SWEDISH

INFORMATION SECURITY: REMOTE ACCESS BY VENDOR OR THIRD PARTY

Administrative Policy	
Approved: February 2012	**Next Review:** February 2015
Department: All departments	
Population Covered: All vendors who are granted remote access to Swedish systems	

Related Policies/Procedures:

Information Confidentiality Agreement
Information Security: Acceptable Use of Information Assets
Information Security: Account and Password
Information Security: Affiliate Access
Information Security: Outside Reviewer/Auditor/Monitor Epic Access
Information Security: Proper Disposal of Confidential Information
Information Security: Remote Access by Swedish Workforce

Purpose

To define the terms and conditions for remote connection to the Swedish network by vendors, consultants or contractors. To protect Swedish information from unauthorized access, use, and disclosure by providing guidelines for appropriate remote access.

Responsible Persons

Department managers or other parties who have contract authority with the third party are responsible to request access for them.

Policy

Swedish relies on the services of vendors and other third parties to complete many basic functions. Third parties pose security risks that exceed those of other users. Third parties, for example, may not benefit from security awareness training, background checks, remote office controls, and policy restrictions imposed on ordinary employees. Therefore, remote access privileges for vendors require special review and a high degree of trust with the vendor.

Eligibility

Remote access to Swedish systems will only be granted to perform specific contracted functions. Third parties will be granted remote access into the Swedish network only if they require it to perform maintenance, troubleshooting, upgrades, or monitoring for devices or systems they have provided to Swedish. Access will be limited to the specific server(s) and communications ports (TCP/IP or UDP) which are the minimum necessary to perform the required support.

Granting Access

Vendors typically will request remote access during the technical review of their product or as part of the installation process. The Information Services Application Owner who is assigned to work with the vendor will provide the necessary information to the Information Security team to evaluate the vendor's requirements. The specific form of remote access which is provided is determined by the Information Security team according to the business need and computing requirements for a given connection.
Each request for vendor remote access will include specific system information (server names and communications ports), Swedish contact information, and designation of a primary Point of Contact at the company. Information will be submitted via a Remote Access Request form.

Web-based Access

The preferred method for intermittent or infrequent vendor access to Swedish computer systems is via the web-based Swedish Secure Gateway "SSG". Data is transmitted via an SSL web connection (https://) which ensures that data sent over the connection is encrypted. Third parties requiring system administration access will be provided with a "Remote Desktop" icon (RDP) which allows them to connect directly to the systems they need to administer.

VPN Access

Remote access via dial-up or Virtual Private Network (VPN) requires additional review and approval by the Information Security team. VPN access is only approved for applications and systems which cannot be accessed via SSG / RDP. Vendors or partners which will be exchanging PHI or monitoring systems on a frequent basis should use a site-to-site VPN or other direct network connection. Application for a site-to-site VPN requires completion of a Site Discovery form before connectivity will be completed by the Swedish Network team.

Confidential Data

Third parties may of necessity come in contact with Swedish production systems containing Protected Health Information (PHI). All vendors must file a Business Associates Agreement (BAA) with the Swedish Privacy Office before they can access Swedish PHI.

Third party staff may be required to complete Confidentiality and Non-Disclosure forms as a condition of access. All Swedish vendors who access Swedish systems are bound by the policy *Information Security: Acceptable Use of Information Assets*. Access to Swedish systems should never be granted to individuals who have not been authorized.

Third party employees who work on site using Swedish-provided network connectivity and/or computers are bound by the full set of Information Security policies posted on the Swedish Standards site.

Security and Monitoring

Whenever possible, remote access to Swedish systems will require two-factor authentication. This is the industry standard and is recommended by the U.S. Department of Health and Human Services for access to systems containing PHI and is required by the Payment Card Industry Data Security Standard (PCI-DSS v.2.0). Two-factor authentication is satisfied by "something you have" and "something you know" such as the SSG token plus the vendor's assigned username and password.

All remote access sessions are subject to monitoring. At minimum, for each login the date, time, and username will be recorded. System records will also show the last time someone logged in and whether there were any access failures.

Termination of Remote Access

Upon termination of the contract, agreement or other official business arrangement with Swedish, remote access will be terminated. Any hardware, including SSG tokens / fobs and Swedish-provided equipment, will be returned to the Swedish Information Service Department.

In the case where individual credentials have been distributed, it is the Point of Contact's responsibility to notify Swedish to remove or disable that user's account. The Point of Contact will contact Swedish when any new accounts or changes to existing accounts need to be made.

A periodic review of all remote access users will be conducted to validate continued need for remote access. All unnecessary or unused remote access privileges will be terminated.

Definitions

Affiliates. Organizations (such as physician offices, contracted clinical service providers, non-clinical business partners, coordinating treatment providers, and other third parties and business associates) that are not owned or managed by Swedish and which required access to electronic health records containing protected health information (PHI). A separate Affiliate Access policy is in force.

Business associate. An individual or corporate "person" that is not a member of the covered entity's workforce who performs on behalf of the covered entity any function or activity involving the use or disclosure of protected health information (PHI). These entities are required to sign specific paperwork called a Business Associates Agreement (BAA) before accessing PHI. The specific format of the BAA is defined by the Legal Services department and Privacy Office as required by HIPAA and HITECH.

Consultants or contractors. Persons who are hired to complete specific tasks or projects, or who work for a vendor or other company which has been hired to perform such work. These individuals are covered under *Information Security: Remote Access by Swedish Workforce*.

Dial-up. An antiquated form of computer connectivity where a home computer's modem would dial a phone number to connect to a remote access system. Dial-up lines are very slow compared to Internet connections. They have been removed from most corporate systems due to security concerns.

Outside reviewers. Parties which require access to limited data sets containing PHI, such as auditors and researchers. Access for these users is authorized by the Health Information Management department. See *Information Security: Outside Reviewer/Auditor/Monitor Epic Access*.

Remote access. The ability to view, edit, print, or communicate information or otherwise make use of any Swedish system resource when not directly connected to the Swedish network.

SSG (Swedish Secure Gateway). The primary means for remote access to Swedish systems. This system uses a secure web browser connection (https://) which ensures that data sent over the connection is encrypted using industry standard protections.

Vendor. Companies which contract to sell specific services to Swedish. Those which require remote access to maintain or support their equipment are covered by this policy.

VPN – Virtual Private Network. Software or hardware-based connections which allow a computer on one network to temporarily join with another network. Most users will not need this connectivity, but some staff who support servers or run particular programs may need to install Swedish-provided VPN software. The determination of whether to use VPN is made by the Information Security team.

Workforce. Employees, medical staff, volunteers, trainees, and other persons whose conduct is under Swedish's direct control while that person is performing work for Swedish. (The person does not need to be paid directly by Swedish.) Contractors who work on-site at Swedish may also be considered part of the workforce, such as temps or staff augmentation services.

Confidential information. Information which may include, but is not limited to:

- Patient information (protected health information, or PHI, as defined below; patient diagnoses, patient treatment plans, medical records, conversations, demographic information, financial information, Social Security numbers, photographic images, video, recordings, or any other information that can potentially identify a Swedish patient)
- Employee information (salaries, employment and payroll records, Social Security numbers, unlisted phone numbers, health records).
- Swedish proprietary information (financial reports, production reports, report cards, reimbursement tables and contracted rates, strategic plans, trade secrets, trademarks, logos, internal reports, memos, contracts, peer review information, credit information, internal communications, computer programs, technology, policies, procedures)
- Third party information (computer programs, vendor information, technology)

Protected health information (PHI). Individually identifiable information created or received by Swedish that relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual. This includes information such as name, address, date of birth, admission, discharge or death, telephone number, fax number, electronic mail address, social security number, medical record number, health plan beneficiary number, account number, certificate/license numbers, vehicle identifiers and serial numbers, device identifiers and serial numbers, Web Universal Resource Locator (URL), Internet Protocol (IP) address number, biometric identifiers, including finger and voice prints, full face photographic and other comparable images, and any other unique identifying number, characteristic or code. HIPAA and other federal regulations specify particular protections for electronic PHI

Supplemental Information

Also see *Frequently Asked Questions about Remote Access* (located on the Information Security section at Swedish Online),

Regulatory Requirement

Health Information Portability & Accountability Act §164 – Security standards for protection of electronic protected information:

- §164.308(a)(1)(ii)(C) – Sanction policy.
- §164.310(b) – Workstation use.
- §164.310(c) – Workstation security.
- §164.312(d) – Person or entity authentication.

The Joint Commission (TJC). IM2.20.

Payment Card Industry Data Security Standards. PCI-DSS v.2.0, Section 8.

DNV – Medical Records Services.

CMS – Patient Rights.

References

COBIT Audit Guidelines, Section DS11 – Access control.

International Organization for Standardization (ISO). (2005). Standard 17799 – Code of practice for information security management (2nd ed.) (a.k.a. ISO/IEC 27002:2005):

- Section 11 – Access control.
- Section 11.5 – User responsibilities.
- Section 11.9 – Teleworking.

STAKEHOLDERS

Author/Contact

Tracy D. Howes, RHIA, CISM, Swedish Information Security Officer
Swedish Information Security Engineers

Expert Consultants

Swedish Information Security and Access Committee

Sponsor

Tom Wood, MD, Chief Information Officer