It’s no surprise that you have concerns about the privacy and security of sensitive data in the cloud. In 2019, there was more data stolen than ever before, with a total of 7.9 billion records compromised.

Without the right privacy controls, data security policies, and technology in place, your data is at risk of being breached.

Data breaches in the public sector cost taxpayers upwards of $1.35 billion in one year alone.

Data breaches are 2.5 times more likely to go undetected for long periods of time relative to other sectors.

State governments allocate $54.5 billion to IT security spend while local governments allocate $53.1 billion.

Balancing Data Privacy with Secure Access.

Four Ways to Manage Your Data in the Cloud

"By enabling full compliance for our law enforcement agency, Virtru gave us a path toward a complete cloud migration."

– Susan Lyon, Manager of Google Cloud Team, State of Maryland

This level of security, privacy, and accessibility requires the implementation of new digital workflows and cloud-based infrastructures.

With Virtru, organizations can share sensitive data—including CJI, PII, and PHI—throughout digital workflows while maintaining compliance.

Contact us to learn how Virtru can help secure your sensitive data in the cloud.

virtru.com/contact-us

Government agencies must consider citizens’ data privacy rights while ensuring that health, safety, and municipal requirements are fulfilled.

To provide constituent aid, government agencies must be able to securely share sensitive information, such as PII and PHI.

End-to-End Encryption to ensure cloud vendors and unauthorized parties will not be able to access your proprietary data, like regulated content, citizen PII, and financial information.

Customer-Hosted Keys that give you direct control of your data stored in the cloud, guarding against unauthorized access by email and cloud providers. This gives you ownership over highly sensitive government and citizen data.

Access Controls to ensure sensitive data is only accessed by authorized collaborators and remains private, wherever it’s shared.

Granular Audit for visibility into who has accessed your data, when and where, making it easy to comply with federal regulations, such as HIPAA, CJIS, and FERPA.

End-to-End Encryption

To provide constituent aid, government agencies must be able to securely share sensitive information, such as PII and PHI.

Customer-Hosted Keys

Access Controls

Granular Audit

With Virtru, organizations can share sensitive data—including CJI, PII, and PHI—throughout digital workflows while maintaining compliance.

Contact us to learn how Virtru can help secure your sensitive data in the cloud. virtru.com/contact-us

© 2020 Virtru Corporation