II-360 Remote Access

Purpose
This policy informs CCHMC personnel of their obligations in establishing, utilizing, and maintaining remote access connections to CCHMC computer resources from public and non-CCHMC private networks. This policy also identifies the corresponding HIPAA and Information Security Policies that must be followed to protect CCHMC computer resources while using remote access privileges.

Policy
Remote access connections to CCHMC computer resources from public and non-CCHMC private networks must be managed and protected. All remote users must have specific authorization.

Process

Authorization (public resources)

Example: www.cchmc.org

1) The primary CCHMC web site shall maintain readily identifiable access and privacy warnings/statements, as they apply to public use.

2) When used in the customary manner (using a client, or browser) by following published hyperlinks, authorization is implicit. No further approval or authorization is required, provided the remote user understands and abides by the access, use, disclosure and privacy statements/agreements as published on the web server.

3) Attempts to access, move, add, modify, reorder, or remove data through non-standard mechanisms, including data residing on back-end/back-office resources, is strictly prohibited. Such activities, including attempts to circumvent access controls or deny service to other site visitors, will be deemed unlawful, and may expose such a user to civil action and/or criminal prosecution.  

   Example: Attempting to change the content of cchmc.org internet site (defacement).

Authorization (non-public resources)

Example: VPN access to KIDS

1) Access to Centerlink, GroupWise and other applications and protocols can be provided via the SSL-VPN resources without the need for any special remote computer configuration and can be accessed from all popular browsers.

2) CCHMC Personnel and other persons bound by CCHMC HIPAA and Information Security Policies require specific, explicit authorization to access non-public CCHMC computer resources from any public or private network.

3) Authorization for remote access will only be granted following submission of a completed Remote Access Request form that has been approved by a divisional director or higher authority. This authority will not be delegated to any individual below Associate Director level.

4) As with internal access, remote access will be limited to only the minimum necessary resources needed for essential, job-related duties and/or tasks.

5) Public networks include, but are not limited to:

   a) The internet;
   b) The public switched telephone network (i.e. phone lines);
c) Broadband networks, including, but not limited to: satellite, cable modem, digital subscriber line (xDSL), integrated services digital network (ISDN); or

d) Internet service provider (ISP) networks, including “dial-up” (SLIP/PPP) access.

6) Private networks include, but are not limited to:

a) Networks of a commercial, educational, non-profit, or government nature which are not directly visible to, or connected with public networks; or

b) Networks to which access by the public is strictly regulated or prohibited.

Example: A dedicated connection from CCHMC to Siemens Medical Systems that does not use the Internet.

Methods

The following are the approved methods for remote access to CCHMC information resources and the alternate methods for which authorization may be requested:

1) Virtual private networking (VPN)

   a) VPN is the preferred method for remote access. VPN technology encrypts (“scrambles”) data at the remote site or computer to allow secure, private communications over an insecure (public) network, such as the Internet. Data is decrypted (“unscrambled”) at the receiving site or computer, creating a virtual “tunnel”.

   b) VPN technology may be used to transmit proprietary or confidential information, including Electronic Protected Health Information (EPHI) or individually identifiable healthcare information (IIHI) when approved.

   c) Acceptable tunneling methods: IPSec and PPTP (Point-to-Point Tunneling Protocol). Use of L2TP (Layer 2 Tunneling Protocol) is expressly prohibited.

   d) Client-to-gateway VPN sessions will be established only for the time window required to perform necessary functions. VPN tunnels will not be permitted to sit idle for more than thirty (30) minutes.

   e) Gateway-to-gateway VPN connections (semi-permanent) will require the explicit approval of the Chief Information Services Officer or the Directory of Information Security.

       Example: DBA direct to CCHMC.

   f) When available, ad hoc VPN connections will be established using strong two factor authentication (such as key fobs or tokens used in conjunction with passwords).

   g) Prior to the authorization of any VPN account approval it must first be determined if sufficient access can be provided via the CCHMC Extranet services.

   h) Where technically capable, all CCHMC employee VPN accounts shall utilize the Nortel IPSec Client and access shall be limited to the minimum necessary internal network resources required to perform their responsibilities.

   i) All non CCHMC employee VPN connections for vendors and third-party support personnel, temporary personnel and consultants performing routine maintenance on CCHMC systems will be established during pre-determined maintenance windows specific to each system, as identified and documented by the system owner. VPN connections for urgent/critical maintenance will be triaged then coordinated by an authorized IS representative. In such cases, the vendor emergency access process shall be utilized.

Where technically capable, all non CCHMC VPN accounts shall utilize the Nortel IPSec Client and access shall be limited to the minimum necessary internal network resources required to perform their responsibilities.
j) Where technically capable, CCHMC gateway-to-gateway and ad hoc VPN connections (for vendor support) will be decrypted outside of an enterprise firewall prior to entering the CCHMC network. This enterprise firewall will deny all access, except to specific destination hosts via pre-established, required protocols.

2) PPP “dial-up” (NOTE: This policy does not include dial-up internet connections)

   PPP is a protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server “Dial-up” or Remote Access Services (NT RAS) use Point-to-Point Protocol (PPP) to allow remote computers to connect to the CCHMC network.

   a) Remote Access Services (RAS) is a Microsoft-specific implementation of PPP.
   
   b) Dial-up/RAS are not typically encrypted, and as such, are vulnerable to interception (“sniffing”) and redirection (“man-in-the-middle” attacks).
   
   c) Use of PPP dial-up/RAS services will only be approved in instances where the use of VPN technology is not practical or feasible. The use of VPN is preferred over dial-up connectivity.
   
   d) Use of PPP dial-up/RAS to connect to other than approved computer resources is not recommended. This includes connecting via a direct inbound dial (DID) line to a modem-equipped workstation. Information Services Security will perform periodic “phone sweeps” to identify and disable such arrangements.

3) Secure Shell (SSH)

   a) Secure Shell (SSH) is a preferred protocol which is encrypted by default. Included in SSH is a secure file transfer capability.
   
   b) The use of SSH to connect to CCHMC computer resources remotely requires that detailed justification be submitted to the Chief Information Services Officer or the Director of Information Security for explicit approval on an individual, case-by-case basis.

4) Other Methods

   Use of Remote Desktop Protocol (e.g. RDP or “terminal services”) is the preferred method accessing personal computers and resources where supported.

5) Methods not approved for use

   Use of the following methods to gain remote access to CCHMC computer resources are not approved general solutions and require the specific written approval of the CISO or Director of Information Security:

   a) Remote control software (e.g., PCAnywhere, VNC, Carbon Copy, Reachout, DameWare);
   
   b) 802.11x wireless access points, Wireless Network Interface Cards, and similar wireless technologies;
   
   c) Wireless devices that have not been tested and approved by Clinical Engineering.

**Authentication**

1) Remote access users will be authenticated by Windows NT domain login, at a minimum.

2) When available in the production environment, remote access users shall be required to utilize two-factor authentication (e.g., SecurID tokens, smart cards, or USB keys).

**Safeguards**

Remote access users will comply with the requirements of CCHMC HIPAA and Information Security Policy: [II-370 Safeguards for Non-CCHMC Computing Devices](#).
Acceptable Use

Remote Access services must be requested through the Remote Access request procedure.

1) Users who have been granted remote access privileges will be bound by all CCHMC HIPAA and Information Security Policies, regardless of their remote locations.

2) Users must read, understand, and agree to abide by the CCHMC HIPAA and Information Security Policy: II-105 Acceptable Use of Information Resources prior to being granted remote access privileges.

3) Use of remote access privileges for non-business Internet use is explicitly prohibited.

Applicability

This policy applies to all CCHMC Personnel and any other party who is authorized to access the CCHMC network including Medical Staff members, remote access users, consultants, temporary employees, and vendors.

Regulatory Authority

HIPAA Regulations: 45 CFR Subtitle A, Subchapter C, Part 164

164.308 Administrative safeguards.
   ➢ (a)(4)(i) Standard: Information access management.

164.312 Technical safeguards.
   ➢ (d) Standard: Person or entity authentication.
   ➢ (e)(1) Standard: Transmission security.
   ➢ (e)(2)(i) Implementation specification: Integrity controls.

Compliance

All CCHMC Personnel, community physicians, and business partners must comply with this policy and the associated standards and procedures. Any CCHMC Personnel found to be in violation of the privilege of CCHMC-facilitated access to business systems, or in violation with this policy, may be subject to disciplinary action, up to and including termination of employment. Medical Staff Members may also be subject to denial or removal of their privileges as part of the disciplinary process. Federal, state, and/or local law enforcement agencies may be notified if evidence of criminal actions exists. Any business partner found to be in violation of the privilege of CCHMC-facilitated access to business systems, or in violation with this policy, may be sanctioned, which could include, denial of access to the CCHMC network, cancellation of any contractual agreement between CCHMC and the business partner, discipline by the Medical Staff, and any other action deemed appropriate.

Refer to CCHMC Personnel Policy F-05 Employee Discipline for additional information regarding disciplinary action.
Implementation

The following parties are responsible for implementing and enforcing this policy:

- Policy authority for this document resides with the Chief Information Services Officer and the HIPAA Security Officer.
- All requests for exceptions to this policy or its standards must be submitted in writing, with justification to the HIPAA Security Officer (securityofficer@cchmc.org).

This policy has been reviewed and approved by the following parties:

- Chief Executive Officer
- Chief Information Services Officer
- HIPAA Security Officer

This policy will be reviewed every 3 years or sooner if deemed necessary.