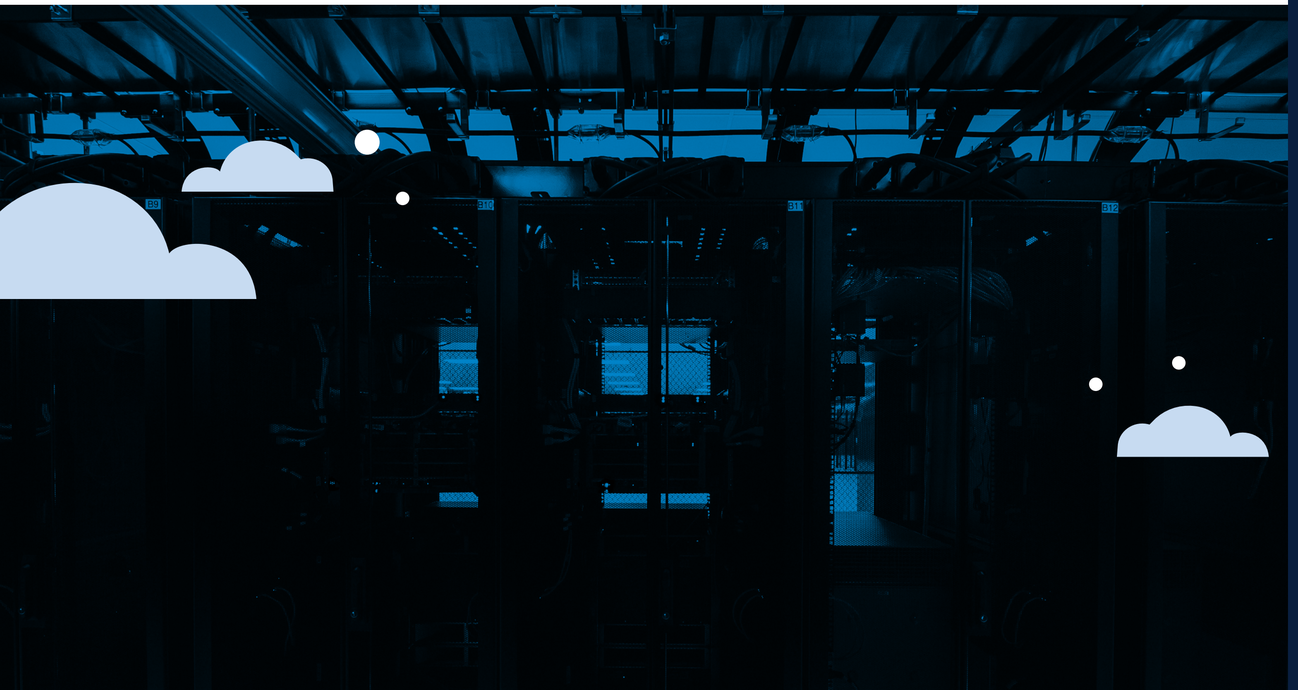
COMPLIANCE IN THE CLOUD

WHAT TO CONSIDER. WHAT TO DO.

US SIGNAL®

TABLE OF CONTENTS



PARTNERING FOR COMPLIANCE

Regulatory compliance, on its own, can be complex and confusing. Add in cloud services, and the complexity multiplies.

However, meeting compliance requirements isn't something that can be ignored or continually delayed. Failure to comply can result in large fines, as well as lost business, damage to the organization's reputation and other business-wrecking effects.

One of the ways to help ease the burden of meeting various compliance requirements or industry standards in the cloud is to work with a cloud services provider (CSP) that is compliant with that particular requirement or standard. CSPs that are PCI DSS certified or HIPAA compliant are good choices.

PCI DSS and HIPAA both entail rigorous security requirements. A CSP that can meet them maintains a well-governed, high-quality IT infrastructure and has strong security processes and mechanisms in place. As such, CSPs can help their customers meet many of their own compliance requirements by leveraging the CSPs' audited and compliant infrastructure.

One of the ways to help ease the burden of meeting PCI DSS and/or HIPAA compliance requirements in the cloud is to work with a cloud services provider (CSP) that is PCI- and/or HIPAA-compliant.

THE PCI-COMPLIANT CSP

With so many organizations handling credit card data and subject to PCI requirements, there's a big market for CSPs to target with PCI-compliant IT services.

Not surprisingly, many CSPs tout being "PCI compliant" or "PCI certified" to get their share of the market. But just because a CSP says it's PCI compliant doesn't make it so. It's essential to verify that any CSP your organization is considering has been certified under PCI DSS as a service provider and its cloud infrastructure operations are PCI DSS compliant.

A CSP that has undergone the required independent PCI audit should be willing to provide its report on compliance (ROC), which attests that all processes and components under its control are PCI compliant.

In addition, it's recommended that the CSP be on the "Approved Service Providers" list for major card brands including VISA. (The lists of approved service providers can be found on each bank card's web site.)

Keep in mind that the PCI standard is frequently updated. The latest version of PCI DSS — and the first major update to the security standard since 2018 — was released in March 2022. If your organization is subject to the PCI standard and are working with a CSP to help meet the requirements, make sure it is up-to-date with the specifics of the latest version.

US SIGNAL®

THE HIPAA-COMPLIANT CSP

For organizations subject to HIPAA, the guidelines for identifying HIPAA-compliant CSPs and working with them are clear. The 2013 final Omnibus rule clarified that CSPs are considered “business associates” of covered entities (which is your organization if it’s subject to HIPAA requirements.) The federal document states:

“A data storage company that has access to protected health information (whether digital or hard copy) qualifies as a business associate, even if the entity does not view the information or only does so on a random or infrequent basis. Thus, document storage companies maintaining protected health information on behalf of covered entities are considered business associates, regardless of whether they actually view the information they hold. To help clarify this point, we have modified the definition of “business associate” to generally provide that a business associate includes a person who “creates, receives, maintains, or transmits” (emphasis added) protected health information on behalf of a covered entity.”

What this means is that CSPs must meet HIPAA requirements. To help ensure they do, require a prospective CSP to sign a business associate agreement (BAA). The BAA outlines the CSP’s responsibilities and those of your organization, as well as the roles of both in protecting PHI from contract start to termination.

Check for a clause specifically related to the breach notification timeline. You’ll also want to review a copy of the CSP’s HIPAA Report on Compliance (HROC), which outlines the scope of the CSP’s independently conducted HIPAA audit.

WHO DOES WHAT

Once you've determined that the CSP you wish to work with is PCI- and/or HIPAA-compliant, you need to understand your organization's compliance requirements and who will be responsible for them.

Some of the requirements can be met by your company. Others can be met by the CSP acting on your organization's behalf. Ultimately, it is always the responsibility of your organization to make sure that it fully meets the compliance requirements, even if some of those requirements are handled by the CSP.

Clear communication and a complete understanding of the division of responsibilities between your organization and any CSP or other IT infrastructure provider you work with is essential.

You must work closely with your CSP to define what is entailed for each responsibility; discuss the arrangements to ensure complete understanding; and then agree to the division of responsibilities.

It is also crucial to understand how the responsibilities for technical security controls map to specific compliance requirements and who will be in charge of making sure the responsibilities are met. The terms and conditions outlined in the CSP's service level agreement (SLA) should align with your expectations.

WHERE'S YOUR DATA

There are several other issues to consider. Among them is the requirement that comes up during audits regarding where your data resides and what protective measures are in place. With cloud services, that's sometimes easier said than done.

CSPs may employ a network of data centers that work together to provide high availability and security of your data. Data may be moved to different data centers across large geographic spans based on service levels, resource demand, cost, latency, disaster recovery/business continuity (DR/BC) needs, and other factors. For security reasons, CSPs may be reluctant to divulge the location of their data centers or where data is specifically located at any one time.

Whether your organization is US-based or just doing business in the US, many regulations require that your CSP's servers be in the US. Even if they don't, a server in a foreign country may be subject to the laws of that country's government, which can present privacy issues. (See the information on GDPR.)

Note: Although neither PCI or HIPAA specifically stipulate that data must be stored within U.S. borders, they do require proof that controls are in place to protect the data.

Bottom line: Make sure you know where your data resides and what controls the CSP has in place to protect it. Require documentation showing where the CSP's servers are located. The specifics should be spelled out in your service level agreement (SLA) with the CSP as well.

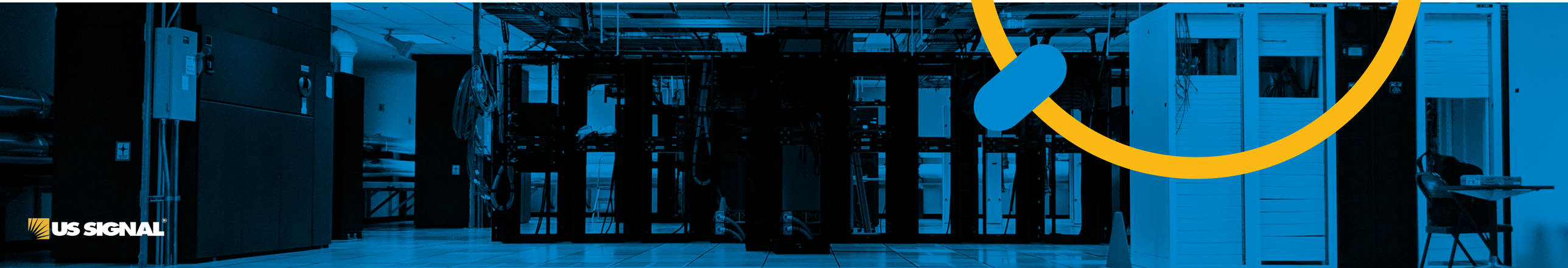
US SIGNAL®

WHO CAN ACCESS YOUR DATA

Most compliance requirements and standards ensure that system and data access is controlled and secure. During an audit, your organization may be required to document every user's access level, and specify how those access controls are enforced.

If your data can be accessed in the cloud, the CSP must also be able to specify all user access. Most reputable CSPs have programs in place to document access levels.

Make sure any CSP you work with is willing and able to prove that it can provide documentation showing which users have access to a system and when, and what data each user can access. This information is important to comply with many different regulations, including the Gramm-Leach-Bliley Act (GLBA), which requires financial institutions to protect the security and confidentiality of customers' non-public personal information.

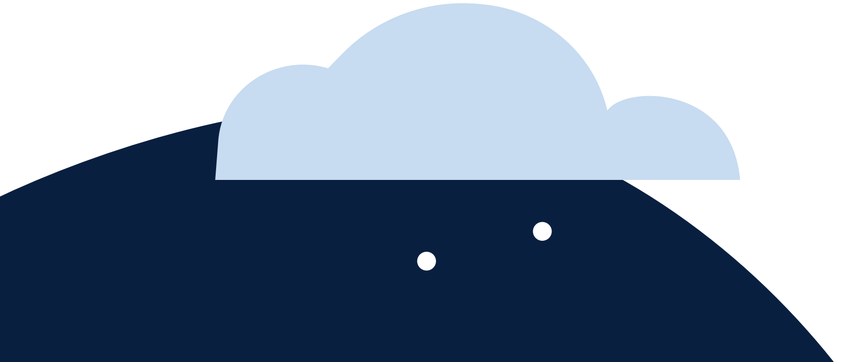


DATA PRIVACY MATTERS

Data access, as well as where data is stored, can also affect data privacy requirements.

The General Data Protection Regulation (EU) (GDPR) is a regulation for data protection and privacy in the European Union and European Economic area. Any entity that collects or processes personal data from residents of the EU must be compliant with the GDPR.

The United States doesn't have a singular law that covers the privacy of all types of data. (Instead, it has a mix of laws such as HIPAA.) However, five states—California, Colorado, Connecticut, Utah and Virginia—have enacted comprehensive consumer data privacy laws. There's a good chance that more will follow.



Before you contract with a CSP to put data into the cloud, or even if you already have, make

- **Consider the data you put in the cloud. Sensitive, critical, or regulated information requires additional security and may need to be segregated. Personal information may be governed by data privacy laws and regulations like GDPR or various state laws.**
- **Ask where the CSP's servers are located, where its primary users work and how data is transferred. The answers to these questions impact legal jurisdiction and data protection laws.**
- **Ensure that the CSP communicates with you during every step of the data oversight process. This is crucial for complying with data privacy and protection laws, which often require prompt notification of any data breach and documentation of all steps taken to remedy the problem.**
- **Know what categories of employees at the CSP access your data and confirm whether the provider uses any subcontractors who may require access.**

Few, if any, companies can do without their data – at least not for very long and not if they want to avoid going astray of various regulatory requirements.

For example, under the HIPAA Security Rule, covered entities (defined as health plans, health care clearinghouses, and health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards) must:

DR AND BACKUP COMPLIANCE REQUIREMENTS

- **Develop and implement a data backup plan**
- **Develop a disaster recovery (DR) plan**
- **Develop and emergency mode operation plan**
- **Develop and implement procedures for testing and revision of contingency plans**
- **Perform an application and data criticality analysis**

PCI DSS applies to any system or environment that stores, processes, or transmits cardholder data. That means the environments housing backups and DR are included within the scope of PCI DSS if they touch cardholder data.

Having the necessary DR and backup solutions in place can help meet these compliance requirements. But if those solutions are built on a CSP's infrastructure that has been audited for PCI DSS and HIPAA compliance, all the better.

GET WHAT YOU EXPECT

Here are some tips to make sure you are getting what you think you're getting — and need — from your CSP.

- **Understand your compliance requirements. Bring in a third-party compliance expert if necessary.**
- **Sit down with the CSP and define your security and compliance needs, and determine who will be responsible for meeting them. Document roles and responsibilities.**
- **Work with your CSP to map its controls to your compliance requirements to help you identify gaps.**
- **Ask for a complete run-down on the CSP's security protocols — logical and physical. You'll also want to know who will have access to or can see your data from the CSP's organization.**
- **Study the SLA. Ask questions if you don't understand something or agree with something. Have your legal representative review it as well.**
- **Ask for references from the CSP, as well as recommendations from peers. Don't be afraid to ask the hard questions.**
- **Verify the CSP has undergone the required independent audits for compliance with the standard, government mandate or regulation you're concerned about. Ask to see the CSP's report on compliance (ROC), which attests that all processes and components under the CSP's control are compliant.**
- **In the case of HIPAA compliance, make sure a prospective CSP will sign a business associate agreement (BAA). The BAA outlines the CSP's responsibilities and those of your organization in protecting protected health information (PHI) from contract start to termination.**

PARTNER WITH US SIGNAL

While US Signal can't eliminate compliance requirements for you, we can help ease the burden. US Signal maintains a well-governed, high-quality IT infrastructure that meets the demands of a wide range of governing agencies. By ensuring the necessary security controls and documented processes are in place and regularly audited, US Signal can help your company meet many of its compliance requirements.

We take pride in going beyond both the norm and requirements in our industry to maintain a well-governed, high-quality infrastructure. Here are just a few advantages we offer:

To learn more, call us at 866.2.signal or email: info@ussignal.com

US SIGNAL®

- **Cloud infrastructure and data centers independently audited to meet SSAE 18, SOC 1, Type 2, HIPAA HITECH and PCI-DSS; all are audit-ready with technical and security controls to meet a variety of regulatory requirements and industry standards including: Sarbanes-Oxley, FDA, Gramm-Leach-Bliley, ITAR, and FISMA**
- **Extensive experience working with customers in industries that must comply with PCI DSS, HIPAA and other regulatory requirements or industry standards**
- **Audit assistance available, including helping with management representation letters and regulatory questionnaires and providing a signed Business Associate Agreement (BAA) or copies of compliance documentation**
- **On-staff compliance officer**
- **Full Governance, Risk, and Compliance (GRC) program**
- **Risk-based BC/DR plan that includes multiple live tests each year, follow-up action item review, and reporting**
- **Vendor due diligence program**
- **People-centric security with all US Signal employees trained at hire and annually on security policies and protocols**

US SIGNAL COMPLIANCE + CERTIFICATION OVERVIEW

US Signal is audited for compliance with or holds certifications for numerous regulatory requirements and industry standards. Among them*:

SSAE 18, SOC 1, Type 2

US Signal is independently audited to meet SSAE 18, SOC 1, Type 2.

HIPAA / HITECH

US Signal is audited for HIPAA compliance annually by an independent third-party auditor, and will sign a Business Associate Agreement (BAA).

SOC 2, Type 2

US Signal has completed the SOC 2, Type 2 attestation, providing third-party assurance to customers that we have the appropriate internal controls and operational procedures in place to protect customer data.

PCI-DSS

US Signal is independently audited to meet standard secure data hosting and processing practices for card holder data.

GDPR PRIVACY SHIELD

US Signal is certified under Privacy Shield and GDPR — compliant for the transfer of European Union subject data to better support customers with international business needs.

FBI CJIS

US Signal is self-certified for FBI Criminal Justice Information System Security Policy (CJIS) compliance. This enables us to provide services to law enforcement agencies at the local, state, and federal level.

INTERNATIONAL TRAFFIC IN ARMS REGULATIONS (ITAR)

US Signal is compliant with the International Traffic in Arms Regulations (ITAR) and maintains self-certification with the obligations and requirements of the regulation.

** Contact US Signal for the most up-to-date list of compliances and certifications.*

US SIGNAL®