

The Health Data Net Security and Responsibility

The Health Data Net: Security and responsibility

©UNI•C May 2003

Version 1.2

By Martin Bech and Ib Lucht

Contents

General conditions.....	1
1 Target groups	1
2 Use	1
3 Security	2
4 The agreement system	3
5 Support	4
6 Financial conditions	4
6.1 Cancellation	4
6.2 Disclaimer	4
6.3 Changes to these terms	5

General conditions

1 Target groups

All stakeholders in the health sector can be connected to the Health Data Net to exchange information between systems on the net, and health sector personnel can access net services and use the net in connection with, e.g. Web searches.

Likewise, patient-information, administrative, teaching and technical support systems, as well as other significant associates which work closely with the health sector, can be connected to the net upon specific approval.

An agreement between the stakeholder and MedCom is a prerequisite for connection to the Health Data System.

2 Use

The Health Data Net may only be used for purpose-related duties within the health sector.

Use of the Health Data Net must take place within the framework established by current laws and regulations.

Use of the Health Data Net must maintain the general decorum of open nets (Acceptable Use Policy - AUP).

These very general regulations are specified in detail in the following – though not exhaustive – list of activities which will be considered as misuse of the Health Data Net.

- Attempts to access to resources (systems) on the network in Denmark and abroad without authorization.
- Attempts to penetrate the security systems of the Health Data Net.
- Attempts to use the net for distribution of information (texts, photographs, sound, etc.) which may not be distributed in accordance with Danish law.
- Attempts to destroy or distort the content of IT-based information (databases), including wilful spreading of viruses.
- Attempts to investigate or reveal other users' activities (e.g. content of electronic mail).

-
- Resale of net connections or net services without prior agreement with MedCom.
 - Disguise of identity (except in cases in which disguise is explicitly permitted).
 - Interruption of normal network functions; conscious waste of resources (involving persons, IT equipment and transmission capacity).
 - Inappropriate messages which annoy and/or inconvenience other network users (e.g. edi-junk mail, hate mail forwarded as electronic mail, etc.).

Moreover, the following regulations also apply.

The Health Data Net may not be used for commercial purposes without the express permission of MedCom.

It is the responsibility of the stakeholder to ensure that the stakeholder's users are familiar with these regulations and observe them.

Violation of these regulations in use of the Health Data Net can result in termination of the stakeholder's access to the Health Data Net, in accordance with the terms stipulated in the Health Data Net agreement.

3 Security

In using the Health Data Net, the stakeholder must observe all security regulations.

Stakeholders are responsible for:

- ensuring that the section of the individual stakeholder's net which can be connected to the Health Data Net is secured against external penetration. This security must be at a level corresponding to DS484-1.
- establishing an encrypted VPN connection to the central node of the Health Data Net.
- setting up NAT to the internal IP addresses of the Health Data Net.
- establishing regulations for the number of client addresses which may be NATed behind an SDN address.
- forwarding DNS messages involving .medcom to the central DNS server.
- establishing bilateral agreements with service providers.
- preventing traffic or services from the Health Data Net from being used by parties outside the stakeholder's net, without the express permission of MedCom.

MedCom is responsible for:

- concluding agreements with stakeholders regarding connection to the Health Data Net.
- issuing any general rules for use of the net.
- informing stakeholders of the conditions for connecting to the Health Data Net, and exercising necessary controls to ensure that rules and regulations are duly observed.

UNI•C is responsible for:

- electronic transfer of data in the Health Data Net on encrypted VPN connections through a central node which is secured in every respect against external attack.
- IP addresses in the Health Data Net, setting up route tables in accordance with established bilateral agreements, traffic control, statistics on use of the net, etc.
- the name server (DNS) of the Health Data Net and new top domains .medcom.
- DNS in connection with edi-mail.
- advising stakeholders in technical questions concerning connecting to – and use of – the Health Data Net.

4 The agreement system

If a stakeholder, such as a county, has been connected to the Health Data Net, the stakeholder cannot use the Health Data Net prior to approving bilateral agreements with the service providers (servers) to which the stakeholder wishes to have access. The reverse is true if the stakeholder makes available a service which other parties in the health sector wish to access by approving an agreement.

Such bilateral agreements are concluded in the agreement system, which is a Web-based system that can be accessed on the open Internet at aftale.medcom.dk.

UNI•C registers the institution, such as a county, and a local administrator. The administrator receives user identification/password, and is then able to register clients and servers, and to conclude agreements.

An agreement is registered in the agreement system and sent by email to both parties for signature. When UNI•C has received the signed papers from both parties, the agreement will be approved in the agreement system.

At least once a day, approved agreements in the agreement system will be transferred to the central router in the Health Data Net as ACLs by an EDP program which, in the router, allows traffic between parties to an agreement at the IP address level on the Health Data Net.

5 Support

MedCom provides administrative support.

Technical support is provided by UNI•C.

Technical support during the day:

email: fwsupport@uni-c.dk

Telephone: +45 35 87 88 88

Connection: Lennart Sorth, email: Lennart.Sorth@uni-c.dk, tel: +45 35 87 89 74

Project coordinator: Ib Lucht, email: Ib.Lucht@uni-c.dk, tel: +45 35 87 88 50

24-hour monitoring:

The node is monitored 24 hours a day. It is not possible to contact UNI•C outside normal working hours. Alarm reports will go to the UNI•C personnel on duty during this time.

6 Financial conditions

Connecting to the Health Data Net takes place in accordance with the financial conditions stipulated in the agreement.

6.1 Cancellation

The conditions for cancellation of a connection to the Health Data Net are stated in the agreement.

In connection with cancellation, the stakeholder should note the following conditions:

IP addresses will be revoked and used elsewhere in the Health Data Net.

Registered domain names in the Health Data Net can no longer be used.

6.2 Disclaimer

The Health Data Net cannot be held accountable for the accuracy of data, its confidentiality or authenticity in connection with electronic transmission, if the regulations stipulated have not been observed.

The Health Data Net cannot be held accountable for the correctness or quality of data provided by suppliers on the Health Data Net.

The Health Data Net cannot be held accountable in the event of either direct or indirect claims for compensation resulting from use of the Health Data Net. See the Health Data Net Agreement.

Agreements regarding the rights to services, information etc. which are accessible via the Health Data Net will be entered into with the holders of such rights.

6.3 Changes to these terms

The terms and regulations for connecting to the Health Data Net and use of it will be adjusted on an on-going basis.

Current terms for the Health Data Net will be made permanently available on the coming Web server.

It is the responsibility of stakeholders to remain informed of current terms and regulations at all times.