DATA PRIVACY AND SECURITY

POLICY OF INDIAN HEALTH PORTAL

SECURITY OF ELECTRONIC HEALTH INFORMATION:

The Privacy Standards and the Security Standards are necessarily linked. Any health record system requires safeguards to ensure that the data is available when needed and that the information is not used, disclosed, accessed, altered, or deleted inappropriately while being stored or retrieved or transmitted. The Security Standards work together with the Privacy Standards to establish appropriate controls and protections. Health sector entities that are required to comply with the Privacy Standards must also comply with the Security Standards.

Organizations must consider several factors when adopting security measures. How a healthcare provider satisfies the security requirements and which technology it decides to use are business decisions left to the individual organizations. In deciding what security measures to adopt, an organization must consider its size, complexity, and capabilities; it's technical infrastructure, hardware, and software security capabilities; the cost of particular security measures; and the probability and degree of the potential risks to the ePHI it stores, retrieves and transmits.

PURPOSE OF THE SECURITY STANDARDS:

The security standards require healthcare providers to implement reasonable and appropriate administrative, physical, and technical safeguards to:

1. ensure the confidentiality, integrity, and availability of all the e-PHI they create, transmit, receive, or maintain
2. protect against reasonably anticipated threats or hazards to the security or integrity of their e-PHI
3. protect against uses or disclosures of the e-PHI that are not required or permitted under the Privacy Standards
4. ensure their workforce will comply with their security policies and procedures

SECURUTY TECHNICAL STANDARDS:

To protect the " INDIAN HEALTH PORTAL" handles by a healthcare provider, the provider must implement technical safeguards as part of its security plan. Technical safeguards refer to using technology to protect IHP by controlling access to it. Therefore, they must address the following standards, focusing on the functionalities thereof. It is worth noting that they will need to use an EHR/EMR solution that is able to successfully and robustly demonstrate the possession and working of these functionalities.

Authentication:

1. Locally within the system the fact that a person or entity seeking access to electronic health information is indeed the one as claimed and is also authorized to access such information must be verifiable.

2. Across the network, however extensive it might be, the fact that a person or entity seeking access to electronic health information across a network is the one claimed and is authorized to access such information in accordance with the standard specified in this document must be verifiable.

ALL RIGHT RESERVED INDIAN HEALTH PORTAL