Global Digital Health Partnership
Cyber Security Workstream

Proposed
Global eHealth Model Security Notice

EXECUTIVE SUMMARY

What is the Global eHealth Model Security Notice (MSN)?

The Global eHealth MSN is a voluntary, openly available resource to help health technology manufacturers and developers clearly convey information about their eHealth product's security controls to their customers and users. The content of the eHealth MSN enables greater transparency and help consumers make informed choices about the technologies that will hold their digital health information.

The eHealth MSN is a complement to an organization's existing Privacy Polices or Notices and expands on confidentiality safeguards by adding details that describe preserving the availability and integrity of the information.

The eHealth MSN provides plain language descriptions of security controls that are most commonly used to achieve these objectives. This content is not exhaustive, and efforts has been made to make this technical information apply to a broad range of audiences. Recognizing that some individuals will seek more information to support decision making, such as policy statements, the eHealth MSN represents a front door or introduction to the topic and should be regarded as important but integrated part of a layered approach to informed security decision-making.

Who is the MSN for?

Increasingly global health citizens are aware of security as an important part of the management of health information. They recognize the risks and have expectations about the safeguards that will put used to manage those risks.

For eHealth Technology Manufacturers/Developers: The eHealth MSN provides a mechanism to document security controls that have been implemented within their systems or services that retains, uses and/or shares individuals' health data. Leveraging this tool, the manufacturer and developer community will be able to provide meaningful and transparent information about their security design considerations.

For eHealth Systems or Service Customers/Users: The completed eHealth MSN will provide plain language descriptions of commonly used security controls to assist them in understanding implemented safeguards and guide in decision making.

Does the MSN meet legislative requirements?

While transparency is an important step in meeting legislative and regulatory compliance requirements, the eHealth MSN is part of a broader security program that should be in place.

Users of the eHealth MSN may also wish to consider the context in which they are operating, including any additional resources, guidelines or compliance requirements that may be applicable in addition to the base control information reflected.

This tool is not meant to be legal advice about all compliance obligations.

What should organizations consider in the implementation of the eHealth MSN?

Any implementation of the eHealth MSN should consider both the accuracy and completeness of the information in the context it is being used as well as the needs of the consumers of the notice.

This might include such steps as validating that the controls described are in place and functioning appropriately. This should also include consideration of the language preferences and accessibility needs of readers of the notice.

For example, in certain contexts, such as those relating to particularly sensitive health information, more detail regarding security controls to maintain confidentiality may be appropriate. In consumer facing applications, an emphasis on identity management and user access controls may be helpful.

In all instances, care should be taken to ensure that information is accurately and completely conveyed while ensuring readability of the information. For this reason, technical language had been reviewed and efforts made to avoid security jargon that is not known to a typical consumer.

As security is an evolving space and the appropriate and expected controls are not static, the eHealth MSN is expected to be reviewed at a regular basis to ensure it remains current and comprehensive.