

GOVERNMENT OF INDIA
MINISTRY OF HEALTH AND FAMILY WELFARE
DEPARTMENT OF HEALTH AND FAMILY WELFARE

RAJYA SABHA
UNSTARRED QUESTION No-2183
TO BE ANSWERED ON 08.08.2023

DATA CONCERNS IN DIGITAL HEALTH ECOSYSTEM

2183 SHRI BINOY VISWAM:

Will the Minister of **HEALTH and FAMILY WELFARE** be pleased to state:

- (a) whether there have been data leaks, fraud or theft reported through digital health ecosystems like CoWIN, e-Sanjeevani, Arogya setu etc, if so, the details thereof;
- (b) the details of the corrective actions taken by Government in response to these issues;
- (c) whether there has been a study on the efficiency of the use of Artificial Intelligence in protecting the initiative from data fraud and theft; and
- (d) whether there is a specified allocated budget to protect the Ayushman Bharat Digital Mission from data theft and fraud and if so, the details thereof?

ANSWER

THE MINISTER OF STATE IN THE MINISTRY OF HEALTH AND FAMILY WELFARE
(PROF. SATYA PAL SINGH BAGHEL)

(a) to (d)

Union Health Ministry has taken cognizance of the cyber incident in collaboration with Indian Computer Emergency Response Team (CERT-In) and coordinated incident response measures, which manages and operates digital applications like CoWIN, e-Sanjeevani, Arogya setu etc. app and database. These include:

- i. Advisories issued by CERT-In are disseminated to all authorised medical care entities / service providers in the country for compliance. These include advisories on:
 - Latest cyber threats/vulnerabilities & countermeasures,
 - Guidelines on information security practices for government entities & specifically for health,
 - Data & network security,
 - Identity and access management, application security, third-party outsourcing, hardening procedures, security monitoring, incident management and Security auditing.
- ii. On observing any cyber security incidents highlighted by CERT-In, remedial actions are taken as per direction and guidance of CERT-In.
- iii. Cyber security mock drills are conducted in consultation with CERT-In and NIC in all divisions of Union Health Ministry.
- iv. Regular training programmes conducted in collaboration with CERT-In, CDAC (Centre for Development of Advanced Computing) & National Informatics Centre (NIC) for sensitization of all the program divisions regarding securing the IT infrastructure and mitigating cyber-attacks.

- v. As per Security audit guidelines and advisories issued by NIC, necessary measures are taken by Union Health Ministry to enforce data security and privacy at web application end.
- vi. National Health Authority (NHA) has issued several guidelines and notification to govern the conduct of digital health applications, which are integrated with Ayushman Bharat Digital Mission (ABDM) ecosystem. These include Health Data Management Policy, Data Privacy Policy & ABDM Health Records (PHR) Mobile App Privacy Policy, which sets out the minimum standards for data privacy and protection.

Union Health Ministry has launched Ayushman Bharat Digital Mission (ABDM), which aims to develop the backbone necessary to support the integrated digital health infrastructure of the country and create longitudinal Electronic Health Record (EHR) for the citizen. Multiple registries are made to ensure that data silos can be broken and longitudinal electronic health record (EHR) of citizen is created under ABDM. Further, it will integrate innovative technologies such as Artificial Intelligence, IoTs, blockchain etc. with existing health IT applications as per need for improving the performance of the health services.

ABDM is a Central Sector Scheme with outlay of Rs. 1600 crore for 5 years from 2021-22 to 2025-26. To ensure the effective implementation of ABDM, the Union Health Ministry provides financial assistance to States/UTs for human resources, information education & communication (IEC), and capacity building including necessary handholding support to integrate state health digital health programs/solutions under ABDM ecosystem.
