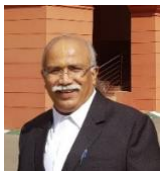
Remedies on Privacy Breach – A Case Study of Star Health Insurance

By M.G. Kodandaram, IRS.
Assistant Director (Retd.),
ADVOCATE and CONSULTANT



Introduction

In the digital age, cybersecurity incidents and data breaches have become increasingly prevalent. Sensitive personal information is continually at risk, especially for organizations handling vast amounts of personal data, such as healthcare providers and insurers. One such incident occurred with Star Health and Allied Insurance, (reported https://www.livemint.com/companies/news/star-health-insurance-under-cyberattack-says-operations-unaffected-even-after-data-leak-11728489332453.html) one of India's largest health insurance firms, which recently faced a significant data breach. Alleged sensitive customer data, including medical records, was leaked online, raising critical concerns about **privacy, security, and accountability**.

In the digital age, the protection of personal data is a fundamental right tied to the privacy of individuals. With the increasing reliance on digital platforms to store, process, and share sensitive information, data breaches pose significant threats to the privacy and security of citizens. Such breaches victimize the Data Principals - the individuals to whom the data belongs - by exposing their personal information to unauthorized access, misuse, and exploitation. The breach involving Star Health and Allied Insurance highlights the pressing need for stringent legal frameworks to safeguard individuals' personal data from malicious actors and organizational negligence.

This article seeks to examine the legal protections available to Indian citizens in cases of privacy breaches that affect individuals and harm the data principal. The analysis focuses on the current legal framework under Section 43A of the Information Technology Act, 2000,

alongside the upcoming Digital Personal Data Protection Act, 2023, which is yet to come into force. This comparison aims to provide a clearer understanding of the evolving privacy protection legal landscape in India.

Background of the Incident

Star Health and Allied Insurance, based in Chennai, India, has insured over 170 million individuals to date. During October 2024, it was revealed that a hacker group had infiltrated the company's systems and leaked sensitive customer data, including medical reports, insurance claims, tax details, and copies of identification cards. The data breach became public when the hacker group created Telegram chatbots to distribute this personal information. Additionally, the group set up a website to host the leaked data, which, according to TechCrunch, included a video allegedly showing conversations between Star Health's Chief Information Security Officer (CISO) and the hackers.

The breach was massive, involving the exposure of customer medical records and financial information, which are considered among the most sensitive types of personal data. This incident not only threatened individual privacy but also called into question the strength of cybersecurity practices at large institutions such as Star Health.

Privacy and Data Protection Concerns

The nature of the data exposed in the Star Health breach emphasizes the grave privacy concerns for customers. Personal data like medical records, home addresses, insurance claims, and tax details can have serious implications when leaked publicly along with the identity of the individual. Such information can be misused for identity theft, financial fraud, and even targeted attacks on individuals. Moreover, the exposure of medical history can cause personal embarrassment, societal stigmatization, or discrimination in certain cases, raising the stakes significantly for the victims. From a legal perspective, data breaches of this magnitude will certainly fall under national data protection laws.

In India, the *Information Technology Act, 2000* (*amended in 2008*) (*herein after IT Act 2000 for brevity)* and *The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011* (*IT Rules, 2011*) provide frameworks

for protecting '*sensitive personal data'*. However, India's data protection regime has historically been weaker, both in legislation and administration - than those of other jurisdictions like the European Union's *General Data Protection Regulation (GDPR)*. The Star Health incident highlights the need for stronger and more comprehensive data protection regulations in India, particularly as personal data handling becomes increasingly complex.

Cybersecurity Vulnerabilities and Organizational Accountability

This incident brings to light critical questions about Star Health's cybersecurity infrastructure. For an organization of its size - providing insurance to millions and processing claims worth billions - a robust cybersecurity system is essential. The fact that a hacker group could gain access to such sensitive data and share it online indicates a significant lapse in security protocols. The company's response, which included initiating a forensic investigation, suggests an attempt to address the issue. However, the damage to its reputation may already be done.

Organizations handling sensitive data have a responsibility to ensure adequate protection against cyber threats. In this case, Star Health's breach appears to stem from inadequate cybersecurity measures, which allowed the hacker group to infiltrate its systems and extract valuable data. The delay in notifying customers or providing detailed public communication further compounds the issue, as transparency and prompt disclosure are critical components of responsible data breach management.

Moreover, incidents like this highlight the need for greater collaboration between the public and private sectors in addressing cyber threats. India's *Computer Emergency Response Team (CERT-In)* has been involved in the response, but its ability to address breaches effectively and swiftly is contingent on better cooperation with private companies. A more integrated approach to national cybersecurity could help prevent such incidents from happening in the future.

The Role of Third Parties: Telegram and Cloudflare

Another dimension of this case involves the role of third parties, such as Telegram and Cloudflare, in facilitating the breach's dissemination. The hacker group used Telegram chatbots to leak customer information, while Cloudflare was allegedly hosting the group's website. Star Health responded by filing a lawsuit against both companies, leading to interim court orders

restricting their platforms from being used for these purposes. Telegram and Cloudflare's involvement raises broader questions about the accountability of tech platforms when they are exploited for illegal purposes. While platforms like Telegram offer privacy-focused communication services, this can also make them a haven for malicious actors. Cloudflare, a content delivery and web security provider, might also find itself in a difficult position when its services are misused for hosting illegal content. Although both companies may claim they are not directly responsible for the breach, the incident raises questions about their roles in ensuring that their platforms are not used to further such criminal activities.

Section 43A of the Information Technology Act

Section 43A of *the IT Act 2000* specifically deals with the protection of sensitive personal data. It imposes a liability on corporate bodies that possess, deal with, or handle sensitive personal information to implement "*reasonable security practices and procedures*." It mandates compensation to individuals if their personal information is compromised due to the organization's negligence in maintaining these security standards. *The IT Rules, 2011* provide the framework for implementing Section 43A. These rules set out how sensitive personal data should be handled and define "reasonable security practices," which include **internationally recognized security standards such as ISO/IEC 27001.**

In the Star Health case, the privacy breach involving the leakage of policyholders' personal information directly implicates the company's responsibilities under Section 43A. The crucial legal issues under this section are:

- **Failure of Security Practices:** The breach raises questions about whether Star Health implemented adequate "*reasonable security practices*" to protect the sensitive health data of its customers. Given the scale of the breach and the sophisticated methods employed by the hackers, it is likely that Star Health's cybersecurity systems were inadequate to meet the standards required under the IT Act (standards such as ISO/IEC 27001).
- **Negligence in Data Protection:** If it is established that Star Health was negligent in safeguarding this data, affected individuals could seek compensation under Section 43A. Negligence, in this case, would be the failure to deploy adequate cybersecurity measures, failure to encrypt sensitive data, or not promptly addressing known vulnerabilities in their data systems. From the available information the negligence is evident as the insiders are also have a vital role in causing this privacy breach.

- **Sensitive Personal Data:** The term "*sensitive personal data*" includes a broad range of information such as financial information (bank account details, credit card information, etc.), passwords, health conditions, sexual orientation, and medical records, Biometric information, or any other data that is prescribed to be sensitive in nature. In this context, medical records and insurance claims clearly fall within this category, making the invocation of Section 43A particularly pertinent, as the protection of such data is essential under these provisions.
- **Compensation for Damages:** Under Section 43A, individuals whose sensitive personal data has been compromised can file a claim for compensation against Star Health. The company may be held liable for failing to implement reasonable security practices and for any resulting losses. The extent of compensation is determined by the adjudicating officers under the IT Act, and there is no upper limit specified under the law.

Affected individuals can file a complaint with the Adjudicating Officer appointed under the IT Act. The officer has the authority to inquire into the complaint and direct the company to pay compensation if found liable for negligence in protecting sensitive personal data. As on date the performance of these adjudicators is not at all dependable and useful. The adjudicating officer has the authority to decide on the quantum of compensation based on the nature and extent of the damage caused to the victim. For large-scale breaches like the one at Star Health, involving sensitive health data, the compensation could potentially be significant, reflecting the severity of the impact on individuals' privacy and well-being.

Reliefs under the DPDP Act, 2023

The *Digital Personal Data Protection Act, 2023 (DPDP Act*) is enacted to provide comprehensive protection to individuals' digital personal data and ensure the responsible handling of personal data by organizations. The Act recognizes two primary stakeholders: (i) Data Principals: The individuals to whom the personal data relates (e.g., Star Health's policyholders) and (ii) Data Fiduciaries: The organizations or entities that collect, process, and store personal data (Star Health). The data breach involving Star Health, where sensitive personal information such as full names, medical records, insurance claims, and ID cards were leaked, triggers several provisions of the DPDP Act. It is to be noted that the term 'sensitive personal data' has no specific inclusion in the said law. The legal requirement of the fiduciary under the said law in brief are:

a) **Obligations of Data Fiduciaries:** Under the DPDP Act, organizations that collect and process personal data have clear obligations:

- Data Security: Data Fiduciaries must take adequate security measures to protect personal data from unauthorized access, breaches, or misuse. This includes deploying robust cybersecurity practices.
- Purpose Limitation: Personal data should be processed only for specific, clear, and lawful purposes. Star Health must ensure that data collected for providing health insurance services is not exposed to unintended risks.
- Data Minimization: Only the data that is necessary for fulfilling the purpose for which it was collected should be processed.

In the case of Star Health, the breach suggests a failure in securing personal data, which could indicate non-compliance with these key obligations.

b) **Consent Requirements:** The DPDP Act mandates that data processing must be based on the consent of the data principal. Data Fiduciaries are responsible for ensuring that the consent is:

- **Informed:** The Data Principal should be made aware of what data is being collected and how it will be used.
- **Specific:** Consent should be specific to a particular purpose.
- **Withdrawable:** The Data Principal has the right to withdraw consent at any time.

For Star Health, if policyholders were not informed about how their personal data would be handled or secured, or if they were unaware of potential security risks, this could be a violation of the DPDP Act's consent requirements.

c) **Data Breach Notification:** One of the most critical aspects of the DPDP Act is the mandatory breach notification requirement. In case of a data breach, the Data Fiduciary (in this case, Star Health) must notify the Data Protection Board of India (DPBI) and the affected Individuals (policyholders) about the breach, outlining the nature of the breach, the data involved, and steps being taken to mitigate harm. This provision ensures that affected individuals can take immediate action to protect themselves from identity theft, financial loss, or further exploitation of their data.

d) Penalties for Non-Compliance: The DPDP Act imposes stringent penalties on organizations that fail to comply with the law. Under Chapter 10 of the Act, heavy financial

penalties can be levied for violations, including failure to Implement Security Measures. If Star Health is found negligent in safeguarding its customers' personal data, it could face significant fines. Penalties can go up to ₹250 crore for data breaches involving sensitive personal information. If Star Health failed to promptly notify the authorities or its customers about the breach, it may incur additional penalties. These financial penalties are designed to act as a deterrent and to ensure that organizations treat data security as a priority.

The DPDP Act establishes the Data Protection Board of India (DPBI) to ensure compliance with data protection regulations and to address complaints and grievances related to data breaches. The DPBI has the authority to☹i) Investigate breaches and incidents of non-compliance. (ii) Impose fines and penalties on organizations that violate data protection laws. (iii) Provide guidance on best practices for data security. In this case of breach, affected individuals can approach the DPBI to seek redressal, while the DPBI could independently initiate an inquiry into the incident, especially given the scale and severity of the breach.

(e) Right to Grievance Redressal: Data Principals can lodge a complaint with the Data Protection Board of India (DPBI) if they believe that their personal data has been mishandled or if the Data Fiduciary (Star Health) has not complied with its obligations under the law.
There is no scope for the victims to seek any damages to the any type of harm caused.
Broader Implications for Data Privacy in India.

The Way Forward

The breach at Star Health is a wake-up call for the broader Indian industry regarding cybersecurity and data privacy. As more companies digitize their operations, they must be prepared for the growing threat of cyberattacks, particularly in sectors like healthcare, which handle highly sensitive data. This incident should encourage organizations to strengthen their cybersecurity infrastructure, implement stricter data protection measures, and ensure compliance with the forthcoming Digital Personal Data Protection Act (DPDP Act) 2023.

While the legal protections available to Indian citizens for data breaches have evolved from Section 43A of the IT Act to the DPDP Act, the latter presents both strengths and weaknesses. Section 43A provided a foundational mechanism for seeking compensation in cases of

negligence, whereas the DPDP Act offers greater accountability for companies and empowers individuals with more control over their personal data. However, the DPDP Act falls short in its aim to fully protect citizens' privacy rights, particularly in terms of providing adequate redress for victims of breaches. There is a pressing need for more robust laws to ensure that the privacy of individuals is properly safeguarded in this digital age.

By M.G. Kodandaram, IRS.
Assistant Director (Retd.),
ADVOCATE and CONSULTANT