

HCIC Documentation of Security Measures for Clinical Videoconferencing Connections

This form is required as written documentation that security measures are in place for all videoconference endpoints and connections that are used for the provision of clinical services to HCIC members.

Name of Network Provider (agency name)

Endpoint location (physical address)

Videoconferencing platform type (e.g., Zoom, Polycom)

Please check the type of connection this endpoint has.

- Private cloud (e.g., MPLS)
- Public Internet Connection
- Public Internet connection through a Virtual Private Network
- Other (Please specify: _____)

HCIC requires secure connections for all clinical videoconferences on the Public Internet and on our private wide area network (HCICnet). Please check one:

- This endpoint is always connected with AES encryption on or via a secure VPN for clinical videoconferences via the public internet and uses a video platform that has AES encryption enabled on it.

Your name: _____

Signature and date: _____

Please send the completed form to [HCIC Telemedscheduling](#) or HCIC Telemedicine Staff, fax 855-411-7558, 1300 S. Yale St., Flagstaff, AZ 86001. Thank you.