ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Data Security and Vendor Agreements: The Chain is Only as Strong as the Weakest Link

Technology, Privacy, and eCommerce

CHEAT SHEET

- ***Know your vendors.*** Prior to entering into an agreement with a vendor that will have access to confidential information, a company should take steps to ensure that the vendor is able to protect their data.
- ***Standardize data security.*** If a company is serious about protecting data, it may be worth developing a set of security standards that a vendor must implement and maintain.
- ***Liability cannot be outsourced.*** While an organization can outsource services, liability in the event of a data breach can usually be traced to the source.
- ***Show your work.*** Even in the event of a data breach or regulatory interest, demonstrating due diligence in selecting vendors is valuable.

In the wake of the growing number of data breaches, consumers and regulators alike increasingly recognize that compromised organizations may be the victims of sophisticated criminal attacks, and are not always at fault. The list of potential attackers includes state actors such as Russia, North Korea and China, organized criminal elements, and even lone individuals with a political motivation. Regardless of the source, all of these cyber criminals bring resources that potentially outstrip those of the average business. While organizations are far from being excused for such incidents, focus has started to shift slowly from the breaches themselves to what businesses are doing to prevent them in the first place.

According to a Ponemon Institute study, approximately 40 percent of breaches are caused by third parties, such as vendors or business partners. And such breaches by third parties drive response costs up: According to another Ponemon study, the involvement of third parties in the cause of a data breach at 36 percent of the companies surveyed increased the costs associated with the data breach.

A well-developed vendor management program can add a critical component to the organization's overall risk management program, and help reduce the danger created by engaging a vendor that is not equipped to guard confidential information. Reasonable steps to protect data should include a comprehensive vendor management program that incorporates thorough data security assessments in advance of contract negotiations.

Some state and federal regulatory agencies provide detailed guidance for companies that wish to outsource functions that will afford a vendor access to confidential information. Massachusetts, for example, requires companies to implement written information security programs (WISP). Under these programs, companies must select and retain third party service providers that (a) are capable of maintaining appropriate security measures for personal information, and (b) take steps to protect data in their care. Similarly, certain healthcare-related entities (These are known as "Covered Entities." 45 C.F.R. § 160-103) that engage vendors to create, receive, maintain or transmit certain health information in electronic form must be sure that these vendors will safeguard such information.

The Federal Financial Institutions Examination Council's (FFIEC) Federal Financial Institution's Outsourcing Technology Handbook provides financial institutions detailed guidance related to vendor management. The FFIEC recommends that financial institutions conduct an assessment of the

service provider's internal control environment, security history and audit coverage, the existence of any past or pending legal actions or regulatory compliance complaints, as well as the scope and nature of insurance coverage. The depth and formality of this due diligence effort may vary according to the risk of the outsourced relationship, the company's familiarity with the vendor and the maturity of the provider selection process.

Evidence that a company has taken reasonable steps to protect data could help with a company's defense if the breach was a result of negligence by the vendor. Such efforts are also likely to make the company a less-attractive target for a regulatory enforcement action. In light of the recent headlines regarding "data insecurity," and various legal and regulatory requirements across multiple sectors of the economy, this article will outline vendor due diligence measures that counsel should evaluate in conjunction with their information technology department (IT) and internal audit department (IA).

Part one: Vendor data security due diligence

Prior to entering into an agreement with a vendor that will have access to confidential information, including the personally identifiable information of employees, customers or others, a company should take steps described herein to ensure that the vendor is in fact able to protect the data. Such due diligence may also help streamline the contracting process, as inherent risks will likely be identified earlier in in the contracting process. It should be noted, however, that the need to conduct due diligence may depend on the nature and volume of the information to be exchanged between the parties.

Preliminary considerations: For which engagements should data security due diligence be conducted?

Resources may limit the amount of due diligence that can be conducted. A company that engages vendors on a regular basis may wish to create an internal governance process that addresses which types of engagements merit data security due diligence. The nature of the engagement, the data to which a vendor will have access, and the volume of such data are all helpful indicators of when to launch a review. Such internal governance process may include representatives from various disciplines inside the company including IT, internal audit and legal.

The nature of the engagement

The nature of the engagement may suggest whether and to what extent due diligence should be undertaken. The following types of engagements may merit consideration, as they often require access and management of a great deal of confidential information, including personally identifiable information:

- Benefits administrators
- Cloud services
- Collection agencies
- Data centers
- Healthcare claims processing services
- Insurance and financial services
- Marketing services
- Mortgage services
- Onboarding services

- Payroll services
- Pension administration
- Platform as a service
- Software
- Software application services
- Software as a service
- Third party administration
- Web hosting services

A single vendor may fall into more than one category above. For example, a payroll service may also host applications that collect and analyze data, thereby functioning as data centers.

What information will the vendor access?

The compromise of some confidential information may create greater liability than other information.

For example, the breach of certain personal information in many states may trigger a notification obligation. Access to certain data by certain foreign nationals may constitute a violation of export laws and regulations. Sharing proprietary business information with third parties may constitute a breach of a confidentiality agreement. The compromise of such data in a vendor's care typically won't relieve a company of liability. Therefore, a review of the type of data to be entrusted with a vendor should factor into whether to conduct data security due diligence.

Personal information and notification obligations

In the event that certain information (i.e., social security numbers and driver's license numbers) is compromised, most states require that the company responsible for caring for the information provide notice to affected individuals, the state attorney general, media outlets and credit reporting agencies. Similarly, when certain health information, defined as "Protected Health Information or PHI" under HIPAA, is compromised, notice must be sent to the US Secretary of Health and Human Services. In cases where personal information is compromised, the law of the state where the individual involved resides governs the notification obligation, not the law of the state where the business is located or incorporated.

A notification obligation may arise when an individual's first name or initial and last name is compromised, along with any of the following:

- Social security number;
- Driver's license number, state identification card number or other government identification number (e.g., passport number, tribal identification number);
- Account number, credit card number or debit card number in combination with any required security code, access code or password that would permit access to an individual's financial account;
- Vital record information in the form of life events kept under government authority (e.g., birth or death certificates);
- Biometric data (e.g., retina, iris image, fingerprints);
- Medical information, including physical or mental health information;
- Health insurance identification number;
- The provision of healthcare to an individual;

- Payment information regarding the provision of healthcare to the individual; or
- Stock or other security certificate or account number; or
- Any other number or code or combination of numbers or codes, such as account number, security code, access code or password, that allows access to, or use of, an individual's medical, financial or credit information.

Other personal information, such as a mailing address, is not typically included in the list that would trigger a notification obligation under applicable law. This area of law is fluid; so always check the law applicable to the engagement to identify the specific data elements. It is important to remember that even if a vendor causes the breach, it is often the company that engaged the vendor that must provide notice and suffer the consequences of any accompanying bad press.

Export-controlled information

Export-control laws are complex, and beyond the scope of this article. Generally, however, these regulations prevent certain foreign nationals from accessing sensitive data and technology. Sharing such data and technology with certain individuals who are not US citizens or lawful permanent residents (collectively, Foreign Nationals), even if they reside in or are currently visiting the United States, may constitute a "deemed export" that is subject to export restrictions. A deemed export may occur if information is shared with a Foreign National who is in the United States performing services, or is outside the United States performing services remotely (including on or through a server located in the United States). These restrictions can be found in regulations issued by several federal agencies, including the US Department of Commerce, the US Department of State and the Department of Energy.

If information and technology will be shared with a vendor in a manner that creates export and deemed export potential, a data security assessment should be considered to determine what controls are in place to prevent access to such data and technology in violation of applicable export-control laws and regulations.

Other confidential information

Additional legal obligations may arise when information is compromised and does not otherwise fit the definition of personal information or information subject to export controls. For example, a confidentiality agreement with another party may be in place to protect designs or business plans that do not contain personal information. Compromise of this information could trigger a breach-of-contract claim. For this reason, consider conducting data security due diligence assessments on vendors who will, for example, host such designs, business plans or other confidential information.

What is the volume?

Consider the volume of data to which a vendor will have access. It makes sense to conduct due diligence on a cloud service provider that will store a database of 100,000 customers' personal information, but it may not make sense to conduct the same level of due diligence on a vendor that will store the same information on only 1,000 customers.

Brand and public relations ramifications of a data breach or compromise

Even if no law or contract applies to protect the data, consider the public relations effect of a breach. The breach of a customer database of shopping preferences is not, for example, a violation of law,

but may prove embarrassing to customers and lead to a loss of revenue for the affected business. An example of loss of consumer confidence in the wake of the Target credit card breach was reflected in a 46 percent drop in the company's fourth quarter earnings after its breach. A wholesale brand collapse can have far-reaching material consequences for the company, and can adversely affect its management for many months, and potentially years, after the breach.

What questions should you ask?

The following are examples of the types of questions to ask a vendor for the purpose of understanding the data security environment and potential gaps. Whether these gaps are significant will depend on the nature of the engagement. The responses, however, will help your company formulate an opinion on whether to proceed with a particular vendor.

Data storage

Where is the data stored? Is the data stored in the United States at a particular data center? Has the vendor conducted due diligence on its hosting vendor? If so, does the data center have the appropriate security controls in place to store the company's data? Can the data center provide sufficient evidence of such controls if they exist? Has that data center experienced a breach in the past five years? If so, what occurred and what did the vendor do in response? Alternatively, if the data center is located outside of the United States, consider whether some data is subject to export restrictions that may be implicated when and if data is sent to that data center.

Subcontractors

Has the security diligence been extended to third-party subcontractors? The vendor may use a separate third party to provide all or part of the service. Subcontractors often provide hosting services, data storage, IT services and other services for vendors. Therefore, it is not unusual for a subcontractor to have access to a vendor's data. The company should understand all of the key players in the "data supply chain," and address their roles in the data security due diligence.

Cyber insurance

What types of cyber insurance does the vendor have in place? New insurance products have emerged that are designed specifically to address first and third party claims related to data, including the costs of responding to a breach. If the vendor under consideration carries such insurance, the vendor will be in a better position to respond in the event of a breach. Does the vendor's policy provide coverage for breach remediation and notification expenses? Management of breach response by counsel? Forensic investigation and credit monitoring services? Does the policy provide coverage for regulatory fines and penalties? Reimbursement for crisis management and public relations services? Does the policy contain exclusions baring coverage for mechanical failure, failure to maintain the computer network or system, failure to maintain risk controls or lack of encryption?

Focusing on these questions before negotiating the vendor agreement can help the parties better understand the options that may be available with respect to liability and indemnification.

Audit reports and certifications

What audit reports are available with respect to the vendor's data security practices? Below are

some examples of audit reports that are increasingly available to a vendor's potential customers:

Service Organization Control Reports (SOC reports), Type I and Type II reports

A Service Organization Controls Report 2 (SOC 2) is intended to demonstrate that the organization's internal controls related to security, availability, processing, integrity, confidentiality and data privacy are operating effectively.

A SOC 2 Type I report focuses on management's description of a service organizations' system, and the suitability of the design of the controls. The SOC 2 Type II report focuses on management's description of a service organization's system and the suitability of the design and operating effectiveness of the controls. The report includes an examination and confirmation of the steps involved, and an evaluation of the operating effectiveness of the controls for a stated period of time.

The distinctions between a Type I report and a Type II report are subtle, but important. When evaluating a Type I report, the focus is on whether management has adequately described the system and adopted suitable controls for security, availability, processing, integrity, confidentiality and data privacy. The Type II report, in contrast, evaluates whether that system operates effectively. What type of report required depends on the nature of the engagement and the data to which the vendor will have access.

SOC reports, which are typically reviewed by IA, are valuable because they are produced by independent third parties (typically auditors) who have verified the controls in place. More and more vendors, particularly those who host or process a large volume of confidential information, produce SOC reports as marketing tools that demonstrate to potential customers the seriousness with which they address data security. The absence of these reports for larger vendors could be a red flag.

Not all vendors will have SOC reports, but may have substitute reports that will suffice to demonstrate a level of data security that a company will not be able to ascertain on its own. These include, but are not limited to, certificates of compliance with Payment Card Industry Data Security Standards (PCIDSS), International Organization for Standards 27001 and 27002 (ISO 27001 and 27001), TRUSTe certifications and Experian Independent Third Party Assessment (EI3PA) certifications.

Offshore resources

Will the vendor use Foreign Nationals? This is only an issue, from a data security perspective, when the vendor will have access to information or technology that is subject to export restrictions. If the vendor will have access to such data, identify whether the Foreign Nationals will have access to it either in the United States, or abroad (including access from abroad to data located on a server in the United States). If they will, an export analysis will be required to determine, based on the nationality of the Foreign Nationals, whether such access will constitute an export (deemed or actual) that (a) is allowed, (b) will require authorization from one or more government agencies, or (c) is prohibited.

Offshore resources also include data centers or other operations to which the data or technology will be sent. This actual export may, depending on the country where such resources are located, require the same export analysis to determine whether sending such data and technology (a) is allowed, (b) requires authorization from one or more government agencies, or (c) is prohibited. Obtaining a SOC report, IS027001 certification or other audit report will help assess such a location.

Data security questionnaire

These questions and others can be standardized in a data security questionnaire for vendors that can be used generally for multiple engagements. If a questionnaire is developed, input from IT and IA will be helpful. Subsequent review and advice from vendors who have completed the questionnaire will help hone the questions over time. As vendors may be unaccustomed to filling out such questionnaires, legal counsel, IT and IA should review it and ask questions, particularly if inaccuracies or discrepancies are spotted.

If, for example, a vendor claims in the questionnaire that it has 10,000 employees, operates in 30 states, but has no subcontractors, that claim should be challenged. It is likely that the company, at minimum, is engaging a subcontractor to provide storage services, IT assistance or other services, and that should be explored further. The information from the questionnaire will allow legal counsel, IT and IA to develop a comprehensive view of the vendor's data security practices, and an understanding of the undertaking.

It is important to understand the limitations of this assessment.

For example, when relying on the responses that a vendor provides or a third party audit report, clarify that the accuracy of the information has not been independently confirmed, unless, in fact, it was. In addition to improving the quality of the decision to proceed with a vendor, this process will also better enable legal counsel to draft provisions in the applicable agreement that will help fill the gaps in data security mitigation.

Part two: What to include in an agreement

Once the due diligence process concludes and it is time to proceed, consider including the following provisions in the agreement to address data security.

Data security standards

If a company is serious about protecting data, it may be worth developing a set of security standards that a vendor must implement and maintain. Such standards may include:

- Encrypting data at rest
- Encrypting data in transit
- Employee training
- Background checks (including fraud convictions)
- Terminating access immediately upon an employee's departure
- Insurance that responds to data security events
- Service Organization Control Reports (such as a SOC 2, Type II)
- Annual penetration tests
- Continuous security monitoring
- Business continuity plan
- Disaster recovery plan
- Data security policies that include discipline for failure to abide by such policies

Audit rights and reports

If the vendors (or its subcontractors) maintain the audit reports and certifications described above, ensure receipt of a copy of such reports on an annual basis for the term of the agreement. Including a

right to audit, particularly in the event that data is compromised, is also helpful.

Indemnification and limits of liability

As a company may be liable for a compromise to data that occurs while in the vendor's care, perhaps the most important part of the agreement will be the indemnification provision. Reasonably expect that the vendor will provide full indemnification in the event that the vendor failed to maintain the data security standards articulated in the contract or if data was compromised.

It is important to note that a compromise to data security alone (i.e., unauthorized access alone), without evidence that clearly indicates an actual breach (i.e., evidence of data leaving the system or unauthorized use of the data), may still trigger damages.

If, for example, a vendor fails to maintain the required encryption measures, and notifies the company of an anomaly in its system affecting its customers' or employees' personal data, the company will have to determine whether a breach occurred as defined by applicable law. Hundreds of thousands of dollars may be spent in actually determining that a breach did not, in fact, occur. If the vendor's liability is triggered only in the event of an actual breach, a company may not be able to recover the cost of this investigation. However, if encryption was a required data security measure, and a failure to maintain such data security standards affords a remedy and indemnification protection, such costs may be recovered.

The key takeaway is to contemplate all possible scenarios regarding incidents affecting data security so that the indemnification provision applies broadly in the event of data security incident.

Carve outs for limits of liability for damages that result from the vendor's breach of its obligations of confidentiality and data security.

If a limit of liability must be included, it is helpful to carve out of that limit the vendor's indemnification obligations, and damages that arise from the vendor's breach of its obligations of confidentiality and data security. These are within the vendor's control, and it is reasonable to require that the vendor take responsibility for them in the agreement. For example:

> Except for vendor's indemnification obligations and damages that arise from vendor's breach of its obligations of confidentiality and data security, vendor's liability to customer shall be limited to $5 million.

If an agreement on that point cannot be reached, consider a separate, higher limit of liability for indemnification and such damages. For example:

> Except for vendor's indemnification obligations and damages that arise from vendor's breach of its obligations of confidentiality and data security, vendor's liability to customer shall be limited to $5 million. Vendor's liability to customer for vendor's indemnification obligations shall be limited to a separate per-event limit of liability of $10 million. Vendor's liability to customer damages that arise from vendor's breach of its obligations of confidentiality and data security, shall be subject to a separate, per-event limit of liability of $10 million.

Prohibition on the use of subcontractors

If time and money has been spent conducting due diligence on the vendor and its subcontractors, a company does not want to learn after the contract has been executed that the vendor is moving its data center to another provider that has not been investigated. For this reason, it is helpful to include a prohibition on the use of subcontractors absent advanced, written consent. If a vendor requests a subcontract once the agreement has been executed, the company has the leverage to insist on a positive outcome to a due diligence review as a condition of any consent.

Export restrictions

If access to export-controlled information or technology will be granted to a vendor, include an export clause in the agreement. Such clause may prohibit absent the company's advanced consent, (a) the use of Foreign Nationals with respect to certain aspects of the services, both inside and outside the United States, or (b) the export of the company's data outside the United States (including storage in an offshore data center). If a vendor approaches after the agreement's execution with a request to use Foreign Nationals or to send data offshore, this provision will provide the leverage needed to conduct an export analysis.

Business associate agreements under HIPPA

Companies that outsource certain healthcare functions subject to regulation under HIPPA, and the vendors to whom they outsource these functions, are required to enter into a business associate agreement (BAA). The BAA requires the vendor to use appropriate physical, administrative and technical safeguards to protect certain health information (PHI), and prevent its use or disclosure other than as provided for by the agreement. HIPAA requirements are detailed compared to other data-protection laws.

For example, PHI stored, maintained, transmitted or retained on portable devices (which include laptops, CDs, DVDs, PDAs and thumb drives) for or on behalf of a company must be rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of certain technology or methodology.

Vendors who are parties to a BAA are also required to notify the company of any (a) security incident, (b) use, access or disclosure of PHI that is inconsistent with the terms of the BAA; or (c) breach or suspected breach of its security related to areas, locations, systems, documents or electronic systems that contain unsecured PHI. The regulations do not, however, address the allocation of costs associated with compromised data, or require a vendor to indemnify the company for which it is performing the outsourced function in the event of a breach. Therefore, you must address the related risk allocation in your vendor agreement (or the BAA).

Conclusion

Many organizations assume that using a vendor to undertake services will relieve them of responsibility for certain liability associated with a service such as processing a payment or paycheck, reviewing a medical claim or hosting data subject to export restrictions. Typically, this assumption is false. Companies may outsource the responsibility for a component of their operations, but they rarely outsource the risk and liability. This is increasingly true with respect to the protection of data, and personally identifiable information in particular. For this reason, companies must take steps to protect themselves when outsourcing a function that will afford a vendor access to sensitive data.

Where practical, given resources and the relative risk, companies should consider implementing a vendor management program to evaluate those whom they plan to entrust with sensitive data, and help ensure that sufficient controls exist to protect it. Counsel can play a role by advising on the legal risks associated with particular engagements and types of data, and by negotiating provisions designed to protect data and the consequences of its compromise. By taking such measures, the organization can better position itself to safeguard data in a vendor's care, and demonstrate appropriate diligence in selecting vendors in the event that its customers or regulators challenge its data-security practices.

Further Reading

2013 Cost of Data Breach Study: United States, Ponemon. Institute, May 2013, p. 8.

2015 Cost of Data Breach Study: Global Analysis, Ponemon Institute, May 2015, p. 13.

201 CMR § 17.04. Specifically, this provision mandates that such information security program include a requirement to oversee service providers, by: (1)Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such personal information consistent with 201 CMR 17.00 and any applicable federal regulations; and (2) Requiring such third-party service providers by contract to implement and maintain such appropriate security measures for personal information…. Id.
The regulation continues to describe what might constitute "appropriate security measures" as: 1) Designating one or more employees to maintain the comprehensive information security program; 2) Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:

- ongoing employee (including temporary and contract employee) training;
- employee compliance with policies and procedures; and
- means for detecting and preventing security system failures.

3) Developing security policies for employees relating to the storage, access and transportation of records containing personal information outside of business premises. 4) Imposing disciplinary measures for violations of the comprehensive information security program rules. 5) Preventing terminated employees from accessing records containing personal information. 6) Reasonable restrictions upon physical access to records containing personal information, and storage of such records and data in locked facilities, storage areas or containers. 7) Regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; and upgrading information safeguards as necessary to limit risks. 8) Reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information. 9) Documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

45 C.F.R. § 164-308; Pub. L. No. 104-191, and its implementing regulations at 45 C.F.R. Parts 160, 162, and 164; Pub. L. No. 111-5.

The Council is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB), and to make recommendations to promote uniformity in the supervision of financial institutions. http://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services/introduction.aspx.

FFIEC's Outsourcing Technology Handbook p. 11.

45 C.F.R. § 164-501.

45 C.F.R. § 164-408. See also 45 C.F.R. § 164-404 ("Notice to Individuals") and 45 C.F.R. §164-406 ("Notice to Media").

15 C.F.R. Parts 300-799.

22 CFR Parts 120-130.

10 C.F.R. Part 810.

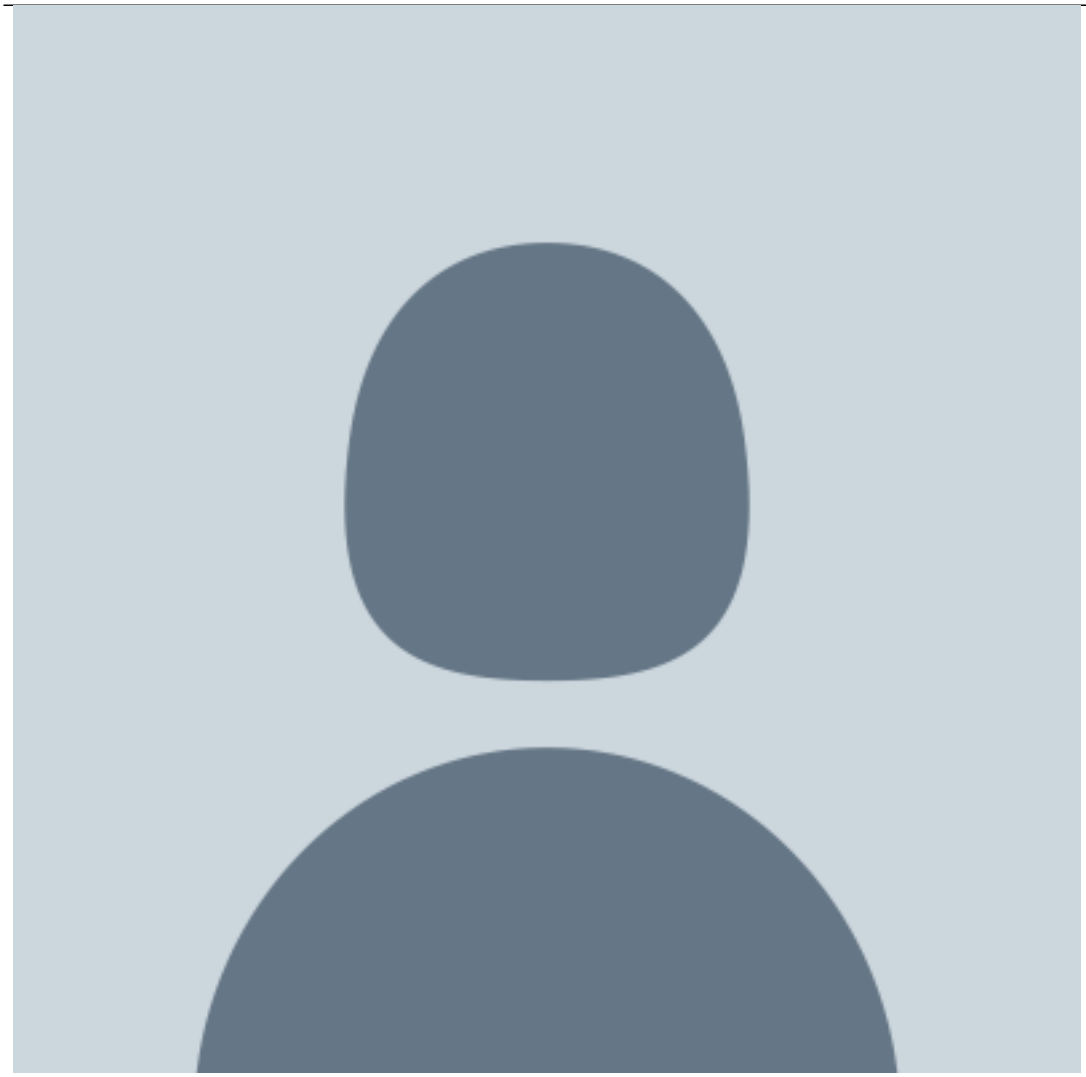
Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, and its implementing regulations at 45 C.F.R. Parts 160, 162, and 164, as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act of the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5.

45 C.F.R. Part 160.103.

45 C.F.R. Part 164.504.

45 C.F.R. Section 164.402.

Dana Atchison

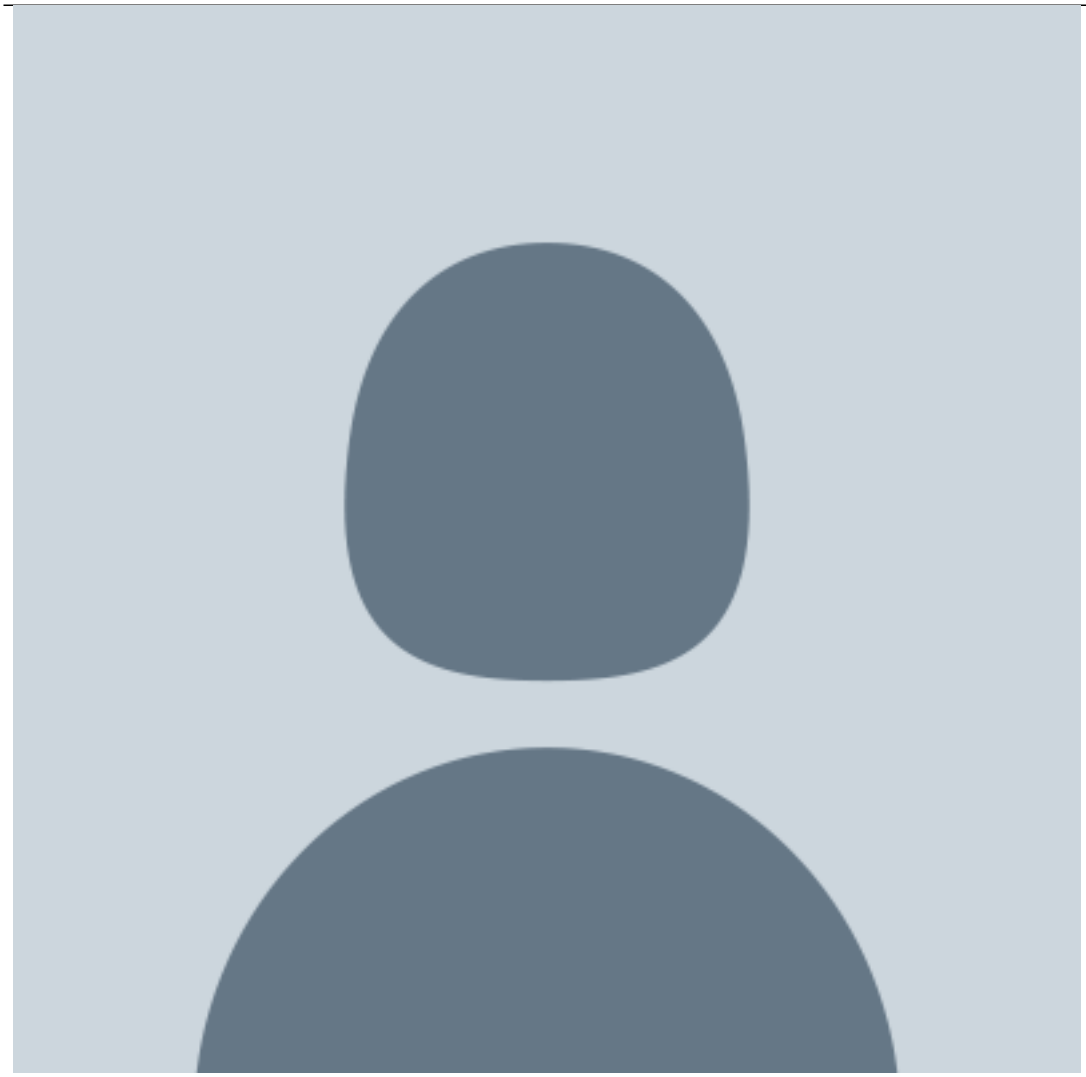


Assistant GC

Entergy Services, Inc

Her practice focuses on transactions, privacy and data security, and IP matters. She also maintains CIPM and CIPP certification through the International Association of Privacy Professionals. Atchison is admitted to practice law in Louisiana, Texas and Colorado. She has a BA from Lake Forest College, a CSS and an ALM from Harvard University, and a JD and Certificate in Arbitration from Tulane Law School.

David F. Katz



Partner

Nelson Mullins

David F. Katz leads the privacy and information security practice at Nelson Mullins. A partner in the firm’s Atlanta office, Katz counsels clients on the development, management and oversight of privacy and compliance programs.