Key Technical and Security Control Capabilities

NextGen Virtual Visits™

This Q/A highlights the solution's key technical and security control capabilities.

QUESTION	ANSWER
What is NextGen Virtual Visits?	NextGen Virtual Visits is an integrated telehealth platform that provides secure video connection between patients and care givers.
What type of data will be utilized, stored, or processed while under your control as a result of the service engagement?	Data stored or processed while under our control includes: • Patient name • Appointment date, time, and location • Event type • Provider name
Does your solution utilize any cloud-based infrastructure?	Yes. Amazon Web Services (AWS).
Is all data maintained in an encrypted state on all devices, including, servers, workstations, portable devices, and removable media?	Yes
Does the solution prevent co-mingling of our data with other client's data?	Yes. All data has a foreign key which is utilized when retrieving data. In addition the system of record for all information remains the EHR, and the telehealth solution only stores a minimal amount of PHI related to appointments and contact information.
Does the solution support the ability for us to own and manage the encryption key(s) utilized for data-at-rest encryption of our data?	No. We are unable to support BYOK at this time.
Do you maintain any industry standard certifications?	Yes. NextGen Healthcare is SOC 2 and HITRUST CSF certified.
Is the solution HITRUST certified?	No. NextGen Healthcare will include operations from the virtual visits application in the next full cycle for HITRUST; however, as part of the OTTO Health acquisition process in 2019, we implemented full adoption of NextGen Healthcare policies, procedures, training, and assurance testing with controls within the HITRUST CSF framework. A SOC 3 and evidence of a valid HITRUST CSF certification will be made available upon request.
Do you conduct solution penetration testing on at least a yearly basis? Is testing performed by an accredited third-party? Are critical and high risk vulnerabilities identified and promptly remediated within 30 days?	Yes. As part of our requirements third-party testing is conducted at least annually, with a third-party, qualified tester. All vulnerabilities are prioritized and assessed for risk.

nextgen® healthcare

Does the solution have any internet facing access points (websites, portals, FTP, etc.) that require providers and other support users to log in?	Yes
Do the above mentioned interfaces support single-sign-on (SSO) utilizing SAML 2.0?	No. This is not currently available today, but is on the product roadmap.
Does the solution require a desktop or server based client to be installed on systems?	No
Does the solution require a browser plugin to be installed on systems?	No
Does the solution require a mobile app be installed on mobile devices?	No
Will this solution require any other component (not detailed above) to be installed?	NextGen Virtual Visits requires an API that would need to be implemented, or made accessible depending on the EHR/PM system you use.
Is any data stored, outside the United States?	No
Is any data processed outside the United States?	No
Is any data accessed from outside the United States?	No
Will access to data in your possession be provided to third-party contractors or offshore resources?	No
Do you maintain an intrusion detection or prevention system that detects or prevents unauthorized activity from traversing the solution?	Edge protections are instituted which include firewall protections. The environment is within a virtual private cloud and public access is not available to backend resources such as databases. Allowlisting is incorporated to ensure that only allowed VPN connections are made to the environment.
Do you maintain data loss prevention (DLP) tools to detect and prevent the unauthorized movement of data from your control?	DLP is not currently enabled for the product; however, the information is held within the customer's EHR application. Patient data stored within the EHR would not be subject to loss with implementation of this product.
Do you conduct, at minimum, quarterly vulnerability scanning? Are critical and high risk vulnerabilities identified and promptly remediated within 30 days?	Yes. NextGen Healthcare conducts scanning for both vulnerabilities and application no less than quarterly or upon major change of the system. These are addressed based on risk and potential impact.
Do you maintain documented business continuity and disaster recovery plans that include information security controls?	Yes. These continuity plans went through a tabletop exercise (TTX) engagement in February 2020.

BETTER STARTS HERE.

For questions contact **security@nextgen.com**