GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 564
TO BE ANSWERED ON: 23.07.2025

DATA BREACH BY STAR HEALTH ALLIANCE

564. DR. BACHHAV SHOBHA DINESH:

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:
(a) whether the Government has taken cognisance of the fact that there was a data breach by Star Health and Allied Insurance which led to highly sensitive personal information including names, phone numbers, residences, tax information, ID copies, test results and diagnoses of Star Health customers being shared on Telegram;
(b) whether as per the Section 70B of the Information Technology Act, the national cyber agency Indian Computer Emergency Response Team (CERT-In) has initiated a probe into the data breach and if so, the details thereof including findings of the investigation;
(c) whether the Government has initiated any punitive action against those responsible for the cause and if so, the details thereof;
(d) whether the rules under the Digital Personal Data Protection Act, 2023, have been notified and if so, the details thereof; and
(e) whether the Government has formulated concrete policies to ensure prevention of such incidents in the future and if so, the details thereof?

ANSWER

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

(a) to (e): In August 2024, Indian Computer Emergency Response Team (CERT-In) received a report regarding data breach at Star Health and Allied Insurance. CERT-In notified the affected organisation along with remedial actions to be taken, and coordinated further incident response measures. CERT-In has sent the details of the technical analysis to Tamil Nadu Police for further investigation.

Government remains cognizant and aware of cyber threats and challenges including those of insurance sector. Following measures have been taken to strengthen cybersecurity in the country:

- 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.
- National Cyber Coordination Centre (NCCC) project is being implemented by CERT-In. NCCC examines the cyberspace to detect cyber security threats. It shares the information with concerned organizations, state governments and stakeholder agencies for taking action.

- CERT-In works with other agencies involved in ensuring cybersecurity including Telecom Security Operations Centre (TSOC), India Cyber Crime Coordination Centre (I4C), National Centre Information Infrastructure Protection Centre (NCIIPC), etc.
- CERT-In along with other agencies was able to successfully prevent cyber-attacks during the G20 summit, Parliament 20 summit, Ram Janmabhoomi event, Maha Kumbh etc.
- Regular training workshops are conducted for cybersecurity professionals, government employees, police and law enforcement professionals, lawyers and public prosecutors, students, etc.
- The Insurance Regulatory and Development Authority of India (IRDAI) also issues cybersecurity guidelines for regulated entities including insurers, brokers, corporate agents, etc.
- CERT-In operates an automated cyber threat intelligence exchange platform for sharing tailored alerts with organisations across sectors for proactive threat mitigation.
- Cyber security mock drills are conducted regularly to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors

Legal provisions:

- 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 body corporate or any person on its behalf, handling sensitive personal data or information.
- 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.

******