4A's MSA Guidance Series

February 2016

Data Security: The Rules of the Road

A Guide to Agency Data Security MSA Predominant Practices Frequently Asked Questions (FAQ's)

Data Security: The Rules of the Road
A Users Guide to Agency Data Security MSA Predominant Practices
Frequently Asked Questions (FAQ's)

Background: 4A's MSA Guidance

The increased importance and complexity of agency-client master service agreements (MSA) has resulted in industry requests for guidance and information relating to MSA considerations. In order to accommodate the industry's information needs, 4A's legal affairs and commercial practices communities collaborated on the development of MSA guidance related to key provisions of agency-client agreements.

4A's guidance related to agency-client agreements is intended to provide agency management with a framework for evolving discussion on master service agreements (MSA) considerations and predominant industry practice. The association's MSA Guidance Series publications include:

- 4A's Client Audit Guidance recommends that agencies and advertisers collaborate to design effective efficient controls and verification procedures related to significant marketing expenditures. The guidance notes that comprehensive stewardship arrangements entail alignment on expenditure policies, clarity on internal control responsibilities, agreement on appropriate transparency and relevant scope of verification.

- Allocation of Risk, Indemnification & Limitations on Liability. The purpose of this guidance is to help agency management understand the importance of negotiating appropriate and equitable allocation of risk and limitation of liability provisions in every business arrangement.

Data Security MSA Overview

There has been extensive discussion within the marketing services community related to agency-client data security and confidentiality master service agreement (MSA) terms. Much of the data security and confidentiality MSA provision discussion relates to overly broad, complex client mandates that seek to impose impractical or inappropriate requirements on vendors.

Members of the 4A's finance, legal, technology and compliance communities believe that it is in the best interest of both agencies and clients to provide information on predominant agency data security and confidentiality practices.

This guide is not intended to replace each agency's need for competent legal advice. Agency-client business arrangements including MSA terms and considerations related to data security arrangements have become increasingly complex; consequently, the need for legal and subject matter expertise has increased. This publication does not attempt to describe all data security MSA considerations that may arise and it is not a substitute for competent legal advice.

Executive Summary

The nuances associated with structuring appropriate data security protocols, policies and contractual arrangements can be daunting even for subject matter experts from the legal, technology, compliance and commercial practices communities. Leaders of the 4A's data security task force identified core principles and fundamental concepts that can help marketing services organizations frame prudent data security practices.

When developing your agency's data security approach you will be well served to evaluate the following data security guidance considerations:

- Agency data security policies and provisions of client MSAs are not one-size-fits-all. Your data security approach should reflect the type of services to be provided and the type of data that is collected and used.

- Understanding each individual client's critical data security issues provides a foundation for jointly customizing data security practices that are grounded in the actual services to be provided by the agency and specific data dynamics of the agencies relationship with that client.

- Involve subject matter experts (SME's) early in data security discussions with clients. Typically, when the right people are involved in discussions of requirements, responsibilities, policies, practices and compliance the sides can develop effective, efficient, equitable and practical data security arrangements.

- Agencies should have documented robust data security policies and procedures that are: (1) well-integrated into the agency's servicing operations, (2) understood by agency employees and (3) can be communicated to agency clients and prospects. Consider developing data security communications that your agency can use to facilitate structured, professional and thoughtful data security discussions with clients and prospects. Proactively describe the sufficiency of your data security approach as well as how the agency's policies and practices are consistent with both industry practice and recognized data security protocols.

- It is not practical for any agency to set up and adhere to multiple ways of working to suit each individual client's data security practices. Industry best practice is for the agency to implement the agency's own robust data security policies and practices that are appropriate for the type of services that the agency is performing.

- Data security agreements must balance effectiveness and efficiency. The objective of data security MSA terms should help the agency and the client to: (1) address the reasonable data security concerns of the client with regard to the specific services performed by the agency, (2) operate in a cost effective manner based upon commercially reasonable and feasible compliance and (3) efficiently facilitate marketing program deliverables in order to achieve the client's marketing goals and timelines.

- The interconnectivity of the marketing ecosystem necessitates a collaborative approach to data security where clients, agencies and third party suppliers coordinate their data security efforts, share responsibilities and equitably calibrate allocation of risks.

- Frankly discuss and document the client's data security obligations. Establish the client's responsibility for compliance with laws and regulations applicable to the client's business, products and services. Stipulate that the client will not share Personal Information (PI) with the agency where it is not necessary. Consider requiring expressed written consent from an authorized agency executive prior to transferring personal information to the agency.

- Discuss data security compliance testing and verification protocols. Data security compliance verification can take various forms and not every situation requires an in-depth audit. Frequently, agency self-certification, SAS 70 systems documentation, SOC 2 Type I/Type II or a SOX compliance letter are efficient mechanisms to address client compliance concerns. Data security verification should not normally entail on premise reviews or penetration testing as a customary practice because they can be extremely disruptive and risk exposure of confidential information of the agency or the agency's other clients. The nature and depth of any review should be based on the services provided, the type of data collected and the corresponding data security measures that are agreed upon.

Agencies are well served to take data security contractual obligations seriously. Ensure that you understand the requirements and that you are able to effectively comply with requested requirements.

Clients are well served to precisely focus their data security efforts on significant risks that can be practically addressed through commercially reasonable efforts. It is not in a client's best interest to impose overly restrictive data security requirements on agencies particularly if the client's requirements are unnecessarily complex or inflexible such that suppliers, even when acting in good faith, may not be able to reasonably comply with the client's proposed data security terms.

Data Security MSA Key Topics and Frequently Asked Questions

Agency executives are frequently asked questions relating to applicable industry standards and commercially reasonable data security and confidentiality procedures and practices. This document provides discussion related to critical agency-client data security and confidentiality MSA terms and references predominant industry practices in the USA. The information is structured in a Frequently-Asked-Questions (FAQ) format, i.e., questions followed by discussion of considerations that contain information and best practices.

Table of Contents: Key Topics and Frequently Asked Questions

Table of Contents (continued:)

FAQ # 1 ... Client Data Security Policies: "Non-Negotiable" Term Stipulations

Question: *How should an agency respond when the client submits MSA language that is communicated as being "non-negotiable?"*

Considerations:

Data security provisions of the MSA should not be one-size-fits-all provisions. Rather, these provisions should be adjusted in light of the services to be provided and the type of data to be obtained by the agency in connection with its engagement.

The agency should respond that they take their contractual commitments seriously and are unable to agree to legal terms without the opportunity to review and understand the requirements.

The agency needs to ensure they are able to comply with what is being requested and that it is relevant to the services being performed. The agency should request a call or meeting to discuss the non-negotiable sections with the right people from the client. The agency can use the discussion to ask questions and highlight where the language may not make sense based on the scope of services being discussed and which may, in fact, be contrary to the marketing client's interests.

Typically, when the right people are discussing policy language, the sides can agree on mutually satisfactory terms.

FAQ # 2 ... Client Data Security Policies: "Non-Negotiable" Timing and Inflexible Terms Stipulations

Question: *How should an agency respond when the client submits MSA language that contains extremely lengthy/complex client policy elements which the client wants the agency to accept without providing adequate time for review or flexibility to discuss alternative solutions to the client's concerns?*

Considerations:

Because clients sometimes are not sure what services the agency will be providing, it is tempting for a client to include the most expansive security provisions in order to make sure that every potential situation is covered. However, clients have to appreciate that there is a cost to the imposition of unusual and unnecessary security requirements. If the agency has to institute more expensive and unusual measures, there will be additional costs that the agency will incur and therefore needs to pass on to the client. Additional security measures also may lead to delays that may affect the client's marketing group's ability to market in the most effective way.

There are complexities associated with data security and retention. Each day new models are created to secure, store, analyze, host and secure data. The models may consist of cloud-based offerings, off-shoring of anonymized data for analysis and other emerging technologies. Both the client and the agency need to carefully review all terms since failing to do so may limit the client's ability to request the agency to provide certain services or to utilize vendors that may otherwise be preferred by the client. Similarly, costs associated with adhering to provisions that are not truly mission-critical to the client may also serve to exponentially increase the client's hard-costs and out-of-pocket expenses.

It is not in a client's best interest to impose overly restrictive data security requirements on agencies particularly if the client's requirements are unnecessarily complex or inflexible such that suppliers, even when acting in good faith, may not be able to reasonably comply with the client's proposed data security terms.

The agency and client should collaborate and discuss the agency's current data security measures and determine whether, in light of the anticipated data to be collected by the agency, they are reasonable and adequate or require some form of modification.

FAQ # 3 … Accommodating Client Data Security Policy Elements

Question: *What is an effective response to client-proposed MSA language that obligates the agency to adhere to all client data security policy terms when many of the client's policy elements relate to research & development, manufacturing, materials management and other activities that do not pertain to marketing services?*

Considerations:

An agency and client might consider contract language that stipulates that the agency will comply with the client's policies provided that the data security SME's of both organizations agree that client's policies are substantially similar to the agency's policy and that the agency's policies are sufficient given the applicable services being provided.

If a client continues to push for security requirements beyond what is applicable to the services of the agency, the agency should refer to practical examples of the type of work the agency will perform and seek to reach agreement on data collection and data security implications related to the agency's services. The parties should also discuss how they can and will work together to protect sensitive information, for example:

- The agency should only receive the data that is truly needed.
- The parties can agree on security notice and process filters that should be in place when the agency will be receiving sensitive information so that the appropriate agency executives (lead account person, IT lead, et al.) are aware of the data being received so they can ensure it is properly managed.
- The agency can require that all sensitive data be sent only to the agreed, specified people to ensure proper handling and acceptance of the associated responsibility.

The agency contract negotiation team should also point out to client decision makers that "excessive" security requirements, i.e., those beyond what are applicable to the agency's services, may in fact hinder the client's ability to achieve their marketing program goals and increase the cost of servicing the client's business (costs of incurring duplicative or unnecessary data security obligations will inevitably be passed along to the client).

Furthermore, terms should be constructed to provide that only applicable policies, as agreed in advance and in writing by the agency, will apply.

FAQ # 4 ... Leveraging the Agency's Data Security Policy and Practices

Question: *What is the best way to establish the agency's data security policy, or alternatively appropriate data security standards, as the foundation for data security contract terms?*

Considerations:

It is impractical for an agency with dozens, or hundreds, of clients to simultaneously comply with the particulars of multiple client data security policies.

Agencies should have documented robust data security policies and procedures that are: (1) well-integrated into the agency's servicing operations, (2) understood by agency employees and (3) can be communicated to agency clients and prospects (upon signing an NDA).

Agencies should share their data security policies with the client and be able to describe how the agency policies and practices are consistent with both industry practice and recognized data security protocols (ISO, NIST, FTC, etc.). The agency-client data security conversation should be based on the sufficiency of agency data security procedures relative to the applicable services being provided by the agency to the client. The parties should also discuss and agree upon compliance monitoring options (for example, agency internal and/or external compliance monitoring).

Building on the foundation of the agency's data security policies and procedures, the agency should explain to the client that the agency operating model is such that the agency works with numerous clients and that each client may have a somewhat different approach to data security. From a logistical, cost and compliance perspective it is not practical for any agency to adhere to, and set up multiple ways of working to suit, each individual client's data security practices.

The ideal best practice is for the agency to implement the agency's own robust data security policies and practices that are appropriate for the type of services that the agency is performing, and which should be satisfactory to meet the requirements of all clients. These data security policies should be specifically designed to manage primary security risks associated with the specific services being performed.

FAQ # 5 … The Key Driver of Data Security – Agency's Scope of Services

Question: *What is the best mechanism for framing data security terms solely within the context of the specific scope of services that are being provided by the agency?*

Considerations:

The overriding objective of data security MSA terms should be an agreement that allows the agency to:

- Address and meet the reasonable data security concerns of the client with regard to the specific services performed by the agency.

- Operate in a cost effective manner within contract terms with which the agency can in fact comply (agencies should stress commitment to complying with client contracts and the need to ensure that what is being proposed can actually be adhered to by the agency).

- Efficiently provide the marketing programs and deliverables required to achieve the marketing objectives and timelines of the client.

Flexibility in the data security terms in an agency-client contract could be important (e.g., to allow for changes in services/products to be provided by the agency or to otherwise capture an ability to renegotiate terms if there is a change in the law or regulations), however, ultimately, the parties should ensure that any contractual obligations relate to the services or products being provided by the agency.

FAQ # 6 … Involving Key Data Security Stakeholders

Question: *Who should be involved in data security MSA conversations?*

Considerations:

The parties should ensure that the appropriate subject matter experts (SME's) from both the client and agency side are involved in MSA discussions regarding data security. Discussions on policies, procedures and compliance will likely best be understood by SME's from the client's technology or security group, while agency legal, finance/commercial business and account teams are in a position to understand the compliance, process and cost implications associated with requested servicing scenarios.

Typically, when the right people are involved in discussing data security concerns and commercially reasonable protections, the sides can agree on mutually satisfactory terms.

FAQ # 7 ... Compliance with "All" Laws and Regulations

Question: *If the client MSA stipulates that the agency comply with all data security laws and regulations, how is an agency supposed to know every local law and regulation?*

Considerations:

In the context of data security, where multiple jurisdictions are regularly issuing new legal requirements, it is not realistic for the agency to agree to know every local law and regulation, given that many might have little or no applicability to the services the agency provides. An agency should make commercially reasonable efforts to comply with the predominant data security laws and regulations that are applicable to the services the agency is providing the client.

Furthermore, when the client has global marketing operations it is important to be mindful of regulations outside of the United States.

The agency should agree to make commercially reasonable efforts comply with only those laws related to privacy and data security that are applicable to the agency's business and services (not the client's business).

The client should be responsible for all laws, rules, regulations, industry codes and guidelines, etc. applicable to the client's business, products and services.

FAQ # 8 … Sensitive Information

Question: *How should data security MSA discussions reflect sensitive data dynamics?*

Considerations:

In today's ecosystem, an agency's actual access to highly sensitive data is often quite limited. Both the client and the agency need to understand and agree to the different roles and responsibilities of each entity that is in the data chain.

Most agencies' general offering of services does not require the collection of sensitive personal information and, therefore, most agency operations do not generally include protocols for collecting and storing such information. If a client is considering having the agency undertake a scope of work that involves sensitive personal information, the client should want to understand the agency's security protocol at the time and, based on that understanding, decide if it makes sense to share or have the agency collect and store the sensitive information itself or whether it makes more sense for the agency to engage on behalf of the client a specialized third party that has all the necessary protocols and processes in place. If it does not make sense for the agency to have access to sensitive personal information, rather than spending valuable time focusing on data security provisions that may never be implemented, the client instead may want to focus on the protocol for choosing and contracting with a specialized third party vendor that has expertise in handling sensitive information and ultimately will be responsible for the collection, storage and processing of the sensitive information.

If it does make sense for the particular agency to be given access, in certain circumstances, to sensitive information, rather than encumbering an agency-client master services agreement with complex customer/consumer data security provisions that are not immediately or directly correlated with the agency's services for the client, the parties should agree that when and if the agency scope of work entails the agency's handling of highly sensitive data, notice should be given to a person with sufficient stature at the agency (to ensure that the necessary procedures are understood and followed), and the client and agency at the time should establish the data security risk, control particulars and responsibilities of each party.

Linking sensitive consumer data security terms to a specific scope of work has multiple advantages:

- The parties can establish that agency handling of sensitive data requires acknowledgement of that fact from the agency, in writing.

- The parties can carve out a definition of highly sensitive data information (e.g., personal information, client's customer list/data, or other sensitive information) from other more traditional confidential data.

- Client and agency can ensure that the more stringent data security requirements apply only to highly sensitive data which can be separately outlined in the project specifications.

- The parties can ensure that more stringent requirements apply only to SOWs or assignments that involve the highly sensitive data.

When a third party vendor that is not under the ownership, control or management of the agency is going to be charged with the collection of the information, at the time that the scope of work is being determined, the client and the agency can focus on ensuring that the agreement with the third party includes the necessary and specific data security requirements. The client can decide whether the client wishes to enter into the third party agreement directly or have the agency enter into the agreement as its agent. However, under either circumstance, the client needs to understand that the third party will not be an agency subcontractor. The third party is providing services that are not agency core offerings and it is the third party that should be solely responsible for sensitive data security obligations.

It is important for the client to understand that no contractual shifting of liability or risk is going to insulate the client from the negative PR or other negative fallout that may result in the event of a breach of sensitive data. From a financial perspective, there is always the risk that, even with the strongest contractual provisions, the agency may not have the financial wherewithal to meet its contractual obligations. Ultimately, it is in the client's best interest to focus on avoiding a breach, even an inadvertent one. No client should assume that just because it includes in an agreement "non-negotiable" onerous provisions with which the particular agency cannot realistically comply that somehow the client has fulfilled its obligations to its stakeholders.

FAQ # 9 ... Personal Information (PI) Considerations

(Note: For the purposes of discussion related to Personal Information the acronym “PI” will be used throughout this document. PI may also be referred to in the industry as “PII”.)

Question: *What are the special legal and contractual considerations related to PI. How can/ should this term be defined?*

Considerations:

Legal and contractual considerations related to PI do not automatically require significantly heightened security standards. Both clients and agencies need to review the then-current standards associated with privacy and requirements associated with providing end-users with notice of unauthorized disclosure of PI (as defined under relevant state or local law).

Security requirements should be appropriate to the type of PI involved. Agencies and clients should consider the following:

- First, determine what information the agency will be receiving.
- Second, determine if any of that information is PI (e.g., name, address, telephone number, marital status).
- Third, determine the sensitivity of the PI (e.g., SSN, date of birth, credit card number or CSV, a password plus email).

There is no single definition in the United States of PI. The definition will vary depending on the state, type of information and the regulatory body responsible for oversight. For example, does the information pertain to children – Children’s Online Privacy Act (COPPA); is it protected health information – The Health Insurance Portability and Accountability Act (HIPPA); is it financial information – Gramm–Leach–Bliley Act (GLBA)? It is important to understand the data elements that the agency will receive from the client because it will help frame the control requirements and procedures for PI.

Furthermore, a client may have its own definitions of sensitive information. For example; Client confidential information (e.g., non-public received from client or generated for client), Highly confidential information (e.g., SSN), Sensitive personal information (e.g., health-PHI). Therefore, it is important to figure out the client’s expected data security elements in order to see if the client’s terms are reasonable and appropriate given the agency’s services. Then decide whether, based on the personal information at issue, such information warrants need special security requirements. For example, encrypt social security numbers in any transmissions.

FAQ # 10 ... Personal Information Requirements and Agency Scope of Services

Question: *The client standard form MSA refers to PI data security requirements, however, the scope of the agencies services currently does not require the agency to use PI. How should the agency respond?*

Considerations:

When the client's standard agreement includes PI data security requirements, but the scope of the agency's services do not require the agency to handle or manage PI, then the agency should explain to the client that it does not need the PI to perform the services and why. This includes explaining what information the agency will need. It is in the client's interest not to share PI with the agency where is not necessary. Moreover, statutory regulations may prohibit the client from sharing the PI unless the agency takes additional steps in order to receive and safeguard the information.

Clients and agencies may want to consider a stipulation that no personal information will be transferred to the agency unless an executive of the agency has agreed in writing to receive it. Keep in mind, depending upon any future use of PI, there may need to be written agreement or amendment in place that identifies the PI involved and sets out appropriate protocols and procedures related to the methods associated with the transmittal, receipt, hosting and uses of such data.

Rather than encumbering an agency-client master services agreement with complex customer/consumer data security provisions that are not immediately or directly correlated with the agency's services for the client, the parties should agree that when and if the agency scope of work entails agency handling of highly sensitive data, at the time a specific scope of work is contemplated, the client and agency should establish the data security risk, control particulars and the responsibilities of each party.

FAQ # 11 ... Personal Information – Future Services Considerations

Question: *If the client references the potential for future agency services that potentially entail use/storage/access to PI, how should the agency respond?*

Considerations:

If there is the potential for future agency services that will require the agency to handle PI, the agency and client should agree to discuss and negotiate in good faith an agreement with respect to such information at a later date when it becomes clear (1) that such disclosure is necessary and (2) the PI to be disclosed.

The appropriate agency response involves an informed agency business decision. There are two primary options:

- One response could be for the agency to explain to the client that the agency will not take on any of the client's projects that require the agency to receive and manage PI and to explain why – for example, the agency does not customarily handle PI and necessary controls may not be in place – and indicate that the client's PI data security terms are not consistent with the agency's services for the client.

- A second response could be to look at the client's proposed terms to see which controls the agency can meet. Then spend the time to negotiate data security controls parameters that are dependent on specific SOW conditions. For example: if the agency is not set up to meet the technical requirements, then the agency should explain to the client the additional steps it needs to take (e.g., it may require additional field support, licenses or approval by the agency's IT security organization as a security exception, as well as the additional costs that will be incurred and passed through to the client). The agency should make sure that it discusses the proposal with its security team and other relevant stakeholders before agreeing to any such security requirements. The agency should keep in mind that the agency may need to enter into a SOW with these additional protocols/procedures/methods if the proposal is cleared.

No agency should agree to MSA provisions that it cannot satisfy simply because the current scope of services does not require the agency to receive and manage PI. Appropriate MSA terms governing PI should be addressed with care when the agency learns that its scope of services will soon encompass PI.

FAQ # 12 … Verification and Compliance/Data Security Audits

Question: *How are client data security verification concerns customarily and appropriately addressed in MSA's and what should be considered in arriving at appropriate client data security contract compliance verification provisions?*

Considerations:

Many agency-client agreements contain provisions related to the client's "audit" rights with respect to data security. However, an audit right in the context of data security is a bit of a misnomer and may lead to inappropriate assumptions. Rather than an audit, which connotes more of a financial type of review of information, the relevant point of discussion in the context of data security is more appropriately a "verification of compliance." As a practical matter, clients want to confirm whether the agency is following the agreed upon protocol with respect to data security. The nature and depth of the review, therefore, should be based on the services provided, the type of data collected and the corresponding data security measures that are agreed upon. In order to verify the agency's compliance, the appropriate discussion should be around the scope of the review necessary to achieve the requisite verification. Any agreed upon measures should be appropriately tailored so that the review is no broader than necessary to measure compliance with the agreed upon protocol.

Data security verification should not normally entail on premise reviews or penetration testing as customary practice.

- Agencies and clients need to understand that an on premise data security verification and compliance review can be extremely disruptive and will expose the auditor to confidential and proprietary information of the agency and its other clients. Clients need to understand that data security compliance verification can take various forms and not every situation demands a full-blown in-depth audit. If the data being collected by the agency is not particularly sensitive, verification in the form of self-certification or a SOX Compliance Letter may be sufficient. In other situations, a questionnaire or interview of the appropriate personnel at the agency is likely to be adequate. The bottom line is that care should be taken to make sure that the compliance verification procedures are no broader than necessary to meet the client's objectives in light of the data collection expectations. In addition, the client should agree that any client auditor must have the requisite experience and background to be able to conduct the compliance verification efficiently and with minimal disruption to the agency. Furthermore, the auditor should be required to sign an agency-provided confidentiality agreement.

- If a client wants the right to conduct external vulnerability assessments or penetration testing on the agency's infrastructure that is used for delivering client work, most agencies contest the request because penetration testing can compromise the agency's confidentiality obligations (to protect the agency's own information as well as agency obligations to protect the information of other clients). Information revealed, intentionally or unintentionally, as a result of security testing might also include sensitive agency infrastructure information which, if exploited, could lead to a breach or compromise of the agency's data security environment. Alternatives to client penetration testing might include: (1) for service arrangements that entail ongoing agency handling of

particularly sensitive information, the agency might explore the feasibility of sharing redacted results or an executive summary of security testing that the agency conducted/or hired a third party to conduct for the agency (the idea being to protect agency-confidential or sensitive information) or (2) consider solutions that allow the agency to deliver work without hosting any client sensitive information on the agency's infrastructure. These alternatives should satisfy the security concerns of client compliance teams.

The parties should discuss the feasibility of establishing separate client-specific infrastructure and IT systems/servers within the agency. Any client-specific infrastructure platform should be created at the client's cost and be accessible for data security compliance verification by that client.

In the unlikely event that the nature and type of data to be collected merits in-depth verification or an on premise review of the agency's systems and processes, the scope of the review requirements and the necessary security measures should be discussed. It should be noted that when conducting a review of the agency's systems, the auditor will be exposed to confidential information of the agency and its other clients – thus putting the agency in risk of breach of other agreements and exposing the agency's proprietary processes to a third party. Therefore, in the unlikely event that the situation and nature of the information collected merits an on premise review, the agency should require a third party independent auditor to conduct the review. If a third party auditor is to be used, the selection of that auditor should be mutually agreed upon to ensure that the auditor has the experience and professionalism to conduct the review in the most efficient and least disruptive manner. In advance of any third party review, the agency and client should agree on the scope of the review, understanding that the scope will differ depending on whether the review is the result of a data security breach or simply to confirm verification with protocols. In either case, the agency and client should clearly communicate to the auditor the audit scope, the auditor code of conduct expectations, as well as any limitations related to information access (including limitations on access to agency confidential information and other clients' data) and the requirements with respect to the disclosure and use of the information gleaned from the audit. The auditor also should be instructed that the only information that may be communicated to the client as a result of the review is either a certification that the agency is in compliance with the agreed upon protocols or a recitation of any specific deviations from the agreed upon protocols. The auditor should be required to sign an agency-provided agreement agreeing to the confidentiality and other agreed upon requirements of the review and the client should pay the cost of the auditor and review. The client and agency should also agree on reasonable notice and appropriate frequency parameters related to any data security verification terms.

In those unique circumstances where data security risks are potentially significant, the 4A's publication 4A's Client Audit Guidance provides helpful suggestions related to structuring audit scope, auditor selection and confidentiality protection principles.

FAQ # 13 … Assumption of Liability (Remediation and Indemnification)

Question: *When discussing data security MSA terms, inevitably there is conversation related to allocation of risk, indemnification and remediation. What considerations should be included in MSA discussions?*

Considerations:

Unfortunately, even with very sophisticated data security, a breach can occur. Clients may request that the agency take on various forms of liability as a result of a breach, including remediation and/or indemnification obligations. The nature and type of liability that is appropriate for an agency to assume should correlate to (1) the type of data collected by the agency and (2) whether the breach is the result of a failure to comply with an agreed-upon security process or the result of an unanticipated and unavoidable hack.

A. Remediation

Remediation in the event of a security breach may take a number of forms. It may include (1) undertaking, and paying for, forensic investigation of the breach, (2) implementation of technological fixes to security systems to halt the breach, (3) implementation of preventative programs and (4) reporting to appropriate authorities. In addition, there may penalties and other remediation measures that are required by law. “Fault” may be an important consideration for agencies in assessing remediation liability. If the breach is a result of the agency’s negligence or willful misconduct in failing to comply with the agreed upon security measures, it may be incumbent on the agency to pay for certain of the costs of remediation. If, on the other hand, the breach was unavoidable with reasonable security measures in place, the parties should consider the fundamental premise that no party should bear responsibility where it does not control the underlying conduct or cannot reasonably protect itself against the risk.

Clients may wish to include additional remediation requirements that impose liability on the agency based on presumed damages. In some cases, clients include a requirement that, in case of a breach, the agency provide more consumer facing remediation, such as consumer disclosure and notification requirements, and assumption of the costs of fraud protection (e.g., credit monitoring). However, the damages that flow from a breach will vary based on the nature of the data that was compromised, and, in many, if not most, cases, in light of the type of information collected, these type of measures may not be appropriate. For example, if the agency is not collecting financial information, there is no correlation between a credit monitoring remedy and any breach of data that may occur. The requirements imposed by law, on the other hand, provide an objective standard that correlates the damages (e.g., fines and penalties) to the type and class of data breached. While clients may want to provide remediation to their customers beyond that which is required by law, the costs of this additional remediation can be significant. A client can generate goodwill with its customers by providing remediation perks, such as fraud protection, etc., that go beyond that which is required by law and may not correlate with the damage to the consumer in light of the type of information that has been breached. It is not a reasonable balance of risk for the agency to finance the cost of generating goodwill when the type of data collected is not correlated to the remedy and the remedy itself is beyond that which is required by law.

B. Indemnification

An agency's indemnification obligations, if any, should be commensurate with the type of data the agency collects or accesses and other business considerations related to the client account. The costs associated with indemnifying for a security breach incident can be high, and agencies should fully understand the potential costs they may face before agreeing to broad indemnification obligations. Once again, fault is an important consideration for agencies in assessing how much indemnification liability is commercially reasonable for the agency to assume. If a breach was unavoidable with reasonable security measures in place, before an agency agrees to indemnify, the agency should consider the risk and liability it is taking on in light of the scope of services provided by the agency and the compensation it is receiving. If, on the other hand, a breach is solely the result of the agency's negligence or willful misconduct in failing to comply with the agreed upon security measures, although the same considerations need to be addressed, the agency may be more agreeable to taking on greater resulting liability to third parties.

In addition, in determining an agency's indemnification obligations, a distinction should be made between services directly provided by the agency and controlled by the agency and services delivered by third party suppliers for the benefit of the client. The agency should not be responsible for guaranteeing the performance of third party suppliers or indemnifying for a data security breach arising out of third party services. Indemnification obligations related to services provided by third party suppliers should be the responsibility of the third party supplier and should be incorporated in the agreement between the third party supplier and the client (or the agency, on behalf of the client).

In any case, before an agency takes on any indemnification liability, the agency should confirm the extent and limitations of its cyber liability insurance to ensure that the agency has (or even can obtain) coverage for any indemnification risk it takes on.

The 4A's publication Allocation of Risk, Indemnification & Limitations on Liability discusses principles related to allocation of risk and limitation of liability provisions in business arrangements.

FAQ # 14 … Insurance

Question: *If the client asks the agency to obtain insurance, how can insurance availability and responsibility be factored into MSA data security discussion and terms?*

Considerations:

Clients, vendors and agencies must collaborate and integrate data security procedures and protections. Data security MSA discussions should include dialogue and agreement related to insurance options that mitigate risks across the data security supply chain.

Negotiating assumption of liability thresholds with clients could involve discussing whether the agency can obtain insurance to cover the liability to which it is agreeing in the MSA. It is possible for agencies to obtain insurance covering selected data privacy and breach risks however the premium costs can be significant and the coverage parameters may be limited. Agencies should carefully review their policies with their providers to determine what coverage may be appropriate for the scope of services that agency provides.

Agencies may consider agreeing by contract with clients that agency and client each maintain certain types and amounts of insurance covering data security risks, provided with respect to the agency, the amounts and types of insurance are reasonable in light of the client engagement.

The cost of agency data security insurance coverage including premiums, deductibles, co-insurance and potential exposure beyond insurance coverage cap amounts should be factored into the agency remuneration structure with the client which could take the form of either a direct pass-through reimbursement by the client or via inclusion of the insurance cost as a factor when arriving at the agency's aggregate level of compensation from the client.

Agency and client should collaboratively structure contractual agreements with third party vendors that specify the vendor or subcontractor's data security insurance obligations.

Agencies should carefully review their insurance policies with qualified insurers/brokers to determine coverage that is appropriate for the scope of each client MSA.

FAQ # 15 … Vendor Terms

Question: *What is the best practice for aligning a client's data security and confidentiality needs with the conduct of entities that are not parties to the MSA but that contribute to work encompassed by the MSA?*

Considerations:

It seems clear that even with a comprehensive MSA, a client's data security concerns cannot be satisfied if third parties obtain confidential data and do not conduct themselves appropriately. It is therefore important to the client that third parties, whether they are described as "vendors" or "subcontractors," conduct themselves in a manner consistent with the client's needs.

In determining the agency's obligations with respect to third party data security obligations, the distinction between a vendor and a subcontractor becomes very important. The agency has different responsibilities to the client with respect to vendors and subcontractors, and the MSA should be drafted to reflect these differences.

A subcontractor is a party that has been engaged by the agency as a principal to perform services that are part of the agency's core staffing and the cost of which is paid by the agency from its own resources (e.g., from its fee income) on an undisclosed basis. Because subcontractors are in effect being covered by the agency's fee or other similar compensation, the agency is being paid for these services and the agency should take responsibility for these services in the same way that the agency takes responsibility for its own services. On the other hand, vendors or suppliers (which terms are generally synonymous and are used interchangeably in this response) provide services that the agency does not offer (or are not part of the offerings for the particular client) and are instead tangential and complementary to the agency's core offerings (examples of vendors and suppliers could include photographers, stock houses, shipping companies, music suppliers, hosting providers, licensors of material, etc.). These parties are generally paid by the agency on a disclosed, pass-through or net cost basis.

Unlike subcontractors, the choice of vendors to a great extent is dictated by the client's budget. It would not make business sense to the agency for the client to be able to save money by going with a low cost provider, and then force the agency to guarantee that party's performance. If, theoretically, the agency was to take full responsibility for unaffiliated third parties, logically the agency would want to choose the most high-end and high-priced provider that would presumably be less likely to have problems (or problems for which they cannot or do not take full financial and other responsibility). The reality is that the agency does not, and should not, have that control.

It may be incumbent on the agency to take responsibility for its own negligence and misconduct in connection with third party vendors, which would include negligence in choosing or supervising the third party. However, as a general matter, clients must recognize that an agency likely has much less control over a third party supplier in connection with its data security obligations than it may have with respect to other types of obligations and services performed by a third party supplier. Therefore, the agency's negligence should be evaluated in light of the nature of the third party's obligations and the client's budget and other requirements that impact the choice of vendor.

Further, any requirement that the agency take responsibility for third party vendor performance can put the agency in conflict with its obligation of loyalty to its client. The agency is acting on behalf of its client when dealing with vendors and suppliers, and, as such, as a general matter, should follow the client's instructions with respect to those dealings. For example, a client may decide that it does not wish to pay a vendor because it believes the vendor did not perform in accordance with its contract. Even if the agency does not fully agree with the client's assessment or feels that the client's assessment, although perhaps correct, does not make business sense, it is ultimately the client's decision on how it wishes to deal with the third party and, as the client's agent or representative, the agency will generally proceed accordingly. However, if the agency were taking responsibility for the third party, it could be in the agency's interest to take an adversarial position to the client and defend the third party if the agency does not agree with the client's assessment or to follow a different path if the agency feels that a different business decision should be made. If the agency follows the client's instructions and also takes responsibility for the third party, the agency could find itself caught in the middle and in the untenable position of being in legal conflict with a third party based on a position that the agency may not agree with or feel strongly about. Therefore, the agency should focus on following its client's instructions and on its duty of loyalty to its client rather than on being adverse to its client in order to avoid the potential imposition of liability that may be alleged to arise out of third party performance over which the agency has no real control.

The MSA should draw a clear distinction between the agency's responsibilities with respect to data security obligations between services performed by a vendor or supplier and those performed by a subcontractor. Subcontractors should be expected to comply with the same (or substantially similar) data security and confidentiality terms that are applicable to the agency. However, the obligations and liabilities related to services provided by third party suppliers should be the responsibility of the third party supplier and should be incorporated in the agreement between the third party supplier and the client (or the agency, on behalf of the client). The focus in the MSA with respect to vendors and suppliers should be on the process for choosing the third party vendor or supplier and on making sure that the vendor/supplier agreement contains terms with which the client is agreeable in light of the nature and type of data that is being collected, and the services that are being performed, by the particular third party vendor/supplier.

Clients may want to consider arrangements such as:

- Presenting the client's data security requirements and commercial terms to the third party at the time of proposed engagement of the third party. If the third party resists conforming to those terms, the agency should obtain written direction from the client as to how it wishes to proceed.

- The agency, in concert with the client, should ensure that the third party contract contains appropriate audit rights in light of the client's corporate position and the type and nature of the data being collected.

- For certain types of third party services, the agency and the client should consider requiring the third party to certify its compliance with appropriate standards (e.g., SAS 70, etc.).

- The agency and the client should assess the availability and protections associated with the third party's insurance.

- The agency and the client should consider identifying a specific position at the agency or the client responsible for assessing the third party's compliance with any data security/confidentiality requirements.

The 4A's publication Allocation of Risk, Indemnification & Limitations on Liability discusses principles related to allocation of risk and limitation of liability provisions in business arrangements.

FAQ # 16 ... Agency Employee Stipulations – Client Policies

Questions: *When client proposed data security and confidentiality provisions require the employees of the agency to agree to client policies, training or testing, how can compliance be reasonably and efficiently be structured?*

Considerations:

The agency's data security process should include training agency staff and reinforcing the importance of stewarding compliance with client contracts.

The agency should also establish mechanisms for informing senior client service staff about any unique client service requirements.

The agency might consider designating someone within the organization with responsibility for training agency staff and stewarding compliance with client contracts (e.g., a designated Compliance Officer or somebody else within the finance/IT/client service team).

The agency data security process should also feature:

- Compliance and staff training requirements can vary by client and so it is recommended that any costs associated with compliance be tracked, so that the agency can factor these expenses (both internal time costs and external third party costs) into the cost of servicing the client, and incorporate data where relevant, into the fee proposal.

- Agency should maintain records that document and track the agency's staff training and compliance monitoring activities including compliance assessment and systemic improvement documentation.

FAQ # 17 ... Agency Employee Stipulations – Background Checks

Question: *Client data security concerns could trigger client requests for agency employee criminal background checks and drug testing. How can an agency simultaneously protect employee rights/privacy and reassure clients?*

Considerations:

An agency should only commit to undertaking employee background checks that are customary by that agency in accordance with their own employment practices.

Client requests for background checks may be more extensive than that performed by the agency in the ordinary course of business. Discussion of any supplemental employee background information should be predicated on the types of sensitive information that the employee will be required to access in the course of their work on the client's assignments.

Agencies should challenge any background checking which goes beyond the agencies rights as an employer in accordance with their own employment policies. The agency and client should recognize that employees may not consent to background checks.

If an agency agrees to perform background checks, the agency should make sure to consult with an employment attorney in order understand what rights they have to act upon any information obtained. An agency should also understand what results of a background check, if any, they are able to share with the client.

Customary business and staffing practices should also be considered. For example, at junior staffing levels and for clients that utilize shared agency staff resources, agency employees may come on and off a client's business frequently, making it difficult to ensure that special types of background checks, that are unique to a specific client, are performed.

FAQ # 18 … Client Data Security Obligations

Questions: *What are the appropriate client obligations that should be included in the data security provisions of agency-client agreements?*

Considerations:

Successful data security programs require collaboration among the client, the agency and suppliers. Comprehensive and balanced data security MSA terms should clarify the responsibilities of each party.

Client data security obligations will vary based on the nature of the services arrangement and the agreed upon scope of deliverables. However, normally client obligations include, but are not limited to, the following considerations:

- If the agency services do not require access to and use of PI the contract should state that handling of PI will not form part of the agency's services and that no PI can be sent to the agency without approval, in advance, in writing from the agency.

- The agency should be protected, and should bear no liability, in the event that the client sends PI that the agency has not agreed to accept. When a client shares or transfers PI to an agency without the agency's pre-approval, there should be an MSA provision stating that the agency bears no responsibility for any breach or unauthorized disclosure related to that information.

- The agency should be protected if the client provides the agency with data or PI that was improperly sourced.

- The client is the expert in their business category. Resultantly, the client should be responsible for predominant laws, rules, regulations, industry codes and guidelines, etc. applicable to the client's business, products and services (for global clients this obligation should include EU and Global legal/regulatory requirements).

- The client's obligation should include protection of agency confidential information and agency employee data. The MSA should specify what constitutes agency confidential information.

- Client should indemnify the agency in the event that a breach of the client's systems results in unauthorized disclosure of consumer, agency or agency employee information.

- When the client designates third party suppliers, the client should be responsible for establishing and verifying third party data security requirements.

- Client appointed consultants, auditors and advisors should be obligated to agree in writing to adhere to the confidentiality and data security protections that are stipulated in the agency-client MSA.

- If the client has unique data security challenges or requires separate data security platforms (for example, if the client requires the agency to set up a dedicated server that only contains that client's information), the client should be obligated to pay for the cost of the agency's custom data efforts.

FAQ # 19 ... Group Contracts

Question: *When there are multiple agency servicing entities being covered by a group contract, how is the best way to structure the agency-client data security agreement?*

Considerations:

Where multiple agencies are included in the agency-client MSA, the data security provisions of the contract should be structured to apply only in those circumstances and only for those agencies that handle the most sensitive data.

An agency should provide reasonable data security assurances to appropriately match data security risks. Security protocols need to be constructed to match risks associated with the data transferred/collected.

Any required modifications to the data security terms and procedures can be agreed to and highlighted within the context of a specific SOW agreement, which will likely facilitate better understanding and compliance by agency operations service teams.

FAQ # 20 … Data Destruction

Question: *How should an agency address data destruction and data return requirements of client MSAs?*

Considerations:

It is vital that the definition of data is clear to both client and agency. In most cases, data is defined upfront in the MSA, however if it is not, a clear definition of data, including agreement on what data should be destroyed and/or returned after the completion of engagement should be documented in writing.

If there is ambiguity in the definition of data, e.g. “all data/ information shared by the client with the agency during the course of engagement,” covered as part of the definition, then there needs to be a discussion with the client about what data is important to them from a protection standpoint that they would like to be destroyed, both in physical and electronic format rather than “all the information,” since destruction of “all information” is impractical and cannot be feasibly accomplished. For example, the information exchanged on emails, which resides on the agency’s mail servers, and is possibly backed up on the agency-owned backup tapes, which follow the agency’s policies, rotation and retention schedules, such backups are not taken exclusively for client information therefore it is not possible to segregate the client information and destroy only client information when the client demands or upon the conclusion of client engagement. There also may be other data destruction scenarios where the secure destruction requirement cannot be fulfilled by the agency, for example, agency hosting of client information on a third party cloud.

Once the definition of data is sorted out and both parties agree on what needs to be destroyed, the understanding should be explicitly documented in the MSA agreement.

If a client requests the return of client data after the conclusion of an engagement, the parties should follow the same process that is applicable to data destruction, e.g., comprehensive pragmatic discussion and mutual agreement associated with data return requirements.

FAQ # 21 … Additional Information on Data Security and Additional Data Security Considerations

Question: *Where can I access additional information about data security?*

Considerations:

As should be clear by now, the area of data security is complex and rapidly evolving in the Unites States and in jurisdictions around the world. The following listings of certain source materials is intended to be helpful, but should not be taken as definitive or comprehensive. Data security is an area where consultation with a qualified attorney should be undertaken in order to ensure that current legal requirements are understood.

State by State Data Security Breach Notification Matrix:

The following attorney firms provide a state by state Data Security Breach Notification matrix –these are searchable databases that provide information on each of the states with security breach notification laws.

Note: These matrixes are for informational purposes only. They are intended as an aid in understanding each state's sometimes unique security breach notification requirements.

Perkins Coie (Attorneys At Law):
https://www.perkinscoie.com/en/news-insights/security-breach-notification-chart.html

Mintz Levin (Attorneys At Law):
https://www.mintz.com/newsletter/2007/PrivSec-DataBreachLaws-02-07/state_data_breach_matrix.pdf

ISO: International Standards Organization
ISO develops and publishes international standards for many industries/practices including publishing the ISO 27000 family of standards which helps organizations keep information assets secure.
http://www.iso.org/iso/home.htm

NIST: National Institute of Standards and Technology

NIST is a non-regulatory federal agency within the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards and technology in ways that enhance economic security and improve quality of life.
http://www.nist.gov/

NIST has issued the publication: *Framework for Improving Critical Infrastructure Cybersecurity* which is available for download from the NIST website at:
http://www.nist.gov/cyberframework/index.cfm

FTC: Federal Trade Commission

The FTC has resources to help companies think through how data security principles apply to business: http://www.ftc.gov

In addition, the FTC has published the guide: *Start With Security: A Guide for Business* which provides 10 practical lessons businesses can learn from the FTC's 50+ data security settlements. The guide is available for download from the FTC website at:
https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business

HIPPA: Health Insurance Portability + Accountability Act
HIPPA Audit Program Protocol

HIPPA addresses privacy, security and breach notification in regard to personal health information (PHI). The US Department of Health and Human Services (www.hhs.gov) which oversees enforcement of HIPPA regulations is in the process of updating the protocol –which can be monitored at:
http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html

PI/PII Information:

New York State: Personal Privacy Protection Law:
https://www.dos.ny.gov/coog/pppl.html#s92

New York State: Glossary: Definition of Terms
Definitions of PI and PPSI under New York State law
https://www.its.ny.gov/glossary

California:
http://leginfo.legislature.ca.gov/faces/codes.xhtml

Insurance:

The 4A's Benefits Group is available to assist member agencies with information about insurance policies that may be available including Professional Liability policy elements that pertain to data security that include optional coverages such as Cyber/Technology Services E&O, Security and Privacy Liability, and Crisis Management and Computer Systems Extortion (first party coverage) endorsements that agencies may want to explore**.**

4A's members seeking additional information can access the 4A's Benefits Group website at www.aaaabenefits.com and contact either Adam Prus: aprus@aaaabenefits.com|
or Elyse Congdon: econgdon@aaaabenefits.com of the 4A's Benefits Group.