Guidance regarding access to, and control of, information held on NIMS

Data protection and confidentially requirements in respect of NIMS users

Background

All organisations that use the National Incident Management System (NIMS) are legally required, under the Irish Data Protection Acts 1998 and 2003, to ensure the security and confidentially of the information held, or processed by them, on behalf of its employees, visitors, patients, service users, students, prisoners, members of the public, etc. The purpose of this guidance is to provide information concerning the obligations and responsibilities of both Delegated State Authorities (DSAs) and the SCA in the use and management of data on NIMS. Failure to adhere to these obligations and responsibilities may result in the unauthorised disclosure or theft of NIMS data, fraud, compromise an organisations objectives and or mandate and possible legal prosecutions or actions.

SCA Access Controls

The SCA as host of the system has implemented policies, procedures, and entered into commitments with DSAs to ensure that access controls are appropriate. In addition, all persons who receive NIMS related training from the SCA are briefed regarding requirements in respect of NIMS access controls in their organisation.

Secure Data by System Design

The NIMS is by design a very secure system. The following is in place to ensure the security of the data that is stored and processed on the system:

- NIMS is hosted on the Government VPN, which means it can only be accessed by users approved to have access to this network;
- The NIMS platform is designed such that there are a number of infrastructural security measures incorporated. A user is allocated access to the system based on their specific location and their requirement and role;
- User access can be limited on the basis of specific fields (i.e. specific pieces of information that are on the system);
- There is a full business continuity plan in place which allows for full recovery of all information in the case of emergencies or other non-normal conditions;
- NIMS is password protected and passwords are changed on a monthly basis;
- User accounts are automatically deactivated where users have not been active on NIMS for a period of two months.

Responsibility of DSAs using NIMS

It is the responsibility of DSAs to ensure persons and processes are in place within their organisation to ensure the following:

- Persons responsible for allocating access to NIMS must be at the appropriate level in the organisation. A formal process must be in place within your organisation and in conjunction with the SCA to ensure that access rights are appropriately allocated;
- Access rights privilege to NIMS should be allocated based on the specific requirements of a user's role and function rather than on their grading or status;
- The criteria used for granting access privilege to NIMS should be based on the principle of "least privilege" i.e. authorised users will only be granted a level of access to NIMS which is necessary for them to carry out the responsibilities of their role or function;
- Processes must be in place within your organisation to review user access level privileges at appropriate time intervals;
- Processes must be in place within the DSA, and in conjunction with the SCA, so that the SCA are notified where user privileges are to be revoked, in the event that the user moves to alternative work within your organisation or leaves your organisation. SCA are then responsible for acting on this notification and removing the user's access rights.

NIMS Reports and Information Sharing

Data protection and confidentially requirements must be adhered to at all times in the implementation, day to day access to, and management of reports from NIMS. Only those DSA employees with appropriate roles and functions should be given access to NIMS reports.

No information from NIMS may be shared or provided to a third party without the necessary legal basis, agreements, and consent in place, appropriate for the type of information that is being considered. Any information provided in terms of reports from the system should be appropriately protected and shared with appropriate members of your organisation only. Any information that is to be provided to third parties, particularly in respect of claims or incident data, should only be done so with the prior consent of the SCA and the appropriate person within your DSA who has responsibility for liaison with the SCA. Information in NIMS generated reports may be sensitive from the perspective of data protection, confidentiality, or commerciality.

Data Protection Bill 2017

In anticipation of the General Data Protection Regulation (GDPR), which is to be promulgated in 2018, the SCA is commencing a further detailed review of all data protection issues in respect of NIMS and its use. Further detailed guidance will be provided in respect of the outcome of this review in due course and it is intended there will be direct engagement with all DSAs who use NIMS to ensure both your organisation and the SCA fully comply with all data protection requirements in respect of NIMS.