Business Communications Compliance & Security in the Cloud Computing Era

FluentStream

(877) 312-6477 | www.fluentstream.com

Table of Contents

1
Background

The cloud has changed nearly every aspect of modern communication. Its benefits are certainly significant - lower cost, increased speed to market, faster and more elastic deployments - and yet many businesses have concerns about compliance and security.

These concerns stem from the fact that Voice over Internet Protocol (VoIP) and other cloud-based telephony services began as a fluid, largely unregulated technology. At first, regulatory agencies maintained a light-touch approach. Then, as cloud-based communication proved itself a superior alternative to landline services, federal and industry regulations finally began to catch up and define new standards.

Now that the space has matured and standards have solidified, cloud-based providers like FluentStream are able to offer internal security frameworks that meet (and even exceed) federal and state regulations.

This summary provides a comprehensive guide to the regulatory requirements of VoIP telephony and FluentStream's role in providing industry-leading security and compliance for our partners and customers.

2

Industry and Government Standards for Compliance and Security

There are a number of standards entities - both within industry and government - that define, regulate, and police the security standards for the communications technology industry. These standards extend beyond general IT cybersecurity and encompass both the regional and industry efforts to ensure the security and reliability of VoIP services. All qualified Enterprise VoIP providers should develop technology, services, and protocols in compliance with these standards.

SECURITY AND FREEDOM THROUGH ENCRYPTION (SAFE) ACT

Under this legislation, any form of encryption is permitted for use, fostering the protection of classified information for all US citizens.

How FluentStream Helps

FluentStream follows Advanced Encryption Standard (AES) encryption best practices for FluentStream Internet-transit traffic. Our online identities are all validated by an external trusted root certificate authority that provides validation not only of our security but of our identity and the legitimacy of our business entity.

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

HIPAA compliance requires healthcare organizations to put mechanisms in place that control access to patient data. This act mandates industry-wide standards for the protection of health care, insurance, and billing information, and any other medical processes as they relate to (PHI) [1]. Compliance measures must be continuously verified throughout the communication lifecycle as policy adapts over time. This places responsibility on the service provider, business subcontractors, and customers.

How FluentStream Helps

FluentStream supports all efforts to comply with HIPAA. In the event that our customers are covered entities, FluentStream will sign a Business Associate Agreement (BAA) with any HIPAA covered entity to ensure HIPAA regulations are met. In our standard Terms of Service, we include an addendum indicating our responsibilities under HIPAA, including the commitment to the BAA.

2

Industry and Government Standards for Compliance and Security

THE PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI-DSS)

This policy sets the global technical and operational standards for all financial and cardholder data shared through applications or devices [2].

How FluentStream Helps

FluentStream follows Advanced Encryption Standard (AES) encryption best practices. Additionally, FluentStream does not locally hold information within the scope of PCI-DSS inside our systems. An outside, certified PCI-DSS 3.2 certified payment provider is used for storage of PII and other sensitive information such as credit cards.

CUSTOMER PROPRIETARY NETWORK INFORMATION (CPNI)

CPNI is the information a service provider collects from subscribers in order to provide the appropriate services and billing. This information includes inbound/outbound call records, features utilized such as voicemail or call forwarding, phone numbers, and more. Federal standards restrict the disclosure and accessibility of this information to authorized personnel under the following circumstances: with customer approval, by law enforcement, and in the provision of customer services from which the information is derived [3].

How FluentStream Helps

FluentStream, along with all other VoIP service providers, are mandated to file annual reports that certify compliance with commission rules protecting all CPNI. In addition, if there are account changes, data security breaches, or suspicious behavior customers will be notified.

E-911

In the United States and Canada, all customer made emergency services 911 calls and Automatic Number Identification (ANI) must be transmitted to the customer's designated Public Safety Answering Point (PSAP). Customers must provide their service provider with their registered location information at the start of service [4] and anytime the customer's location changes.

How FluentStream Helps

In the United States and Canada, we offer E-911. This associates your device with a physical location to guarantee that emergency calls are directed to the appropriate Public Safety Access Point and routed to the necessary emergency services. By ensuring your numbers and locations are registered to the appropriate databases, the Public Safety Access Point will have the appropriate information to dispatch emergency services, should they be required. We also support room level E-911 upon request.

3

Information Privacy and Data Security in Hosted Cloud-Based Telephony

Due to the distributed nature of cloud-based technology and the shared responsibility of data security, safety concerns are a top priority for interested businesses.

The actual and perceived risks for data in the cloud occur in three primary environments:

- **Internal security** encompasses reliability of service, data availability, in-house data security, and data destruction.
- **External security** risk includes hacking, eavesdropping, and failure to segregate private information.
- **Physical security** includes data center infrastructure and storage of information.

4

Internal Security

A key metric to note when auditing VoIP providers is the four nines, meaning **99.99% service uptime.**

AVAILABILITY

The primary concerns of a customer using cloud-based technology are often the accessibility of data and reliability of service. A key metric to note when auditing VoIP providers is the four nines, meaning 99.99% service uptime. Adherence to this standard is designed to prove the provider protects access to data and services, no matter the circumstance, and even through many forms of catastrophic failure.

How FluentStream Helps

FluentStream uses a number of failover tools that ensure service reliability maintains the highest uptime possible, regardless of natural disasters or unforeseen outage occurrences. Should a failover occur, redundant Tier IV datacenters with provider diversity ensure continuity of service and geographic isolation of independent computing elements prevent systemic failure. Additionally, FluentSteam's flexible failover of voice communications include automatic call rerouting to additional SIP destinations, as noted in the Service Level Agreement, including access to Toll Free SMS/800 database routing. FluentStream services offer an innate suite of security protocols and architecture plans based on industry best practices. Service providers allocate special attention to security throughout the lifecycle of products and services; implemented in the design, development, and application of technology.

4

Internal Security

DATA CONFIDENTIALITY AND CLASSIFICATION STANDARDS

FluentStream takes advantage of the third-party Cloud Computing Services (CCS) ability to set granular permissions with least privilege access configurations. Administrators can manage user access and permission levels via the Role Management application. With the ability to classify different roles on the front-end system and in Application Programming Interface (APIs), administrators can implement and enforce security protocols to protect data confidentiality, based on company policy or classification standards. Permissions can be assigned to predetermined roles or individual users, via the discretion of the administrator.

TRACK, MONITOR, AND AUDIT DATA ACCESSIBILITY

FluentStream's use of CCS allows a defined hierarchy of information privileges to prevent internal information breaches. By providing definitive roles tied to unique permissions, we can completely control the access and manipulation information.

DATA DESTRUCTION

VoIP data management services include: data acquisition, sustainability, deployment, and destruction processes. This allows clients to comply with all internal corporate responsibility objectives while maintaining federal security standards.

The use of CCS allows FluentStream to meet all best practice standards for data destruction within CCS. Except where required by law, Amazon Web Services (AWS) uses deep data scrubbing of deleted data in our systems, to ensure that data is not preserved when it has been asked to be deleted.

5

External Security

FIREWALLS

Firewalls are designed to prohibit unauthorized access to private network information via proxy servers, packet filtering, Intrusion Detection Systems (IDS), and more [5].

How FluentStream Helps

FluentStream technology allows for packet filtering that controls information transmission based on the source or destination IP as well as the Differentiated Services Control Protocol (DSCP). This allows network and security administrators to apply policies that support a defense in depth approach and to provide attribution for voice ingress and egress paths in the network environment.

Your data is available to you, and only you, **24/7/365.**

SEGREGATION OF DATA IN THE CLOUD

The transmission of all customer and provider data is continually monitored for inconsistencies or failures. This ensures data is securely segregated from other customer environments and inaccessible to Cloud Security Provider (CSP) personnel. Supporting Session Initiation Protocol (SIP), Transport Layer Security (TLS), and ZRTP and SRTP signaling for call and media transmission, your information can be secured throughout the entire communication lifecycle [6].

How FluentStream Helps

FluentStream's comprehensive data-security technologies include: intrusion-detection systems, fraud analytics, system hardening, vulnerability scans, and system logs. FluentStream provides authentication platforms and identity verification protocols that ensure a user can never access data outside of their own network. Finally, our geographically-dispersed, redundant data centers ensure 99.99% uptime and are systematically monitored and upgraded to ensure confidence in service longevity. Your data is available to you, and only you, 24/7/365.

6

Physical Security

AWS data center infrastructure and security Company data stores are accessible on a least privilege access model and bound by a confidentiality non-disclosure agreement with FluentStream. All electronic and physical access is logged following compliance guidelines.

STORAGE OF CUSTOMER DATA

When data is “at rest” it is encrypted and stored within a cloud service to provide data asset security and compliance with security standards, such as HIPAA and PCI-DSS. All FluentStream customer information is stored on a computer system located in a controlled facility with limited, secured access.

7

Joint Governance of Safety, Risk, and Compliance

Information security is a shared responsibility between a service provider and subscriber, contingent on provider diligence and the subscriber's willingness to participate. There are a number of policies, processes, and technology that are key to optimizing security and compliance that should be considered when considering service providers.

Written policy documentation between the provider and subscriber which outlines measurable objectives, designation of responsibilities, and consequences for violation is the key framework to ensuring information security for both parties. Voice over IP service providers have a unique set of responsibilities that include network controls, data security, and safety infrastructure. Subscribers' responsibilities include end user policy management and dissemination, password integrity, limiting internal access to information, and the mindful use of technology. These actions when followed accordingly work in concert to provide confidence in security, privacy, and compliance.

SERVICE PROVIDER RESPONSIBILITY

The primary function of a service provider is to provide and to help integrate a suite of redundant network controls including firewall protection, encryption, access controls, and maintenance procedures. By offering redundant and complementary protective measures providers produce a comprehensive security plan for combatting external unauthorized attacks on private or personally identifiable information.

SERVICE SUBSCRIBER RESPONSIBILITY

The key responsibility of a subscriber is to intelligently utilize cloud-based technology and take a number of steps to facilitate cybersecurity and information privacy. This extends across multiple layers of use.

Subscribers can take a number of actions to solidify in-house information security. First, restrict administrator privileges to a few trusted members and utilize strong passwords and PINs, including a reliable mechanism to systematically update them over time. Additionally, administrators should attempt to avoid known voice phishing attacks and scams and block malicious numbers of unwanted inbound calls to restrict unwanted communications that can serve as an attack conduit.

8

Strategy for the Future

As cloud computing and VoIP telephony continue to replace antiquated infrastructure and technologies, more industry and federal standards will adapt to encompass these technologies. To ensure continued compliance and security, cloud-based technology will remain adaptable.

There are a number of different protocols, technologies, and infrastructures in place to provide comprehensive security for data hosted in cloud-based systems. It is FluentStream's policy to maintain best in class support for these security and compliance efforts and to partner with customers in the designing and developing best-in-class service and support in the Voice over IP industry. Please contact FluentStream with questions about compliance efforts or for assistance in aligning your organization's needs for telephony compliance with solutions in the market.

9

References

1 "HIPAA." What Is HIPAA. California Department of Health Care Services, n.d.
Web. 19 Apr. 2016

2 Security Standards Council. "PCI Security." PCI. N.p., n.d.
Web. 1 Apr. 2016

3 Rouse, Margaret. "What Is Gramm-Leach-Bliley Act (GLBA)? Definition from WhatIs.com." SearchCIO. WhatIs.com, n.d.
Web. 19 Apr. 2016

4 Federal Communications Commission. "Protecting Your Telephone Calling Records." Federal Communications Commission. N.p., 17 May 2011
Web. 19 Apr. 2016

5 "Indiana University Indiana University Indiana University." What Is a Firewall? Indiana University, 18 Nov. 2013
Web. 19 Apr. 2016

6 Ghaffar, Ahmar. "Internet Telephony Feature Article: How Secure Is VoIP?" Internet Telephony Feature Article: How Secure Is VoIP? N.p., n.d.
Web. 19 Apr. 2016