Microsoft

Think Cloud Compliance

# The Use of Cloud Services by U.S. Lawyers and Law Firms: Myth vs. Fact

Firms everywhere are moving their IT systems to the cloud to take advantage of the many efficiency, productivity, and innovation benefits that cloud services provide. Lawyers practicing in the United States, however, have asked whether the use of cloud services is consistent with applicable bar rules and other professional standards, including obligations to protect client confidentiality and attorney-client privilege; maintain data privacy and security; and protect data against third-party access.

Microsoft's cloud services can help lawyers meet or exceed these standards and, in many cases, offer stronger protections than most law firms achieve today through on-premises IT systems.[1] With Microsoft cloud services, customers retain complete ownership over and access to their data and receive the benefit of industry-leading technologies and practices to protect the confidentiality of their client information, including against security breaches.

***Myth #1: Several state bar associations have cautioned that storing client information in the cloud could destroy attorney-client privilege.***

**Fact:** Not true. All state bar associations that have considered the issue have held that lawyers *may* use cloud-based services to create, transfer, and store client-related information so long as they take reasonable steps to ensure that such information remains secure and protected.[2] Adhering to this standard of reasonable care requires lawyers to select a cloud services vendor that offers robust privacy and data security tools and practices, and that lets lawyers strictly control access to data.[3] Microsoft's enterprise cloud services offer a wealth of features to ensure that attorneys can satisfy

---

[1] This article is provided for informational purposes only and not for the purpose of providing legal advice.

[2] *See Cloud Ethics Opinions Around the U.S.*, AMERICAN BAR ASSOCIATION (June 13, 2016), at https://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html; *see also* Dennis Garcia, *Perspective: The Legal Ethics of Using the Cloud*, BLOOMBERG LAW (February 18, 2016) https://bol.bna.com/perspective-the-legal-ethics-of-using-the-cloud/.

[3] *See, e.g.*, Virginia State Bar Association, Legal Ethics Opinion 1872, (holding that lawyers must have a reasonable expectation that a vendor will keep client data confidential and inaccessible by others); Pennsylvania Bar Association, Formal Opinion 2011-200, (holding that lawyers select vendors that have reasonable safeguards to protect data from breach, data loss, and other risk); State Bar of California Standing Committee on Professional Responsibility and Conduct, Formal Opinion No. 2010-179 (holding that lawyer ownership and access to data must not be hindered).

their obligations while taking advantage of the significant benefits that cloud solutions offer. Our commitment to a trusted cloud is built on four principles:

- Security. One of the most critical elements to protecting attorney-client privilege is making sure that appropriate security measures are in place. Microsoft follows a company-wide development process that embeds security into the entire software lifecycle, from planning through deployment, and builds security into all of its cloud services from the ground up. Microsoft also has implemented industry-leading security management and threat mitigation practices and uses state-of-the-art physical security protections at its datacenters (the responses that follow provide further details). Further, Microsoft's Digital Crimes Unit combines big data analytics, cutting-edge forensics and novel legal strategies to fight global malware and reduce digital risk, and the learnings from this work is incorporated in developing cloud solutions and designing data center security features.

- Privacy & Control. Another key element of the reasonable care standard is safeguarding the privacy of client information and ensuring that customers retain control of their data. Microsoft has pioneered the development of robust online solutions to protect data privacy. Our approach to privacy is grounded in our commitment to organizations' ownership of and control over their data. Customers can access their data at any time and for any reason, without assistance from Microsoft, and they have control over where it is stored, who can access it, and when it is deleted. Unlike some cloud service providers, Microsoft does not use customer data for advertising or other commercial purposes. Microsoft's adoption of the world's first international code of practice for cloud privacy (ISO/IEC 27018) is just one example of our commitment to privacy.

- Transparency. Microsoft understands that legal-sector customers need visibility into where their data is stored, who can access it, and under what circumstances. Microsoft's Online Services Terms and Online Services Privacy Statement describe in detail our policies and practices governing the location and use of customer data. Microsoft also provides customers with access to numerous security audit reports and certifications for its services, so they can independently verify that Microsoft meets robust security standards and practices.

- Compliance. Legal-sector customers can take further comfort that entrusting their data with Microsoft's cloud services will satisfy their reasonable care obligations from the broad set of leading security standards that Microsoft's cloud services meet. For example, Microsoft's enterprise cloud services, including Microsoft Azure Core Services, Microsoft Dynamics 365 Core Services, Microsoft Intune Online Services, and Office 365 Services all comply with ISO 27001 and HIPAA, and most of these services comply with SSAE 16 SOC 1 Type II and SOC 2 Type II.[4] Rigorous third-party audits verify Microsoft's adherence to these security controls, and customers

[4] Microsoft's Online Services Terms include a table in the "Online Services Information Security Policy" section that lists cloud services and related key security standards and frameworks and a commitment to comply with such standards unless they are no longer used in the industry and are replaced with a successor.

have a contractual right to verify Microsoft's implementation of these controls by reviewing audit results.[5]

Customers can learn more about Microsoft's commitment to these four principles at the Microsoft Trust Center.[6] Given Microsoft's industry-leading security technologies and practices and our commitment to privacy and control, transparency and compliance, using Microsoft's cloud services could make it easier for lawyers to protect attorney-client privilege than storing data in an on-premises IT system.

***Myth #2: My State's bar rules require lawyers to take reasonable steps to protect the confidentiality of client information, including against security breaches. Storing client information in the cloud could make it less secure.***

**Fact:** Not true. There is a growing consensus that cloud services may offer *stronger* security for client information than on-premises IT systems.[7] Your job as an attorney is providing great legal services to clients; Microsoft's job is providing secure cloud services to the most demanding enterprise customers. Microsoft has invested billions of dollars to make our cloud services more resilient to attack by adopting robust security at the physical, network, host, application, and data layers:

- Data and operational security. Microsoft uses an "assume breach" stance as a security strategy, and our global security incident-response team works around the clock to mitigate the effects of any attacks against Microsoft's cloud services. These practices are backed by centers of excellence that fight digital crime, respond to security incidents and vulnerabilities, and combat malware.

- Encryption. Strong encryption is essential to protecting the confidentiality of client information—both for data in transit and data at rest. For data in transit, Microsoft's enterprise cloud services use industry-standard encrypted transport protocols between user devices and Microsoft datacenters, and within Microsoft's datacenters themselves. In addition, law firms can use the industry-standard IPsec protocol to encrypt traffic between the firm's corporate VPN gateway and Microsoft's cloud services, as well as among the virtual machines located on the firm's virtual network. For data at rest, Microsoft Azure offers law firms the flexibility to choose from numerous encryption options, such as support for AES-256.

- Identity and access management. Another key element to protecting the confidentiality of client information is the ability to control who accesses it. Azure Active Directory is a comprehensive identity and access management solution that helps secure access to both information and applications. It combines core directory services, advanced identity governance and security, and

[5] Microsoft's Online Services Terms provide that "Microsoft will provide Customer with each Microsoft Audit Report so that Customer can verify Microsoft's compliance with the security obligations under the" Data Processing Terms (which are included within the Online Services Terms).

[6] *See* https://www.microsoft.com/en-us/trustcenter

[7] *See* Daniel Solove, *Attorney Confidentiality, Cybersecurity, and the Cloud*, TEACHPRIVACY (June 6, 2016), https://www.teachprivacy.com/attorney-confidentiality-cybersecurity-and-the-cloud/.

makes it easier for law firm IT departments to build policy-based identity management into the firm's applications.

- Security Development Lifecycle. Lawyers using Microsoft's cloud services have the confidence of knowing that security is built into our services from the ground up. Our Security Development Lifecycle follows proven security practices consisting of multiple phases in which core software assurance activities are defined and tested.

In addition, Microsoft contractually commits to implementing, maintaining, and following appropriate technical and organizational measures designed to protect customer data against accidental, unauthorized or unlawful access, disclosure, alteration, loss, or destruction.[8] Furthermore, if Microsoft becomes aware of any unlawful or unauthorized access to equipment or facilities resulting in loss, disclosure, or alteration of customer data, Microsoft contractually commits to notify the customer; investigate the incident and provide the customer with detailed information; and take reasonable steps to mitigate the effects and minimize any resulting damage.[9]

***Myth #3: In order to comply with professional rules, my firm places a premium on data privacy. But if I store documents in the cloud, client-related information will not remain private.***

**Fact:** Not true. Microsoft's robust privacy policies and practices provide law firms using Microsoft's cloud services confidence that client information will remain private in Microsoft's Cloud. We adhere to stringent privacy standards and back them up with contractual commitments. For instance, Microsoft's enterprise cloud services use customer data *only* to provide the requested services and for purposes compatible with those services, such as troubleshooting and protecting against malware.[10] Unlike some cloud services providers, Microsoft does not use customer data for advertising.[11]

The cornerstone of Microsoft's privacy program is the Microsoft Privacy Standard, which sets forth the general privacy rules for developing and deploying Microsoft cloud services. Privacy requirements are also defined and integrated into the Microsoft Security Development Lifecycle (described above).

---

[8] Microsoft's Online Services Terms provide that "Microsoft has implemented and will maintain and follow appropriate technical and organizational measures intended to protect Customer Data against accidental, unauthorized or unlawful access, disclosure, alteration, loss, or destruction."

[9] Microsoft's Online Services Terms provide that "[i]f Microsoft becomes aware of any unlawful access to any Customer Data stored on Microsoft's equipment or in Microsoft's facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of Customer Data (each a "Security Incident"), Microsoft will promptly (1) notify Customer of the Security Incident; (2) investigate the Security Incident and provide Customer with detailed information about the Security Incident; and (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident."

[10] Microsoft's Online Services Terms provide that "Customer Data will be used only to provide Customer the Online Services including purposes compatible with providing those services."

[11] Microsoft's Online Services Terms provide that "Microsoft will not use Customer Data or derive information from it for any advertising or similar commercial purposes."

Microsoft was also the first major cloud provider to adopt the international code of practice for cloud privacy, ISO/IEC 27018. The controls incorporated into this code include a prohibition on using customer data for advertising or marketing purposes without the customer's express consent.

Microsoft also uses strict controls to govern access to customer data, assigns the lowest level of privilege to Microsoft personnel required to complete key tasks, and revokes access by Microsoft personnel when it is no longer needed. Tools such as multi-factor authentication help limit data access to authorized personnel only. Microsoft also employs accredited firms to perform sample audits to attest that access is for only legitimate business purposes.

***Myth #4: My State's bar rules require lawyers to maintain client ownership of and access to client data. A cloud service provider could assert ownership over those documents or place limits on my access.***

**Fact:** Not true for Microsoft customers. Our customers own all data they place in Microsoft's cloud services — including text, sound, video, or image files and software — and can access their data at any time and for any reason without assistance from Microsoft. In fact, Microsoft includes a contractual commitment providing that our customers retain all right, title, and interest in and to customer data — and that Microsoft acquires no rights in customer data, other than the rights customers grant to Microsoft to provide the cloud services.[12] Customers can also remove their data from Microsoft's cloud services (see response that follows).

***Myth #5: Our firm requires all lawyers to return client documents to the client on request. If we store documents in the cloud, the provider could refuse to return those documents, or that data could exist in the cloud indefinitely.***

**Fact:** Not true for Microsoft customers. Lawyers using Microsoft's enterprise cloud services can have confidence that they can retrieve any documents they store with these services at any time. Enterprise customers retain control over their data in the Microsoft Cloud. If a customer leaves the service, Microsoft provides tools that make it easy to transfer the data to a new service. Microsoft also follows strict standards and specific procedures for removing customer data from its cloud services systems and overwriting storage resources before reuse.

Further, Microsoft contractually commits to specific processes when a customer leaves a cloud service. Specifically, if a customer decides to leave our cloud services, Microsoft will store the data in a limited-function account for 90 days to give a customer time to extract the data. After the 90-day period, Microsoft will disable the account and delete customer data, including any cached or backup copies.[13]

---

[12] Microsoft's Online Services Terms provide that, "[a]s between the parties, Customer retains all right, title and interest in and to Customer Data. Microsoft acquires no rights in Customer Data, other than the rights Customer grants to Microsoft to provide the Online Services to Customer." This provision applies to all of Microsoft's enterprise online services.

[13] Microsoft's Online Services Terms provide that, "[a]t all times during the term of Customer's subscription, Customer will have the ability to access and extract Customer Data stored in each Online Service. Except for free trials, Microsoft will retain Customer Data stored in the Online Service in a limited function account for 90 days after expiration or termination

***Myth #6: If I store client data in the cloud, governments will have ready access to my data and I will never know it.***

**Fact:** Not true for Microsoft customers. Microsoft commits that it will not provide any third party, including government entities with direct, indirect, blanket or unfettered access to customer data. Because Microsoft believes that customers should control their own data, Microsoft will not disclose customer data hosted in any of its enterprise cloud services to a government or to law enforcement, except as directed by the customer or where required by law.

Microsoft is committed to transparency and limiting what it discloses when governments or law enforcement make a lawful request for customer data. Microsoft contractually commits that when it receives a request for customer data, Microsoft will always attempt to redirect the requesting party to obtain the data directly from the customer. Microsoft will also promptly notify the customer of any third-party request and provide a copy of the request, unless legally prohibited from doing so. For valid requests that Microsoft is not able to redirect to the client, Microsoft will disclose information only when legally compelled to do so and will always make sure to provide only the data specified in the legal order.[14]

of Customer's subscription so that Customer may extract the data. After the 90-day retention period ends, Microsoft will disable Customer's account and delete the Customer Data."

[14] Microsoft's Online Services Terms provide that "Microsoft will not disclose Customer Data to law enforcement unless required by law. If law enforcement contacts Microsoft with a demand for Customer Data, Microsoft will attempt to redirect the law enforcement agency to request that data directly from Customer. If compelled to disclose Customer Data to law enforcement, Microsoft will promptly notify Customer and provide a copy of the demand unless legally prohibited from doing so." These contractual commitments apply to all of Microsoft's enterprise online services.