GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 1857
TO BE ANSWERED ON: 04.08.2023

LEAKAGE OF COWIN DATA

1857. SHRI JAYANT CHAUDHARY:

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

(a) whether recently there was a report regarding the leakage of CoWin data and Ministry of Health and Family Welfare termed this news as baseless and mischievous, yet proposed to get the inquiry done by CERT-In;
(b) whether the Ministry of Electronics and Information Technology stated that there was no direct leakage of data and the present leakage news belongs to previous data hacking, thereby accepting the leakage, if so, the reasons for conflicting reports by two entities of Government;
(c) whether Delhi police has made some arrests from Bihar, in connection with hacking of data; and
(d) the measures Government will take to protect the privacy of citizens data?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI RAJEEV CHANDRASEKHAR)

(a) and (b): The Government is committed to ensure that the Internet in India is Safe & Trusted and Accountable for all users. With the expansion of the Internet and more and more Indians coming online, the possibility of cyber incidents have increased. Government is fully cognizant and aware of various cyber security threats.

Indian Computer Emergency Response Team (CERT-In)had taken cognizance of a telegram bot and alleged cyber incident and coordinated incident response measures with Ministry of Health & Family Welfare (MoHFW) which manages and operates CoWIN app and database. The MoHFW has lodged a complaint and F.I.R was registered by a law enforcement agency. CERT-In has provided inputs to facilitate investigation. Statements of Ministry of Electronics and Information Technology were based on the assessment of CERT-In of this reported cyber incident from time to time.

(c) and (d): Yes sir (based on inputs from Delhi Police).

As per the information provided by MoHFW, Co-WIN portal of Ministry of Health & Family Welfare already has necessary security measures and adequate safeguards for data privacy. The measures taken to protect the privacy of citizens data are as follows:

(i) Beneficiary to access vaccination details by registered mobile number through OTP authentication only.
(ii) Mobile Numbers, Aadhaar Number & other Photo ID Card numbers of beneficiary are masked. Only last 4 characters are visible to users (service providers) of Co-WIN.
(iii) Complete Co-WIN database is encrypted using “Encryption Algorithm” key to protect citizen data and data integrity is maintained for all vital information.
(iv) Two factor authentication feature (Password & OTP) while login by the users (service providers) is put in place restricting unauthorised access to Co-WIN.

Government has taken following measures to enhance the cyber security posture and prevent data breaches:

(i) On observing the data breaches and data leaks, CERT-In notifies the affected organisations along with remedial actions to be taken. CERT-In coordinates incident response measures with affected organisations, service providers, respective sector regulators as well as law enforcement agencies.

(ii) CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers, networks and data on an ongoing basis.

(iii) A special advisory on security practices to enhance resilience of health sector entities has been communicated by CERT-In to the Ministry of Health and Family Welfare, for sensitising health sector entities regarding latest cyber security threats in December 2022. The Ministry has been requested to disseminate the advisory among all authorised medical care entities / service providers in the country.

(iv) CERT-In has issued guidelines on information security practices for government entities in June 2023 covering domains such as data security, network security, identity and access management, application security, third-party outsourcing, hardening procedures, security monitoring, incident management and security auditing.

(v) CERT-In operates the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) to detect malicious programs and free tools to remove the same and to provide cyber security tips and best practices for citizens and organisations

(vi) Security tips have been published for users to secure their desktops and mobile phones and to prevent phishing attacks.

(vii) To protect personal data of users, the Central Government, in exercise of its powers under the Information Technology (IT) Act, 2000, has prescribed reasonable security practices and procedures and sensitive personal data or information through the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

These include the requirement that any person collecting, receiving, possessing, storing, dealing or handling information provided should publish on its website a policy for privacy and disclosure of personal information, that such person use the information collected for the purpose for which it was collected and keep it secure, that disclosure of sensitive personal data be done with prior permission of the information provider, that sensitive personal data or information not be published, and that a third party receiving sensitive personal data or information shall not disclose it further.

(viii) Section 72A of the IT Act provides for punishment for disclosure of information in breach of the lawful contract. It provides that any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both.

(ix) In order to protect the privacy of the citizen data, The Ministry of Electronics and Information Technology has prepared a draft Bill, titled 'The Digital Personal Data Protection Bill, 2022'.A copy of the draft Bill is available on https://www.meity.gov.in/content/digital-personal-data-protection-bill-2022. The draft Bill sets out the rights and duties of the citizen (Digital Nagrik) and the obligations of the Data Fiduciary for protecting the same, thereby empowering the citizen to secure data privacy.

****