GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 2932
TO BE ANSWERED ON: 20.12.2024

CYBERSECURITY OF THE INSURANCE SECTOR

2932. SHRI MANOJ KUMAR JHA:

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

(a) whether Government is aware of the data breach involving 3.1 crore customers of health insurance companies, if so, the details thereof;
(b) whether any regulatory actions have been initiated against such companies for the breach, if so, the details thereof;
(c) the measures being taken to enhance cybersecurity in the insurance sector to prevent such breach in future; and
(d) whether Government plans to introduce stricter penalties and accountability frameworks for companies failing to secure customer data, if so, the details thereof?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI JITIN PRASADA)

(a) to (d): Government is fully cognizant and aware of cyber threats and challenges including those of insurance sector. Government is committed to ensure an open, safe, trusted and accountable internet for its users and has taken several key initiatives aimed at safeguarding personal data of the citizens which, inter alia, includes:

i. The Indian Computer Emergency Response Team (CERT-In) is designated as the national agency for responding to cyber security incidents under the provisions of section 70B of the Information Technology Act, 2000.
ii. On reporting of cyber security incident by a private sector health insurance company to CERT-In in August 2024, CERT-In coordinated incident response measures with concerned organisation and service providers.
iii. The Insurance Regulatory and Development Authority of India (IRDAI) has issued Guidelines on Information and Cyber Security dated 24th April 2024, for protecting the information assets of all regulated entities including Insurers, Brokers, corporate agents etc. in order to enable the insurance industry to strengthen their defenses to deal with emerging cyber threats. The guideline is periodically updated to address evolving cyber security challenges.
iv. IRDAI has issued advisories to all Insurance companies on modus operandi, techniques, tactics and procedure (TTP) and recommended action to protect the information assets of Insurers.
v. IRDAI seeks comprehensive response of the Insurer/s regarding the cyber security incidents. On the basis of severity of cyber security incident, insurers are directed to conduct a comprehensive audit of entire IT landscape by an independent auditor.
vi. National Cyber Coordination Centre (NCCC) implemented by the CERT-In serves as the control room to scan the cyberspace in the country and detect cyber security threats. NCCC facilitates coordination among different agencies by sharing with them the metadata from cyberspace for taking actions to mitigate cyber security threats.
vii. CERT-In has issued an advisory in November 2023 to various Ministries outlining the measures to be taken for strengthening the cyber security by all entities that are processing the digital personal data or information including sensitive personal data or information.
viii. 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.

ix. In order to ensure data protection, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal data or Information) Rules, 2011 ('SPDI Rules') mandates reasonable security practices and procedures for compliant body corporate or any person on its behalf, handling sensitive personal data or information. Body corporate or any person on its behalf shall obtain written consent from the provider of such information regarding lawful purpose of usage before collection of such information.

x. In order to safeguard the personal data of individuals and ensure that their data is shared only with their consent, the Digital Personal Data Protection Act, 2023 (DPDP Act) has been enacted. The DPDP Act is aimed at safeguarding the personal data of individuals and ensuring processing of personal data for the lawful purposes. As per the Act, appropriate technical and organisational measures must be implemented for processing of the personal data and reasonable security safeguards must be taken to prevent any personal data breach. Further, in the event of any such breach or complaint by the Data Principal with respect to exercise of her rights, the Data Protection Board after an inquiry, may impose monetary penalty as per the provisions of the Act. The Act prescribes different monetary penalties for different types of breaches of the Act, with the maximum penalty upto two hundred and fifty crore rupees.

****