NARBHAnet 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 NARBHA members.

Name of Network Provider (agency name)

_____

Endpoint location (physical address)

_____

Endpoint type (e.g., Polycom HDX 6000) _____

Please check the type of connection this endpoint has.

- ☐ Point-to-point connection (e.g., T1)
- ☐ Private cloud (e.g., MPLS)
- ☐ Public Internet Connection
- ☐ Public Internet connection through a Virtual Private Network
- ☐ Other (Please specify: _____)

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

- ☐ This endpoint has AES encryption enabled for clinical connections on NARBHAnet.
- ☐ This endpoint is always connected with AES encryption on or via a secure VPN for clinical videoconferences via the public internet.

NARBHA requires specific privacy measures on the codec (see Provider Policy 10.10) Please check all privacy measures employed on this codec:

- ☐ The codec is set to "auto answer mute."
- ☐ The codec is password-protected.
- ☐ The codec is set to "auto answer multipoint: Do Not Disturb."
- ☐ The codec is always turned off when not in use or the camera lens is always covered when not in use.
- ☐ The codec is NOT set to "allow video display on Web."

Your name: _____

Signature and date: _____

Please send the completed form to telemed@narbha.org or NARBHA Telemedicine Staff, fax 855-411-7558, 1300 S. Yale St., Flagstaff, AZ 86001. Thank you.