holds such information. This Commentary from The Sedona Conference Working Group on Electronic Document Retention and Production (WG1) is intended to help all legal service providers—solo practitioners, large law firms, and legal support entities—determine which policies and practices are best suited for each unique situation.

The principles that inform this Commentary are:

Principle 1: Legal service providers should develop and maintain appropriate knowledge of applicable legal authority including statutes, regulations, rules, and contractual obligations in order to identify, protect, and secure private and confidential information.

Principle 2: Legal service providers should periodically conduct a risk assessment of information within their possession, custody, or control that considers its sensitivity, vulnerability, and the harm that would result from its loss or disclosure.

Principle 3: After completing a risk assessment, legal service providers should develop and implement reasonable and appropriate policies and practices to mitigate the risks identified in the risk assessment.

Principle 4: Legal service providers' policies and practices should address privacy and security in reasonably foreseeable circumstances, and reasonably anticipate the possibility of an unauthorized disclosure, breach, loss, or theft of private or confidential information.

Principle 5: Legal service providers' privacy and information security policies and practices should apply to, and include, regular training for their officers, managers, employees, and relevant contractors.

Principle 6: Legal service providers should monitor their practices for compliance with privacy and security policies.

Principle 7: Legal service providers should periodically reassess risks and update their privacy and information security policies and practices to address changing circumstances.

The full text of this commentary is available free for individual download from The Sedona Conference website at
https://thesedonaconference.org/publication/Commentary_on_Privacy_and_Information_Security.