GDHP WORKSTREAMS
Cyber Security

GLOBAL DIGITAL HEALTH
PARTNERSHIP

Global Digital Health Partnership
Cyber Security Workstream

Proposed
Global Digital Health Model Security Notice (Ver 3)

May 2023

INTRODUCTION: The Cyber Security Workstream focuses on strategies that can strengthen the processes and practices designed to protect healthcare related devices, systems, and networks, as well as the data within them, from security risks and cyber-attacks.

The Global Digital Health Model Security Notice (MSN) is being proposed as an openly available resource designed to help developers clearly convey information about their security policies to their users in one easily accessible resource. Like a standard Nutritional Facts Label, the Digital Health MSN provides a snapshot of a company's existing security practices, encouraging transparency and helping targeted consumers make informed choices when selecting products. The Digital Health MSN does not mandate specific policies or substitute for more comprehensive or detailed security policies but allows for documenting a company's standard security practices and applied security models or frameworks.

DEFINITIONS:

- **Security Notice Criteria**: A set of security measures to be addressed by developers, manufacturers or other Digital Health companies.
- **Implemented Safeguards**: Cyber Security measures that have been applied for specific Digital Health technologies.
- **Digital Health System or Service**: A generic term used for information and communication technology to support health and healthcare. Examples of Digital Health technologies may include mobile telemedicine, health monitoring and surveillance devices, mobile device applications that may be provided on patient monitoring devices, personal digital assistants (PDAs), laptops and more.

Color Code: Digital Health developers or manufacturers will provide information on their product's security policies and measures by completing the "Contact Details" and "Implemented Safeguards" sections of the MSN.

Blue Text: Form guidance language

Green Text: Prompts for additional information

Global Digital Health Model Security Notice Form

Sub-Sections	Manufacturer/Developer Contact Details
ConDe.1	• [Legal Entity Name] • [Digital Health Technology Name] • [Link (URL) to primary website] • [Link to full Security Policy] • [Link to Online Comment/Contact Form] • [Security Contact Name] • [Security Contact Email Address] • [Security Contact Phone Number] • [Address; *minimum, Country*]

SECTIONS:	SECURITY NOTICE CRITERIA	DIGITAL HEALTH SYSTEM OR SERVICE IMPLEMENTED SAFEGUARDS
Sub-Section	**Confidentiality Control:** This section describes what security controls are in place to keep customer/user data private.	

SECTIONS:	SECURITY NOTICE CRITERIA	DIGITAL HEALTH SYSTEM OR SERVICE IMPLEMENTED SAFEGUARDS
Con.1	**Authorization Control**: *the process of approving access a system or data.* How is access granted to authorized users?	• Responses should address: ☐ Authorization is granted by user identification and password ☐ Passwords are assigned to customers/users and can be modified as needed ☐ Access to system/data is controlled by customer/user roles and cannot be changed by the customer/user ☐ User Account reviews to identify valid accounts are conducted [Identify review frequency] ☐ [Approved Authority Role] is responsible for account request approvals ☐ Access is granted and controlled using an imbedded third-party (external technology, vendor or service provider) [Identify third-party provider] ☐ The policy or regulatory framework that defines authorization is publicly available here: [provide resource location] Additional Authorization controls *(optional), for example biometric access and/or passphrases*: [Open Text]
Con.2	**Access Control**: *the process of granting or restricting connection to a system or data.*	• Responses should address: ☐ Unique identifiers [user ID] are used to determine how and when customer/user information is accessed

SECTIONS:	SECURITY NOTICE CRITERIA	DIGITAL HEALTH SYSTEM OR SERVICE IMPLEMENTED SAFEGUARDS
	How is access to data controlled and monitored?	☐ Unique identifiers are used before access to data is permitted ☐ Authorization is granted and controlled using a third-party (external vendor or service provider) [Identify third-party provider]
Con.3	**Data Classification**: *the process of categorizing data by sensitivity level.* What is the classification of the data being stored, processed and/or transmitted?	• Responses should address: Describe the data classification of the data stored, processed and/or transmitted by the Digital Health technology: ☐ Personally Identifiable Information: [List applicable PII elements] ☐ Personal Health Information ☐ Electronic health records ☐ Administrative data ☐ Claims data ☐ Patient / Disease registries ☐ Health surveys ☐ Clinical trials data ☐ Claims and PII/PHI data are stored separately [If your organization uses third-party systems (external technology, vendor or service provider)] ☐ [Identify third-party provider]

SECTIONS:	SECURITY NOTICE CRITERIA	DIGITAL HEALTH SYSTEM OR SERVICE IMPLEMENTED SAFEGUARDS
		☐ Describe the level of sensitivity of the third-party resource: [Open Text]
Con.4	**Authentication**: *the process of determining whether someone or something is who or what it says it is.* How are users or systems authenticated before being granted access data?	• Responses should address: ☐ The Zero Trust Architecture Model is used This framework requires all users to be authenticated, authorized, and continuously validated. ☐ Two-Factor (2FA) or Multi-Factor Authentication (MFA) is used. (For example, biometrics, PIN numbers, or tokens) This authentication requires two or more forms of identification for access. ☐ Electronic access tokens are used Access tokens are required for electronic authentication to verify authenticity. ☐ Strong and complex usernames and passwords are used ☐ No default passwords are used If your organization uses additional or alternative methods of authentication. List here: [Open Text]
Sub-Section	**Integrity Control:** This section describes what security controls are in place to maintain the consistency and trustworthiness of customer/user data.	

SECTIONS:	SECURITY NOTICE CRITERIA	DIGITAL HEALTH SYSTEM OR SERVICE IMPLEMENTED SAFEGUARDS
Int.1	**Data Integrity**: *The process of confirming the overall accuracy, completeness, and consistency of data.* How is the overall accuracy of data maintained?	• Responses should address: ☐ Risk-based validation is performed on all information on a regular basis ☐ Back-ups of data are performed on a regular basis [Describe the frequency and duration] ☐ Duplicated data is removed ☐ Data validation techniques are in place and performed regularly, such as: ▪ Data type validation; ▪ Range and constraint validation; ▪ Code and cross-reference validation; ▪ Structured validation; and ▪ Consistency validation.
Int.2	**System Integrity**: *The process of guarding against improper system modification or destruction.* What controls are in place to protect against malicious code or other malware?	• Responses should address: ☐ Development included security processes This ensures that security is introduced early in the development process from initial design through delivery. ☐ Unknown applications or software are blocked from access ☐ External files or folders are blocked from access (For example, USB drives)

SECTIONS:	SECURITY NOTICE CRITERIA	DIGITAL HEALTH SYSTEM OR SERVICE IMPLEMENTED SAFEGUARDS
		Other: If your organization uses a third-party resource (external technology, vendor or service provider) ☐ [Identify third-party provider] [Open Text]
Sub-Section	**Availability:** This section describes what security controls are in place to ensure customer/user data is available with minimum interruptions.	
Ava.1	**Availability**: *The process ensuring timely and reliable access to and use of information.* What controls are in place to ensure the **system and data** will be available when needed?	• Responses should address: Data availability is maintained using: ☐ Patches are applied and tested on a regular basis ☐ Data formatting and processes have been streamlined to meet customer/user needs ☐ Monitoring is performed to identify corrupted data, which is removed when discovered ☐ System and data recovery times are performed as described in established Service Level Agreements *(where applicable)* ☐ Data redundancy is prioritized to improve availability ☐ Automated failovers are in place ensuring minimal to no downtime Data availability is protected from Denial of Service or Distributed Denial of Service attacks using the following security controls:

SECTIONS:	SECURITY NOTICE CRITERIA	DIGITAL HEALTH SYSTEM OR SERVICE IMPLEMENTED SAFEGUARDS
		[Open Text]
Sub-Section	**Transmission Security Control**: This section describes what security controls are in place to ensure how customer/user data is safely transmitted.	
Tra.1	**Transmission Control**: *The process of ensuring the secure sending or receiving of data.* What controls are in place to protect data being sent or received?	• Responses should address: ☐ Transmission security measures include: ▪ Email encryption ▪ Website encryption ▪ Secure File Transfer Protocol (SFTP) ▪ Secure Hypertext Transfer Protocol (HTTP or HTTPS) ☐ Encryption is compliant with the following standard(s): (Examples of encryption standards) ▪ ISO/IEC 18033-2:2006 (International Organization for Standardization/ International Electrotechnical Commission) ▪ Federal Information Processing Standards publication 140 (FIPS 140) Other: If your organization uses a third-party resource (external technology, vendor or service provider)

SECTIONS:	SECURITY NOTICE CRITERIA	DIGITAL HEALTH SYSTEM OR SERVICE IMPLEMENTED SAFEGUARDS
		☐ Security/Service Level Agreements or Data Exchange Agreements have been established with all external technology, vendor or service provider ☐ [Identify third-party providers]
Sub-Section	**Data Encryption:** This section describes what security controls are in place to protect customer/user data from unauthorized access.	
DaE.1	**Data Encryption**: *The process of converting human-readable plaintext into incomprehensible text.* What controls are in place to protect data from unauthorized access?	• Responses should address: • Data is transmitted through mobile application or medical device: ☐ Encryption is enabled by default ☐ User must enable encryption settings [Include link to instructions for enabling encryption] ☐ Data is not encrypted • Data is stored on internal servers or stored with a third-party system (external technology, vendor or service provider)]: ☐ [Identify third-party provider] ☐ Encryption is enabled by default ☐ Encryption can be enabled by request ☐ Data is not encrypted • Data is transmitted through the organization's network:

SECTIONS:	SECURITY NOTICE CRITERIA	DIGITAL HEALTH SYSTEM OR SERVICE IMPLEMENTED SAFEGUARDS
		☐ Encryption is enabled by default ☐ Encryption can be enabled by request ☐ Data is not encrypted
Sub-Section	**Organizational Security Policies** This section describes how customers/users are notified of changes in organizational security policies.	
Pol.1	• Responses should address: Describe how the changes to security policies are communicated to customers/users • Opt/In communications methods: ☐ Email ☐ Text messages ☐ Postal Mail • Continuous communication methods: ☐ Organization Website [Provide security policy link] • Other [Provide other communication methods] [Open Text]	
Sub-Section	**Organizational Breach Notification Process** This section describes how customers/users are notified of security breaches.	

SECTIONS:	SECURITY NOTICE CRITERIA	DIGITAL HEALTH SYSTEM OR SERVICE IMPLEMENTED SAFEGUARDS
Bre.1	• Responses should address: Describe how the organization communicates security breaches to customers/users • Opt/In communications methods: ☐ Email ☐ Text messages ☐ Postal Mail • Continuous communication methods: ☐ Organization Website [Provide security policy link] • Other [Provide other communication methods] [Open Text]	
Sub-Section	**Organizational Risk Management Methodology** This section describes what risk management standards the Digital Health technology organization complies with.	
Rmm.1	• Responses should address: Describe the risk management standards the organization complies with: (Examples of encryption standards) ☐ International Organization for Standardization (ISO) 31000 Risk Management Standards ☐ National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) ☐ International Medical Device Regulators Forum (IMDRF) risk categorization framework	

SECTIONS:	SECURITY NOTICE CRITERIA	DIGITAL HEALTH SYSTEM OR SERVICE IMPLEMENTED SAFEGUARDS
	☐ Organization for Economic Cooperation and Development (OECD) Recommendation on Digital Security Risk Management for Economic and Social Prosperity • Other [Provide other standards] ☐ [Open Text]	