FACT SHEET

UCAAS

Windstream Enterprise UCaaS HIPAA Safeguards

For Windstream Enterprise Unified Communication as a Service (UCaaS) there is a possibility that electronic Protected Health Information (ePHI) could be contained within the voicemails being stored as a part of the solution, and for that reason Windstream Enterprise is providing the details about HIPAA safeguards we apply to our solution.

Windstream Enterprise UCaaS HIPAA Safeguards

For transmission services Windstream Enterprise offers where we would not have routine access to and would not host protected health information when providing the services, we would meet the conduit exception to the HIPAA Final Omnibus Rule. This includes Windstream Enterprise network and connectivity solutions.

Windstream Enterprise provisions our UCaaS solution with virtual separation between each customer's instance. Furthermore, Windstream Enterprise deploys the UCaaS solution for each end user in a single tenant configuration.

The Windstream Enterprise UCaaS solution can implement on customer request additional software to encrypt the voicemails while at rest and this would be included as a component of the solution once requested to be included.

Finally, in conjunction with our Strategic Alliance partner TierPoint, Windstream Enterprise's UCaaS workload is hosted in dual data centers to provide diversity and resiliency. TierPoint holds HIPAA certifications for those data centers. The access to those physical areas is limited to Windstream Enterprise Day 2 support staff. That access is logged and tracked.

For additional details, attached is a checklist that details how Windstream Enterprise's UCaaS solutions addresses different security criteria.

UCaaS Security Checklist

CRITERIA	YES	NO	COMMENTS
Does the product modify and/or access electronic Protected Health Information (ePHI)?		x	
Is the product software-based?	+		
Is the product website-based?		x	
Is the product hardware-based?		x	
If yes, can the hardware be locked in place?			
Does the hardware have protections against tampering?			
Does the product use cloud-based technology?	+		
Does our organization have the following:			
Business Continuity Plan?	+		
Disaster Recovery Plan?	+		
Security Incident Response Plan?	+		
Data Destruction Policy?	+		
Data Retention Policy?	+		System backup and application data is stored — up to 6 months.
Access Control Policy?	+		
Does our organization own the data used by the product?		x	The application data is owned by our end customer.
Does our end customer own the data used by the product?	+		
Is the product at a minimum FIPS 140-2 certified?	+		
Are redundancies in place to prevent possible downtime?	+		
Does the product use unique IDs?	+		
Does the product use passwords?	+		
If Yes, do passwords require the following: - At least 8 characters? - Uppercase? - Numbers? - Symbols?	+		Passwords use all of the criteria listed.
Does the product have auto-login capabilities?		x	
Does the product have auto-logoff capabilities?	+		
Does the product have timeout capabilities?	+		
Does the product use two-factor authentication?		x	
Are there administrative capabilities?	+		
Does the product have Access Controls for our end customer to utilize?	+		Limited
Are there audit reports that the end customer can review for HIPAA and/or other security procedures?	+		Call Accounting
Is the data at rest encrypted? If Yes, please indicate the encryption standard you are using.	+		At customer request encryption at rest can be added to the solution. All data at rest is over private cloud via encrypted MPLS.
Does anyone other than Windstream Enterprise and the end customer have access to the stored data?			Upon request file and volume level data-at-rest encryption with AES 128-bit and 256-bit key length encryption and integrated, secure encryption key management to separate keys and encrypted data.
Where is the data physically stored?			Windstream Enterprise UCaaS solution is a private cloud instance over MPLS
Is the data stored by a Third Party? If Yes, please indicate the Third Party.	+		Data is stored in dual TierPoint data centers
Is the data in motion encrypted? If Yes, please indicate the encryption standard being used. If No, please indicate how the data is being protected.		x	All data in motion is over private cloud via encrypted MPLS.
Is there any latency/lag with the transmission of data?	+		All latency is within parameters required for real time communications.

2958 I 01.18 ©2018 Windstream Services, LLC. All Rights Reserved.

WINDSTREAM ENTERPRISE