Model Code of Conduct

November 2011

Copyright Notice

.

* See: http://creativecommons.org/licenses/by/3.0/us/ *(last visited 11/8/11)*

TABLE OF CONTENTS

Introduction

This Model Code of Conduct (MCoC) sets forth aspirational guidelines intended to serve as a basis for ethical decision making by all participants in the electronic discovery process. The MCoC was drafted by members of the EDRM MCoC Project and reflects years of exhaustive dialogue and a wide array of viewpoints representative of the interests of corporations, law firms and service providers across the country. Adherence to the MCoC is voluntary.

The MCoC consists of five Principles and their Corollaries, which contain statements of the duties of Service Providers[1] and the related duties of their Clients. Each Principle and Corollary set is accompanied by Guidelines and a Discussion section, providing our view of ethical considerations that should be addressed by participants in the electronic discovery process.

The MCoC is not intended to address or resolve business or legal quandaries, or dictate operational guidelines for participants in the electronic discovery industry or the clients that purchase their products or engage their services. Additionally, it is not intended to replace or substitute for the establishment or construction of contractual relationships between Clients and Service Providers. While we recognize that such matters impact the day-to-day operations of Service Providers, and their relationships with their clients, they are simply outside the scope of this document. The MCoC is not intended to create a legal liability standard, and the MCoC Project claims no enforcement authority.

Many have referred to the electronic discovery industry as the "Wild West", where rules and ethical boundaries for interactions between Clients and Service Providers or Service Providers and other Service Providers are constantly changing to reflect shifting whims. While some would argue that the market will operate to address these issues, time has shown that for a market to mature, ethical boundaries must be clearly delineated and industry participants must agree to be bound by them. We believe that establishing these guidelines for ethical decision-making will provide predictability in business relationships and will lead to a more stable market.

Our hope is that participants in this market will utilize the MCoC in ways that will promote its positive use and wide-spread adoption in the establishment and maintenance of contractual relationships. Service Providers may wish to promote their voluntary adherence to the MCoC. Clients may wish to reference the MCoC in their vendor selection process, including addressing the MCoC in Requests for Information (RFIs) or Requests for Proposals (RFPs). Clients and Service Providers may elect to expressly incorporate the MCoC into their written agreements.

[1] The term "Service Provider" as used in the MCoC is intended to encompass all individuals and organizations – including consultants, vendors, service bureaus, software developers and law firms – that are providing services and/or goods in connection with or relation to the broad range of activities covered by the EDRM.

We recognize that the MCoC does not provide an exhaustive exploration of every potential ethical issue that may arise in the electronic discovery industry. As noted above, the MCoC is aspirational in nature, and voluntary in application. In recognition that the Principles and Corollaries are broad statements, and are further defined in the Guidelines and accompanied by the Discussion reflecting our thinking in their establishment, we expect this document will be construed by our constituents to reflect the evolving marketplace for electronic discovery products and services.

/s/ Kevin Esposito
Co-Chair

/s/ Eric P. Mandel
Co-Chair and Reporter

/s/ Nancy Wallrich
Co-Chair

November 2011

Principle 1 - Professionalism

Principle

Service Providers should perform their work in a competent, accurate, timely and cost-effective manner, adhering to the highest standards of professionalism and ethical conduct.

Corollary

Clients should be forthright, accurate and timely in their dealings with Service Providers and act at all times in accordance with the highest professional standards of ethical conduct.

Guidelines

1. **Competence:** A Service Provider shall provide competent performance of services to a Client. Competent performance requires the application of knowledge, skill, candor, diligence, thoroughness and preparation reasonably necessary to meet the needs of the engagement.

2. **Advice:** In representing a client in an advisory capacity, a consulting Service Provider shall exercise objective professional judgment and render candid advice.

3. **Accuracy:** Service Provider(s) and Client(s) should provide each other with accurate and reasonably verifiable information and resulting materials in connection with each engagement.

4. **Diligence:** A Service Provider should act with reasonable diligence and promptness in performing work for a Client.

5. **Communication:**

    a. A Service Provider should:

        i. Consult with the Client about the means by which the Client's objectives are to be accomplished;

        ii. Keep the Client informed about the status of the matter consistent with the reasonable expectations of the Client;

        iii. Promptly comply with reasonable requests from the Client for information;

        iv. Promptly advise the Client of any limitation(s) that could materially impact the extent or quality of services to be provided;

v. Promptly report the existence of suspected child pornography to the appropriate legal authorities as required by law.

b. A Client should:

i. Promptly inform a Service Provider of any circumstance that may materially alter that Service Provider's engagement, including, but not limited to, changes in timing, scope and payment for services rendered or to be rendered;

ii. Keep the Service Provider informed about changes in the status and scope of the engagement that may materially impact the Service Provider;

iii. Keep the Service Provider reasonably informed about payment for services rendered in connection with the engagement; and

iv. Promptly comply with reasonable requests for information that may assist the Service Provider in performance of its duties.

6. **Reasonable Fees and Expenses:**

a. A Service Provider should not make an agreement for, charge, or collect unreasonable fees or an unreasonable amount for expenses. The factors to be considered in determining the reasonableness of a fee include the following:

i. The novelty and difficulty of the engagement, and the skill requisite to perform the service properly;

ii. The likelihood, if apparent to the Client, that the acceptance of the particular engagement will preclude other employment by the Service Provider;

iii. The fee customarily charged for similar services;

iv. The amount involved and the value to the Client of the services rendered;

v. The time limitations imposed by the Client or by the circumstances;

vi. The nature and length of the professional relationship with the Client; and

vii. The experience, reputation, and ability of the Service Provider and its personnel in performing the services.

b. A Client should pay undisputed invoices in a timely manner, subject to terms agreed upon by the Client and Service Provider in advance.

7. **Cost-Effective Alternatives:** A Service Provider should make commercially reasonable efforts to inform its Client throughout the engagement of reasonably foreseeable, cost-effective, alternative processes or products available through that Service Provider for achieving the Client's stated objectives.

8. **Confidentiality:** A Service Provider shall not reveal information relating to an engagement unless the Client gives written consent for such disclosure.

9. **Candor:**

   a. **Information about Products or Services:** A Service Provider shall not make false or misleading statements about the Service Provider or its services. Nor shall a Service Provider make any knowingly false or misleading statements about any other Service Provider. Any statement issued by a Service Provider regarding its capabilities, or the capabilities of any competitor, should have a factual, empirical basis that can be reviewed with the Client upon request.

   b. **Judicial, Quasi-Judicial or Regulatory Proceedings:** A Service Provider shall not make a false or misleading statement in connection with any judicial or quasi-judicial proceeding, including formal hearings, meet and confer conferences, or any other proceeding related to ongoing or pending litigation, regulatory or legislative inquiry.

Discussion

Competence, clear communication, diligence, and candor by the Service Provider are essential practices in establishing and maintaining appropriate standards of professionalism in connection with electronic discovery. Further, these practices should be reciprocated by the Client.

The committee does not take any stand regarding the specific value and associated pricing for products and services offered by Service Providers. We acknowledge and support the principle of caveat emptor. That principle, however, does not excuse taking unreasonable advantage of a buyer who clearly lacks knowledge of the electronic discovery marketplace. Thus, we provide guidelines for ethical decision-making in determining whether fees and expenses charged by a Service Provider in connection with any engagement may be considered to be reasonable.

These guidelines include seven factors that should be weighed in their totality. For example, when we discuss the issue of the fees customarily charged for a service, one should consider the total package of services provided on a given matter versus a specific unit / hourly cost for one component of the package. The value of the service provided to a purchaser can, and will, vary from case to case. What may be of value to one purchaser may be of little value to another, and we recognize that price and value are highly subjective.

Our intent is to provide ethical guidelines for pricing to the sophisticated seller who is knowingly facing an unsophisticated buyer. As a corollary, we believe an unsophisticated buyer has an obligation to gain knowledge and expertise of the market prior to making purchasing decisions either directly or through engaging the services of a knowledgeable E-Discovery consultant.

We specifically call out the issue of the discovery of child pornography in regards to professionalism. Images of apparent child pornography are found from time to time during the electronic discovery process. Due to strict liability laws regarding the possession of such images, Service Providers who discover them are required by law to immediately contact law enforcement and surrender possession. This legal reporting obligation supersedes any duty owed to the Client.

Principle 2 - Engagement

Principle

Service Providers should collaborate with Clients to establish and memorialize the terms of their relationship including any reasonably foreseeable parameters as early as possible upon the initiation of any new engagement.

Corollary

Clients should provide sufficiently detailed information about the subject matter, the parties involved in the litigation and any material issues or variables that would assist the Service Provider in accurately defining the engagement.

Guidelines

1. Clients should make reasonable efforts to conduct and complete appropriate pre-proposal research to adequately understand the requirements of the engagement prior to issuing a Request for Information or Proposal.

2. Requests for Information or Requests for Proposals should be made in a good-faith attempt to secure services or products for an actual and specific engagement. Such requests should be sent only to Service Providers who may be reasonably anticipated to be eligible to be awarded part or all of the prospective engagement.

3. If prior to the formalization of an engagement the Client discovers information that may materially impact the engagement, the Client should not proceed with the engagement until the impact of the new information has been incorporated into the proposed engagement.

4. Consistent with Principle 1, Clients and Service Providers should make timely disclosures of any information that may materially impact the engagement, time frame, scope, payment terms or parameters related to the work to be performed.

5. Consistent with Principle 1, Service Providers should, at time of engagement, disclose any reasonably foreseeable fees or expenses that may be charged to the Client at any time during, or at the conclusion of, the engagement.

6. Consistent with Principle 1, circumstances that result in material changes in the objectives, scope, approach, assumptions, timing, or fees should be communicated promptly by both parties.

7. Service Providers should disclose to the Client the anticipated use of any sub-contractors or other third-party providers prior to use of such personnel.

Discussion

The Guidelines set forth above are intended for the majority of standard litigation and regulatory matters where the engagement of a Service Provider is part of an overall discovery process and is done with foresight and planning. We recognize that the demands of business and practice of law occasionally require that an engagement begin before the full parameters of a specific engagement may be known by all of the parties. Likewise, we recognize that some engagements are for a very limited time and scope, and a full Request for Information or Proposal process would be impractical. Our intent is to promote reasoned and ethical decision-making that is exercised through the standard day-to-day business process of at least two of those parties attempting to reasonably define and agree upon some of the basic elements common to all engagements. Agreement as to scope, duration, and material elements of an engagement will help to avoid future conflict and to protect either the Client or the Service Provider from incurring undue fees and expenses or legal exposure.

Principle 3 - Conflicts of Interest

Principle

Service Providers should employ reasonable proactive measures to identify potential conflicts of interest, as defined and discussed below. In the event that an actual or potential conflict of interest is identified, Service Providers should disclose any such conflict and take immediate steps to resolve it in accordance with the Guidelines set forth below.

Corollary

Clients should furnish Service Providers with sufficient information at the commencement of each engagement to enable each Service Provider to identify potential conflicts of interest. If an actual or potential conflict of interest is identified and disclosed and the Client elects to proceed with the engagement, the Client should work in good faith with the Service Provider and other parties to facilitate a resolution to any such conflict in accordance with the Guidelines set forth below.

Guidelines

1. A conflict of interest may arise when an organization or individual is in possession of proprietary information from a current or former Client. It may also arise when an organization or individual has a financial stake in a process, software product, Service Provider, or staffing organization. The issue is whether an independent observer might reasonably question whether the advice given to a current or potential Client may be improperly influenced by the Service Provider's financial interest or possession of such proprietary information.

2. To avoid potential conflicts of interest, Service Providers should maintain a conflicts checking system and divulge any interests that are relevant to the engagement at hand. A conflicts checking systems should include up-to-date information on each matter for which they have been engaged, including the Litigants, their legal representatives, and a description of the work performed, as well as matters for which employees of Service Providers have worked other than at the current Service Provider.

3. Prior to commencing any new engagement, a Service Provider should request, and the Client should provide, the caption information for the matter, the list of all legal counsel for all parties, and any other relevant information that will assist the Service Provider in identifying potential conflicts of interest.

4. Service Providers should process all available information regarding the parties and their legal representatives through their conflicts checking system in order to identify any conflicts of interest prior to commencing work on the matter. In the event that the Client requires services to immediately commence in order to meet a court imposed deadline, this checking should be done as soon as reasonably practical.

5. In the event a Service Provider identifies a conflict of interest, the Service provider has two courses of action: (a) turn down the proposed engagement, or (b) make timely disclosure to the appropriate parties.

6. Once a conflict of interest is identified and disclosed, the impacted parties should work together in a timely manner to determine if such a conflict can be mitigated.

7. Conflicts of interest that cannot reasonably be mitigated must be avoided.

8. If, following informed disclosure, all impacted parties determine in good faith that the identified conflicts can be mitigated, the impacted parties should agree on steps that will adequately memorialize the disclosure of the conflict and the steps taken to mitigate that conflict.

9. Service Providers should not proceed with an engagement where one or more conflicts have been identified until those conflicts have been resolved and the resolution is adequately memorialized to the satisfaction of all parties involved. In the event of a merger or acquisition involving two or more Service Providers, the Service Providers should take appropriate steps to ensure that the information in both of their respective conflicts checking systems is consulted at the start of a new engagement.

10. In the event of a merger or acquisition involving two or more Service Providers, the Service Providers should, within a reasonable period of time, identify conflicts of interest resulting from the merger or acquisition, and take prompt steps to disclose and mitigate any such conflicts.

11. In the event a Service Provider encounters unforeseen conflicts of interest during an engagement, the Service Provider should disclose the identified conflicts and attempt to mitigate such conflicts in accordance with the guidelines set forth above.

12. A Service Provider should implement appropriate procedures for establishing an ethical wall to screen out one or more employees, if required, to resolve a conflict.

13. Absent superseding contractual obligations, Service Providers should withdraw from an engagement to avoid a conflict of interest that cannot be otherwise resolved. Any withdrawal should be performed in such a manner as to reasonably avoid undue prejudice or disruption to the Client.

14. Service Providers should not divulge or reveal the substance of any communications between the Service Provider and any Client to any third party absent express written permission from that Client (or its authorized representative) or a valid order from a court of competent jurisdiction.

15. Service Providers should not release a Client's ESI or other materials to any third party without the express written permission from the Client (or its authorized representative), or upon service of a valid order from a court of competent jurisdiction.

Discussion

This Principle makes paramount the timely identification, disclosure, avoidance or mitigation of conflicts of interest between Service Providers and one or more Clients.

Defining "Conflicts of Interest"

In the context of this rule, Conflicts of Interest arise when a Service Provider has two or more duties that are in opposition to one another. Such duties may be personal or professional, contractual or fiduciary, formally prescribed by law or informally established by societal norms. Conflicts of Interest must be distinguished from the competing day to day obligations that arise in the context of business and personal relationships. Routine obligations resulting in competing priorities do not rise to the level of a Conflict of Interest and are not addressed in this Model Code. This Model Code is intended to address only the Conflicts of Interest which occur in connection with the establishment and performance of a business relationship between a Client and a Service Provider.

Conflicts of interest are classified as actual conflicts, potential conflicts and springing conflicts. **Actual conflicts** are those already in existence at the time a relationship commences. **Potential conflicts** are those that may be reasonably anticipated to occur sometime during the existence of a relationship but have not yet matured. **Springing conflicts** are those that did not exist and were not reasonably anticipated at the commencement of a relationship, but arise unexpectedly during the course of an engagement.

Special Issues Related to "Clients"

A Service Provider owes a duty to the Client. In the simplest terms the "Client" is any signatory party to an agreement with a Service Provider. In the electronic discovery services industry, engagements often include three parties: a Service Provider, a Law Firm, and the Litigant (i.e., the Individual or Organization who is a party to a legal or regulatory action subject to Discovery). Often a law firm is the sole signatory party to an agreement for discovery services and it is the law firm that exclusively directs and supervises a Service Provider for the benefit of the Litigant. The tangential relationship of the Litigant to the party requesting electronic discovery services begs the question: "is the Litigant also a Client?" If the Litigant may also be considered to be a client of the electronic discovery service provider, to which client does the Service Provider owe the ultimate duty? There may be circumstances in which the actions of the Service Provider may favor one client over the other.

Business Conflict vs. Conflict Of Interest

Conflicts between the instructions or the interests of the Litigant and the Law Firm can give rise to a business conflict for a Service Provider, but not an ethical Conflict of Interest. Such business conflicts are outside the scope of this Model Code.

Conflicts with Other Codes of Conduct

Service Provider organizations often employ attorneys, accountants, and other professionals who are subject to binding rules of conduct governing ethical behavior within those professions. We recognize that these professionals may be subject to ethical obligations that are both superseding and superior to those set forth in this Model Code of Conduct, even if they are functioning in the role of Service Provider and not the role of their professional license (e.g., a licensed attorney serving as a discovery consultant, not as legal counsel).

Even though an organization determines, under the guidelines set forth herein, that it may mitigate a conflict, an employee who would be assigned to the engagement may still determine that work on such an engagement would conflict with his or her superseding professional obligations. Professionals who find themselves torn between duties to their professional ethical obligations and their duties to either their employer or Client should exercise due care in determining their individual best course of action, and the Service Provider and its Clients should be sensitive to employees who face this dilemma.

Personnel Transfer Resulting in Conflicts

The principle of the Ethical Wall (a/k/a Chinese Wall, Firewall or Screened) should apply to Service Providers to the same extent, and under the same rules, as the creation of an Ethical Wall for attorneys at a Law Firm. (S*ee, ABA Model Rules of Professional Conduct, Section 1.10(a)(2).*)

Principle 4 - Sound Process

Principle

Service Providers should define, implement and audit documented sound processes that are designed to preserve legal defensibility.

Corollary

Clients should cooperate with Service Providers to ensure that auditable, documented sound processes, appropriate for each engagement, are defined and implemented by all concerned parties to preserve legal defensibility.

Guidelines

1. Service Providers should exercise reasonable diligence to remain knowledgeable and competent in regards to current best practices related to sound processes for preserving legal defensibility.

2. Service Providers who develop products for use in the legal or regulatory process should exercise reasonable diligence in ascertaining and confirming that each product meets current best practices related to sound processes for preserving legal defensibility.

3. Service Providers who perform services in connection with the legal or regulatory process should exercise reasonable diligence in ascertaining and confirming that their services meet current best practices related to sound processes for preserving legal defensibility.

4. Prior to the acquisition or use of a product created for use in the legal or regulatory process, the acquiring party should make reasonable inquiry of the developing Service Provider regarding the testing, scientific validity, and legal defensibility of the processes incorporated into the product, as appropriate.

5. Prior to sales, and upon inquiry, Service Providers who have developed a product for use in the legal or regulatory process should make reasonable disclosure of the processes incorporated into their product, including auditing features, to permit the acquiring party to determine if the product meets current best practices for ensuring legal defensibility.

6. Prior to engagement, Clients should make reasonable inquiry of their Service Providers regarding the standard auditable, sound processes utilized by the Service Provider, as well as customizable sound process that may be implemented for that specific engagement.

7. Prior to engagement, and upon inquiry by a prospective Client, Service Providers should make full disclosure of all standard and customizable sound processes utilized by the Service Provider.

8. Service Providers should promptly notify Clients of any known breakdown in a process, respond to Client inquiries relating to the breakdown, and promptly implement appropriate remedies.

9. Clients should not disclose to any unrelated party any proprietary information regarding the processes employed by the Service Provider; provided, however, Clients may make such disclosures as reasonably necessary to avoid or resolve disputes (a) regarding the legal defensibility of the Service Provider's processes, or (b) between the Client and the Service Provider.

Discussion

This Principle rests on two concepts: Legal defensibility and risk mitigation.

The first concept relates to the overriding requirement that technology and processes must meet the requirements of defensibility in connection with legal and regulatory matters. "Legal defensibility" as discussed herein is measured by various rules of civil and criminal procedure, as well as standards for the admissibility of evidence in courts of law, alternative dispute resolution, administrative and legislative hearings. These rules may require the application of scientific principles and practices to the legal process. Amongst these principles include defined repeatable processes, established procedures for testing and auditing results, and the potential for peer review.

The second concept relates to ensuring that potential human and/or machine errors are anticipated, and the attendant risks are mitigated in advance. Sound processes for Service Providers, therefore, must include implementation and ongoing maintenance of protocols, hardware and software, that reduce the impact of any such potential error. Quality control and assurance should be an organizational imperative for Service Providers, and a Service Provider's failure or refusal to proactively address these issues not only raises the potential of litigation based upon a perceived or actual legal liability, but is by itself ethically suspect.

A Service Provider offering a product for use in the legal and regulatory process should, upon request, provide to a Client sufficient detail regarding the operation of its product to permit the Client to adequately assess the potential legal defensibility of that product. While a Service Provider may not be required to disclose any trade secrets other than by valid court order, a Service Provider's refusal to make full disclosure of any facts that may impact the legal defensibility of its products and processes may be taken into consideration by a Client in selecting a Service Provider. If a Service Provider elects to disclose trade secrets during the selection process, it may reasonably request appropriate legal protections be implemented.

In honoring a Service Provider's request to protect proprietary information, a Client should not disclose any such information to any individual or organization that has no direct interest and involvement in the selection of the Service Provider for the purposes of the engagement.

Principle 5 - Security and Confidentiality

Principle

Service Providers should establish and implement procedures to secure and maintain confidentiality of all Client ESI, communications and other information.

Corollary

Clients should work with Service Providers to ensure that reasonable measures, appropriate for each engagement, are established and implemented by all concerned parties to secure and maintain confidentiality of all ESI, communications and other information.

Guidelines

1. Service Providers should develop policies and procedures for ensuring the security and integrity of Client ESI, confidential communications and other information.

2. Service Providers should exercise reasonable diligence to remain knowledgeable and competent in regards to best practices related to privacy and data security in all aspects of handling Client ESI, confidential communications and other information.

3. Prior to engagement, Clients should make reasonable inquiry of their Service Providers regarding the level and types of security measures that the Client deems appropriate for that specific engagement.

4. Prior to engagement, and upon inquiry by a prospective Client, Service Providers should make full disclosure of all standard security measures implemented by the Service Provider, as well as security measures available and recommended for that specific engagement.

5. Service Providers should implement reasonable measures to secure their facilities from unauthorized physical access.

6. Service Providers and Clients should implement reasonable measures, appropriate to Client requirements, in connection with securing ESI, confidential communications and other information from unauthorized logical access.

7. Service Providers should implement reasonable measures, appropriate to Client requirements, to secure ESI, confidential communications and other information contained on portable devices taken outside the Service Provider's facilities.

8. Service Providers working internationally or with Client ESI coming from international sources must be capable of complying with applicable foreign data privacy laws related to security and confidentiality.

9. All ESI, communications and other information received from a Client should be presumed by a Service Provider to be confidential unless otherwise stated in writing (*See also, Principle 1 – Professionalism*).

10. Service Providers have the duty to promptly notify Clients of the unauthorized release, disclosure, or loss of Client ESI, confidential communications or other information in the custody of the Service Provider.

11. Upon request of a Service Provider, Clients should not disclose to any unrelated party any of the Service Provider's proprietary or confidential information provided to the Client in connection with an engagement or prospective engagement; provided, however, Clients may make such disclosures as reasonably necessary.

12. Service Providers and Clients should agree in writing to the disposition of Client ESI, confidential communications or other materials upon the termination of any engagement, including its return or destruction.

Discussion

The principle of confidentiality is deeply rooted not only in the basic expectation that Client information will be protected from disclosure to unauthorized parties, but also with due regard to applicable evidentiary issues. We give significant attention to the principle of confidentiality throughout this Model Code, and the requirement for all parties to take reasonable and affirmative steps to preserve the confidentiality of Client ESI, communications and other information.

We repeatedly use the phrase "ESI, communications and other information" in this Principle, with the intent that confidentiality shall broadly cover all case/matter related materials, in electronic or hard copy form, as well as relevant work product and written or verbal communications related to the engagement.

Likewise, we consider work product to be broadly inclusive of all engagement related documents, including, but not limited to, RFIs/RFPs and responses, instructions, project specifications and scoping documents, chain of custody materials and status reports.

We intend the term "communications" to be inclusive of all exchanges by or between the Client and Service Provider, as well other related and authorized parties involved in a case/matter. We firmly believe that such exchanges should be presumed confidential, without regard to whether such exchanges fall under the legal definitions of information covered by the attorney-client privilege or under the doctrine of work product.

The guidelines advise implementing reasonable procedures to secure portable devices. For the purposes of this Principle, such devices are not limited to those that are typically used for the transportation of case specific Client ESI, such as USB hard drives, but are intended to broadly cover all portable devices containing confidential communications and other information. We intentionally do not distinguish one portable device from another, since all ESI, communications and other information must be safeguarded from unauthorized access or release regardless of the precise device on which such information is housed or carried.

The guidelines additionally advise implementing reasonable measures in securing ESI, confidential communications and other information from logical security penetration, either while the ESI is housed or in transmission. Logical security is defined by one common source as "software safeguards for an organization's systems, including user identification and password access, authentication, access rights and authority levels." Because transmission of such ESI is between at least two parties, determination of what is reasonable applies equally to both Service Providers and Clients.

As a practical matter, we note that certain Service Providers have implemented physical and logical data security practices in accordance with recognized certification standards such as SAS70 or ISO-27001. Clients should be aware that under those standards, the Service Providers cannot operate their security programs below certain thresholds. As a corollary, we recommend that Clients cooperate with the operational constraints inherent in such SAS or ISO certified operations so as to ensure that data security is consistently maintained above certain those minimal levels and are equally supported by all Service Providers involved throughout the case/matter.

Subject to Principle 3, Service Providers should maintain confidentiality absent express release by the Client, or as otherwise provided in a written contract between the parties, even in the event that confidential communications or other information become part of the public record.

www.edrm.net/projects/mcoc