|  |  |  |
| --- | --- | --- |
| Remote Access to Systems by Vendor(s) | Last Revision: | April 2019 |
| Last Reviewed | April 2020 |
| Applies to the following THA Group of companies: | * Island Health Care * Island Hospice * Independent Life at Home * RightHealth® * Palliation Choices * THA Services |
| Included in the following THA Manual: | Administrative Policies & Procedures  Management of Information & HIPAA |

PURPOSE

To define the conditions and controls under which authorized information technology vendors are allowed remote electronic access to our information system assets. It is a generally accepted practice in the industry to permit IT vendors remote access to the portions of the system that they support or maintain. This is often the quickest and most economical means of support/maintenance for both the vendor and customer. However, the organization takes reasonable steps to assure that such access is appropriate and protected from potential abuse.

POLICY

1. Conditions of Access

Vendors are permitted remote access solely to support or maintain our system. This includes assistance such as posting updates to their product, troubleshooting to resolve a problem we report, and training as requested by an authorized employee. When accessing the system vendors are not permitted access to any patient information without our approval, which is withheld unless such access is required to achieve a legitimate business purpose. Access is specifically prohibited for any purposes related to sales, marketing, research, or any other internal needs of the vendor not specifically required to support or maintain our use of the system. All vendors for whom such access is permitted will have a chain of trust agreement/business associate contract with THA Group.

1. Written Agreement

A written agreement is required from any vendor requesting remote access to our system. The agreement includes, at a minimum:

1. Agreement under what circumstances they are permitted remote access
2. Agreement that they will abide by reasonable access controls we may require
3. Acknowledgement that they will protect the security and confidentiality of our systems and data/information residing in it
4. Acceptance of liability for unauthorized use or access by, or on account of, their organization and/or employees
5. Such verbiage may be part of a purchase/lease/maintenance contract with the vendor, other contracts used in support of HIPAA compliance - - or other forms of written agreement.

3. Requirement to Update This Policy

This policy is reviewed and/or updated at least every three years or more often as appropriate. If any major changes to remote access methods are made, the policy is updated prior to the new changes going into routine operational production