



May 17, 2003

To: CEOs and Administrators of Missouri Telehealth Network Sites
From: Joe Tracy, Executive Director of Telehealth
RE: MTN Network Policies Related to Security/Privacy

In recent weeks several MTN sites have taken actions to help secure their internal networks. This is a good thing, especially since HIPAA is now in place. However, this is also a bad thing because these sites did not involve the MTN technical staff upfront before changes were made to the respective network. As a result their telehealth and/or teleradiology connections were rendered useless for some period of time.

Please note that all of us at MTN are concerned about privacy and security as it relates to the network. However, please remember your main connection the Internet is provided through us via MORENet. As such, your technical staff or consultants should always work with us before implementing any changes that may impact the network as it is currently configured. We are here to assist you in that process.

The MTN, MORENet and MU Health Care Information Technology staff have been working on several things behind the scenes as it relates to your network connections and HIPAA. Here now is a glimpse of what we will most likely implement in the next few months to protect all of us:

1. We will be installing a secondary network card in each router. The telehealth and/or teleradiology equipment will use one of the cards and the second card will provide your local network with connectivity to the Internet. We are doing this for three main reasons:
 - a. The telehealth/teleradiology connections must run outside of any internal firewall you may install to protect your local network;
 - b. It provides you with the flexibility to install your own local area network firewall without impacting the telehealth connections; and
 - c. It provides MORENet with the ability to **temporarily** terminate your connection to the Internet if one of the devices on your local area network is found to be compromising the security of the larger network. Such problems are sometimes the result of an infected PC trying to spread a virus. Once your internal problem has been solved, MORENet will reconnect you to the Internet. Please note that disconnecting your Internet connection for this purpose will not impact your telehealth and/or teleradiology connections.
2. We will also be installing our own firewall/encryption devices to protect the telehealth and/or teleradiology transmissions across the network.

I have attached the MTN Acceptable Network Configuration and Security Policy for your files. It will become effective on the date we install the second network router card at your facility. Please keep a copy in your records and distribute one to your information technology staff or consultants.

As I said earlier, network security is very important to us and we want to ensure you are protected too. So please have your IT staff or consultants call us prior to installing any hardware or software that may impact the current network configuration. We stand ready to help.

Thanks for your time. As always, if you have any questions please feel free to call me.



Date: June 4, 2004

TO: MTN Site Chief Executive Officers and Telehealth Site Coordinators

FROM: Joe Tracy, Executive Director of Telehealth

SUBJECT: MTN's Network Security Implementation Effective July 15, 2004

Last May a letter outlining our intention to develop a new level of security for the Missouri Telehealth Network (MTN) was sent to you. A copy is enclosed in this packet of information. I'm pleased to announce that we are now ready to implement the new network security measures that are designed to better protect all MTN sites from network security problems. With that said, on or before July 15, 2004, all MTN sites must comply with the network security and configuration policy attached to this memo. Any site that is not in compliance by that date can do one of the following:

- a) request an extension, in writing, of not more than 30 days in an effort to meet the rules set forth in the policy; or
- b) notify MTN of their desire to terminate their Internet access that is now provided through MOREnet. *It is important to note that due to recent changes in MOREnet's policy related to Internet access by MTN sites, any site choosing to terminate their current access will not be able to re-establish it at a late date.*

Sites that do not comply with the policy by July 15, 2004 and that have not exercised either option "a" or "b" above, will be automatically disconnected from the Internet on July 16th.

I hope you understand that these policies are being put into place to protect the security and utility of the entire network which will serve about 1/3 of Missouri counties by the end of 2004.

If you have any questions or NEED assistance reconfiguring your network, please contact Frank Gannan or Beth Stephenson as soon as possible. They can be reached by calling (573) 884-7958 or by e-mail – gannanf@health.missouri.edu or stephensonem@health.missouri.edu. You will also need to contact Frank or Beth about Internet Protocol (IP) address information during the network transition.

As always, if you have any questions or concerns please give me a call.



Missouri Telehealth Network (MTN) Acceptable Network Configuration Policy

This policy defines the required security standard for network configurations for MTN video and/or Teleradiology applications using routers provided by MTN and the Missouri Research and Education Network (MOREnet) at your site.

Section 1 – Network Configuration

In general, each telehealth site has a telecommunications circuit (T1 line) leased by MOREnet. For all telehealth sites installed prior to 2004 that T1 line may continue to be used for general Internet service, but only if general Internet service existed in 2003. If general Internet service did not exist at the site in 2003, the service can not be added.

The T1 line terminates at a router that was provided by MTN and is managed by MOREnet. That router has now been equipped with a second port that will be an important component of this policy. Below is a description of each router port and its approved use.

Router Port One (MTN’s responsibility)

- This port is for the exclusive use of MTN’s Telehealth and Teleradiology equipment.
- MTN may install a switch on Port One, allowing connections of MTN network or telehealth equipment only.
- Under NO circumstance can Port One be placed behind the local facility’s network firewall or connected to the facility’s local area network (LAN).

Router Port Two (Local Site’s responsibility)

- An MTN site’s local area network (LAN) may be attached to Port Two and used for general Internet connectivity. The LAN on port two can be configured how each facility sees fit as long as it does not compromise MTN’s wide area network (WAN) of locations.
- MTN recommends that a firewall be installed and configured on this port to protect the security of the information on the LAN.
- All costs associated with configuring the LAN from via Port Two are the responsibility of the local site.

Section 2 – Network Security

MOREnet manages the network connection at each MTN site and they can monitor problems as well as provide sophisticated monitoring for worms, viruses, and other unscrupulous network activities. In short this service provides the level of security MTN needs to maintain a quality network.

In the event that activity on any MTN site’s LAN jeopardizes the security of the overall network, or interferes with the application of Telehealth and/or Teleradiology, MOREnet is authorized to IMMEDIATELY shut down the

offending router port until the problem is resolved. Shutting down Port One of the router will result in the loss of Telehealth and Teleradiology services, but will have no impact on the facility's Internet connections. Conversely shutting down Port Two will result in the loss of Internet connectivity for the facility's LAN, but will have no impact on MTN's Telehealth or Teleradiology equipment.

A representative diagram for the MTN network configuration is attached to this policy. MTN suggests that a broadband router link PC's to Port Two on the router. The router also needs to be able to act as a Dynamic Host Configuration Protocol (DHCP) router.

Examples are:

Linksys 4-Port Ethernet Broadband Router

Brand/Model: LKS BEFSR41



AND

Netgear Web-Safe Ethernet Broadband Router with 4-Port Switch

Brand/Model: NTG RP614



These routers are examples only. The Missouri Telehealth Network does not promote the use of any vendor or product.

MTN New Network Configuration

