Strong Authentication Device User Policy

As an AHS Remote Network User, I will:

1. Keep the token and Personal Identification Number (PIN) private. It will not be shared with anyone at anytime.
2. Prevent the User ID and PIN from being divulged, shared or compromised.
3. Keep the token in a secured location at all times (e.g. not in open view in an unattended workspace).
4. Use the User ID and token only for the purposes specifically required and permitted for my role.
5. Maintain the confidentiality and security of any data accessed from the AHS network or any data handled on behalf of AHS.
6. Not release any information to any unauthorized people.
7. Report a lost or stolen token immediately to the AHS IT Service Desk at 1-877-311-4300.
8. Return the token to my manager if it is no longer required for my role.

Inappropriate collection, use or disclosure of person identifiable data may result in disciplinary action and termination of your AHS network access User ID.

I understand and agree to comply with the AHS Strong Authentication Device User Policy for remote network access.

You are welcome to explore more information on the RSA SecurID Tokens Fact Sheet.