Plug the breach

Posted at: 19/12/2023

Introduction:
About two months after intelligence agencies reported that personal details of more than 80 crore people had been leaked from the ICMR website and put on sale on the dark web, the Delhi Police has arrested four persons.

Severity of the leak:

1. Leak included sensitive data like Aadhaar, phone numbers, passport details, and health records.
2. These are not just personal identifiers but keys that can unlock information on financial transactions, personal communications and medical details.
3. The breach also raises concerns about privacy violations.

How digital healthcare data can help?

1. The utility of digital systems in healthcare was demonstrated during the Covid vaccination drive.
2. Electronic repositories of patients' medical histories, diagnoses, treatments and other healthcare information can lead to quicker diagnosis, better treatment decisions, and improved safety standards.
3. The Centre's initiatives including the Ayushman Bharat Digital Mission have brought digital healthcare to the centre stage.
4. It operates on the principle of a federated architecture — data isn't stored in a single repository but information flows between all participants in the system.

Two biggest breach of healthcare data in recent time:

Last year, a ransomware attack on the AIIMS servers pushed the top government hospital in the capital to shift a large part of its operations to the manual mode for almost two weeks. The data was reportedly repopulated into the hospital's systems.
The NHS in the UK has suffered several attacks in recent times. In July, it lost 70 terabytes of sensitive information in a ransomware attack.

Laws to Protect healthcare system from data Breach (Globally):

1. The UK's Data Protection Act enjoins health service providers to inform people if their data is compromised.
2. In the US, the Health Insurance Portability and Accountability Act requires regulated entities to comply with its breach notification rules.
3. These laws have, by all accounts, not made systems foolproof.
4. But they are a part of an ongoing process to make healthcare repositories more secure.

What more can be done to save healthcare data from data breaches?
Technical measures:

1. Data encryption: Implementing robust encryption at rest and in transit ensures unauthorized access is difficult even if a breach occurs.
2. Access control: Granting access to sensitive data only to authorized personnel with the minimum necessary privileges reduces the attack surface.
3. Logging and monitoring: Continuously monitoring system activity and logging user actions can help detect suspicious behavior and investigate potential breaches quickly.
4. Regular backups and disaster recovery: Regularly backing up data and having a robust disaster recovery plan in place allows for quick restoration in case of a breach.
5. Software updates: Keeping software and systems up-to-date with the latest security patches helps address vulnerabilities exploited by attackers.
6. Security awareness training: Educating healthcare personnel about cybersecurity best practices can help prevent human error-related breaches.

Policy measures:

1. Strong data protection laws: India's recently introduced Data Protection Act needs to be fine-tuned to address the specific challenges of securing health-related information. This includes stricter breach notification requirements, data minimization principles, and robust enforcement mechanisms.
2. Standardized security protocols: Establishing and enforcing national standards for healthcare data security practices across hospitals, clinics, and other healthcare providers can ensure consistency and effectiveness.
3. Cybersecurity infrastructure: Investing in national cyber defense capabilities and fostering collaboration between law enforcement agencies, policymakers, and the healthcare sector can strengthen the overall response to cyber threats.
4. International cooperation: Sharing best practices and collaborating with other countries facing similar challenges can help develop effective solutions and stay ahead of evolving cyber threats.

Additional measures:

1. Focus on user privacy: Building trust with patients by ensuring transparency about data practices and providing them with control over their health information can reduce vulnerability to exploitation.
2. Promoting cybersecurity awareness: Public awareness campaigns can educate individuals about protecting their health data online and encourage safer practices.

Conclusion:

India’s recently introduced Data Protection Act has been criticised for being insensitive to the demands of securing health-related information. The attack on ICMR should push policymakers to make systems more robust