



THE SCOTTISH OFFICE

NHS
MEL (1992)45

National Health Service in Scotland Management Executive

St. Andrew's House
Edinburgh EH1 3DG

Dear Colleague

COMPUTER SECURITY GUIDELINES

Summary

1. The Department's circular of August 1988 (SHHD/DGM(1988)47 refers) drew the attention of General Managers to CCTA guidance on internal controls and audit requirements as well as the need for contingency planning. At that time Boards were asked to consider the adequacy of the arrangements made by their own internal audit departments in such areas. More recently DIS has sponsored a general review of security across Scotland, and also a more detailed CRAMM (CCTA Risk Analysis and Management Method) study of one specimen Health Board, Teaching Hospital, and Computer Consortium. As a result I am now writing to notify you of the outcome of this work, to offer guidance in the form of the attached guidelines and to indicate what action is required.

Action

2. Boards/Units/Trusts are now asked to take the following action as soon as possible:-
 - 2.1 Responsibility for ensuring the security, integrity and resilience of computer based information systems rests with the General Manager or, for Trusts, with the Chief Executive. They must ensure that this responsibility is delegated clearly to a designated officer at a senior level who will be responsible for taking action.
 - 2.2 Adequate controlling and reporting structures must be put in place to ensure:-
 - (a) local reviews of systems etc are undertaken and problem areas identified.

16 September 1992

Circular SHHD/DGM

is cancelled

Addressees

For action:

General Managers,
Health Boards

General Manager,
Common Services Agency

General Manager, State
Hospital

Chief Executives, and
Chief Executive
Designate,
Trusts

For information

General Manager,
Health Education Board
for Scotland

To be copied to Unit
General Managers

Enquiries to:

Mr R Anderson
Technical Consultant
Health Systems Division
Keith House
2 Redheughs Rigg
South Gyle
EDINBURGH

Tel: 031-317-7577
Fax: 031-317-7467

- (b) resources and project timescales are properly controlled.

The guidelines which are attached for your use will assist in this process, but this is a significant task and adequate resources must be allocated.

- 2.3 Develop a programme of prioritised work to resolve any identified weaknesses from the review.
 - 2.4 Consider, in particular, contingency arrangements and requirements. DIS should be consulted about contingency arrangements once requirements have been identified.
 - 2.5 Assess training requirements. You may wish to consider the Information Training Initiative programme run by MDG (contact Shirley Watt telephone 031-332-2335) and take advantage as appropriate, or introduce other commercial security training as required.
 - 2.6 Exploit DIS initiatives such as Microcomputer Standards, COSECO Contingency Planning Package, and Disaster Standby mainframe at Maryfield.
 - 2.7 Review Audit facilities - medical systems can carry more potential risk than financial systems.
3. I am copying this letter and enclosure to your IT Director and to all Computer Centre Managers for their information.

Roles and Responsibilities

- 4. Boards/Trusts are responsible for the security of computer based information systems including access to data and contingency planning. DIS will provide advice and guidance where appropriate and ensure by periodic review that Boards/Trusts take the necessary protective action.

Review Findings and Way Ahead

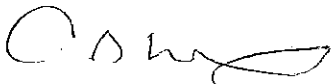
- 5. The key points established by the CRAMM study are summarised at Appendix 1. Given the increasing rate of uptake of computer based system, encouraged by the falling cost of PCs etc, we become increasingly vulnerable to systems failure and security breaches. This will have serious implications on the management of the service which depends more and more on ready access to information.
- 6. The attached IT Security Guidelines are designed to help managers responsible for IT systems to evaluate and improve their IT security. Further work is now being undertaken in DIS as a matter of urgency to establish an appropriate IT Security Policy and to define standards for use by the NHS in Scotland. An Awareness Campaign to raise the profile of Security is planned.

7. DIS intends to invite Board/Trust/Unit General Managers, and their senior officers designated as in para 2.1 above to a half day presentation to discuss the Security Review findings, and recommendations for the way forward.
3. DIS accepts that because of the importance of information systems security it would be acceptable for Boards/Trusts to use their existing CDCF/SIF allocations for 1992/93 to help meet some of the costs of resolving specific problems which they may identify during any security reviews. We are currently bidding for additional funds to be allocated for 1993/94 and will let you know the result in due course.

Boards/Trust Actions

9. In the view of the seriousness of some of the shortcomings identified during the DIS review of sites all Boards and Trusts should now examine their internal arrangements for:-
 - Security Reviews
 - Computer Auditing (in respect of both financial and medical systems)
 - Contingency Planning
 - Physical Security
 - Security Reporting
 - Offsite Systems Backup
 - Observing 'good practice' guidelines
 - Applying security standards (where they exist)
10. The Management Executive accept that addressing the above issues should be regarded as high priority in the national information strategy.
11. In future we will also require the inclusion of an appropriate section in each Board/Unit/Trust Information Strategy covering:-
 - Security Review procedures
 - Audit
 - Contingency Planning
 - Physical security

Yours sincerely



C B KNOX
Director of Information Services

DIS CRAMM STUDY

Key Points

- . Clincial Systems > Accounting Systems in value
- . Inadequate Mainframe contingency
- . Mini systems have no adequate contingency
- . Micro Systems lack control in acquistion and development.
- . Lack of Standards for IT Security
- . Lack of Awareness of IT Security
- . PICK Security exposure
- . General lack of physical security
- . IT security priority too low on budget.