NHSnet—learning from academia

T J Roscoe, M Wells

The government white paper *The New NHS* has suggested that all general practices will be connected to NHSnet, the NHS computer network, by the year 2002.¹ NHSnet is a secure private network based on internet technologies. It will be the largest public sector project to connect computers in this country since the early 1980s, when the Joint Academic Network (JANET) was created by the universities and research councils. The policy decisions relating to security, networking products, and funding that were taken when JANET was created are pertinent to NHSnet and require deeper consideration and wider discussion.

Creation of JANET

The Computer Board for Universities and Research Councils was formed in 1966 in response to difficulties in funding computing resources in the tertiary education and research sector.² The board initially concentrated on funding computers in individual universities but increasingly came to focus on the provision of shared regional systems to allow access to large scale computing. The board also fostered the development of computer networks, primarily to provide access to powerful shared facilities that were being set up in the 1970s. In 1975 a working party recommended a rolling programme of investment in network services and the creation of a unit to oversee developments to facilitate networking.

With this encouragement, the academic sector in Britain developed a number of more or less separate networks, and by the early 1980s there was replication of provision—some sites had several connections while others had none. The research councils had established their own networks, which served their research establishments and some council funded groups in universities. Incompatibilities existed between the networking standards in use. To address these problems the computer board agreed in 1983 to fund a single national network to connect all the university and research council sites.

JANET came into formal existence on 1 April 1984 with the objective of providing a connection between the campus networks at each of the connected sites. It also provided onward links to other networks around the world, and a central support unit was established for the setting and development of network standards. It established a forum for discussion with end users as well as the computing services of universities and research councils.

The success of JANET is evidenced by the fact that the academic community now regards it as “part of the

Summary points

The Joint Academic Network (JANET) and the NHS network NHSnet are both large, widespread computer networks in the United Kingdom, and the lessons learnt in creating JANET should be considered for NHSnet

Policy decisions about security, connectivity, and finance have a great effect on the type of network that is created

Confidentiality is of paramount importance in NHS communications, and it is vital that NHSnet has secure safeguards built into it

Connecting a computer to thousands of others must make it less secure; security has to be the remit of end users

furniture.” There is an automatic presumption that computer systems will be connected to their local campus network. All staff and students of academic institutions have access to their campus network, and all campus networks are connected to JANET, and hence to the internet. Several hundred thousand users daily exchange many terabytes of data and access users on other networks around the world. The network carries traffic relating to every aspect of the work of universities and research councils.

Policy decisions underlying JANET

From the outset, the computer board made three major policy decisions relating to security, connectivity, and charging. These had a fundamental effect on the way JANET developed, and the NHSnet can learn from this experience.

Security—Managing security was delegated to the connected sites, and to those running end user systems at each site. JANET restricted the type of institution that could be connected to ensure that the public funds supporting the network were not being diverted to other purposes, but this was not related to security.

Connectivity—Every university and research council site was offered a connection to JANET. Those wishing to be connected were required to support a set of standard software products. This guaranteed that all sites were compatible and could work together freely.

Beighton Health
Centre, Sheffield
S20 1BJ

T J Roscoe,
informatics tutor,
Institute of General
Practice and Primary
Care

Department of
Physics, University
of Leeds, Leeds
LS2 9JT

M Wells,
emeritus professor

Correspondence to:
Dr Roscoe
troscoe@medical-
legal.co.uk

BMJ 1999;318:377-9

Conversion facilities to ensure that sites using these standards could communicate with other common standards in use at that time were provided.

Finance—Institutions were not charged for connection to JANET, nor were there charges relating to the amount of network traffic. All costs were met centrally from computer board funds.

Comparing networks

Costs

The table, which is based partly on published figures and partly on reasonable extrapolations, compares the potential costs and size of a national NHS network with those of JANET. The total annual costs of the two sectors differ by a factor of roughly four, although the numbers of users are broadly similar. JANET has connections to fewer sites, each with thousands of users, a highly developed campus network, and local expertise. The NHS sector also has a number of large sites (hospitals, health authorities, etc) with hundreds of users, good internal networks, and expertise. However, the NHS also includes at least 10 000 smaller sites—general practices, etc—each with fewer than 50 users and only a limited internal network and limited expertise. Providing connections between these sites and the NHSnet backbone will be costly not only in terms of equipment but also in effort.

The fundamental facts relating to the costs of providing and operating a network have not altered in the past 20 years. The total annual cost for any network is dominated by the standing charges for staff, lines, and switches. These costs are fixed, and reducing the number of messages passing through the network saves nothing. Equally, increasing the number of messages creates no additional costs, up to the point where network capacity must be increased by introducing faster lines and more powerful switches. In times of financial stringency, it is imperative that we make proper use of the investment.

Costs and structure of the Joint Academic Network (JANET) and national NHS computer network

	JANET	NHS network
Annual budget (£)	~10bn	~40bn
Annual costs of networking (£)	~60m	Not known
No of users	~1.2m	~1.0m
No of sites	~400 "universities"	~1000 "hospitals" ~10 000 "surgeries"
No of users at each site	1000-5000	100-500 in "hospitals" 10-50 in "surgeries"

"Universities"—universities and research council establishments.

"Hospitals"—hospitals, health authorities, and other large NHS establishments.

"Surgeries"—general practices.

Charging policies

When JANET was established, it was concluded that charging for connection or for use would be counterproductive for two reasons. Firstly, there is no better way of discouraging would be users from using a network than the imposition of charges, especially those related to use. Secondly, discussions with commercial network operators showed that accounting adds greatly to the difficulty and cost of creating and operating the network. A scheme for charging for use might treble the total cost of operating the network. Consequently, the policy was to provide free initial connections to sites. Current policy imposes charges that relate only to the speed (strictly the bandwidth) of the connection, and there are no charges for use except for access to transatlantic links.

In contrast, users of the NHSnet are charged for connection and for use. It is not yet clear what the scale of these charges will be, as this will depend on the volume of messages, and any discounts may be consequent on this volume. This is a major concern for individual general practices that are being asked to connect. As there is no choice about connection, we are being asked to sign up to an unknown future cost. The cost of administering charging is also not yet clear; as stated above, it may be uneconomic to do so and may discourage use. Most of the anticipated efficiency savings are likely to be in management and secondary care rather than primary care, although much of the work will take place in general practices.

Security issues

Major policy differences over security exist between the NHSnet and JANET. JANET does carry some sensitive traffic—some of it commercially valuable, some of it relating to named individuals—but the control of access to this data is the responsibility of those who send or receive the data. In the NHS sector security is important for everyone, and the whole NHSnet must provide a secure forum for information management restricted to those who are entitled to see it (see box). To facilitate this, potential sites must abide by a "code of connection."³ This requires that they must have set up systems for maintaining the security of information before they are connected to the network, and that their security is audited while they remain connected. All access to the network is subject to authentication at the time of use. The systems providing password protection are complex and are designed to ensure that breaches of security are unlikely.

The transmission of sensitive data requires the utmost respect for confidentiality. Confidentiality must be seen as a function of the end user systems and the

applications running on these systems, not as something that can be achieved by controlling access to the network. The creation of a secure private network to be used for confidential details creates a target for those seeking the information. Regulating and managing access to a network with 10 000 sites is never going to be easy. A network that can be accessed openly may be more subject to eavesdropping and to attempts at interference. However, the proper use of encryption and other cryptographic services would make it extremely difficult to interpret the contents of messages or to interfere successfully with traffic.

The end user systems, which, of course, include the staff operating these systems, must ensure that information in transit can be received or deciphered only by its intended recipient. This means that encryption will have to be used.

It is widely accepted that most security hazards arise from inside an organisation: a poorly trained individual may inadvertently leak information, and a malicious insider or one subject to coercion may deliberately leak it. Insiders can allow a leak more easily than an outsider can defeat a properly managed cryptographic system. Getting information from a paper medical record is already much easier than getting computer details. No computer system will be made more secure by connecting it to thousands of others, and if the systems to be connected are not adequately secure themselves then they should not be networked. We all need to be aware of the vital issues (and the code of connection should focus our minds in this respect), but it does not solve the problem. Proper training, continued vigilance, and the use of encryption is the key.

Current state of NHSnet messaging

Currently, few of the major NHS computer systems are connected, except on a local level. The only broad national information exchange is for data from health authorities sent centrally for mainly accounting administration purposes (the NHS-wide clearing system). Much of this is still being done by sending information on tapes by post or courier. It has recently been shown that more than 1 in 8 general practitioners are connected to the internet outside NHSnet. They are using it regularly to access a variety of sites, and internet technology is seen as acceptable to general practitioners for exchanging information.⁴ Messaging by email between parts of the NHS is still fairly localised and not used to its full potential. This contrasts with information gathering and messaging within NHS organisations, which are highly complex and well developed.

The hope of the white paper is that all general practices and all hospitals will be connected to NHSnet

Further information

- Information about NHSnet can be obtained from NHS Telecommunications Branch, 19 Calthorpe Road, Edgbaston, Birmingham B15 1RP
- For information on the NHSnet aimed at general practitioners, see <http://www.info-com.com/nhstb/ag/tfs/ds-4-i.html>.
- Information about JANET can be found at <http://www.ja.net/>

by 2002 and that they will use the network to transfer information ranging from individual referrals and discharges to that required for the planning of health care in its broadest sense for large populations. Most of the pilot projects for such information flows have been completed, and the problems have been identified and solved. Full implementation of many of these projects requires only that potential users be connected to the network. Although the use of information technology for messaging is accepted and the pilots are complete, there is a dearth of experts to implement the projects. Trying to roll out this complex messaging and information management to the whole NHS is going to be difficult and costly.

Currently, only a few hundred individual general practices (mainly in Scotland) are connected to NHSnet, although most health authorities and hospital trusts have some access. The technology exists to implement appropriate security management for each connected system or user, offering a secure means of transferring information and restricting access to information to authorised users. A major prerequisite is agreement as to what is to be provided, rather than the means by which it is to be implemented.

Conclusions

Creating a network on the scale of NHSnet will inevitably cost a great deal. It will take time for this cost to be recouped from savings or from efficiency gains, which will themselves be difficult to identify. There will also be appreciable security hazards if large numbers of poorly protected systems and applications come to rely on the network to provide security, especially when much of the risk to security comes from inside the NHS.

The success of JANET has shown that central funding and a national organisation that made the service free at the point of need led to a rapidly expanding network. This has been of inestimable use to the academic community. In effect, JANET carries all computer traffic for workers in this sector. Security issues were, and continue to be, the remit of the end users and their systems. Before NHSnet goes too far down its current intended path, these issues of funding and security need to be looked at again.

Funding: None.

Competing interest: None declared.

- 1 Department of Health. *The new NHS*. London: Stationery Office, 1997. (Cm 3807.)
- 2 Verdon FP, Wells M. Computing in British universities: the computer board 1966-1995. *Computer J* 1995;38:822-30.
- 3 NHS Executive Information Management Group. *NHS-wide networking*. London: NHS Executive, 1995. (IMGE5216.)
- 4 Roscoe TJ. Two surveys of internet use in primary care. *He@lth Information Internet* 1998;3:2-3.

(Accepted 6 October 1998)

NHSnet security policy

The policy aims to ensure that NHS information

- Is not disclosed to unauthorised people
- Is used only for the purpose for which it is intended
- Has not been modified accidentally or maliciously
- Is presented in the correct sequence for messaging applications (that is, presented in a way that existing applications can understand)
- Is available when required