SBC Medical Group Discloses Breach Affecting Over 2 Million People in Japan



SBC Medical Group told the SEC that attackers accessed an online platform it manages and stole personal and some medical data tied to clinics in Japan. A separate incident at the reservation service Tribeau exposed data of about 19,000 people.

- Basic data of 1,624,000 individuals was stolen, including names, contact details, dates of birth, patient card numbers, member IDs and survey responses.
- Smaller groups also lost reservation requests, web form content, treatment descriptions, image file names and review text; credit card data was affected for 14 people, all cards unable to process further payments.
- Customer passwords and 20,000 employee records with names, IDs and passwords were taken; 459 employees had bank, pension and tax documents affected.

- A separate breach of third-party service Tribeau exposed administrator accounts and data of about 19,000 people.
- The company says both incidents are remediated: the affected server was isolated, attackers removed and Tribeau passwords rotated.

SBC Medical Group Holdings, a California-based company that provides consulting, management and operational support to medical corporations and clinics, has disclosed in an SEC filing a breach affecting more than 2 million people in Japan.

What happened

Attackers accessed an online platform managed by the company and compromised databases holding customer information linked to certain clinics. The investigation is ongoing, but the company has confirmed that personal and medical information was likely compromised.

The largest set covers 1,624,000 individuals whose names, addresses, phone numbers, emails, dates of birth, gender, patient card numbers, member IDs and survey responses were stolen. Other groups lost reservation requests (255,416), web inquiry form content (217,769), treatment descriptions and image file names (4,513) and review text with treatment names (15,007). Credit card data of 14 people was affected, though the company says those cards could no longer process payments.

Customer passwords and 20,000 employee records containing names, IDs and passwords were also stolen. For 459 employees, onboarding documents such as bank, pension and tax forms were affected.

The third-party incident

In a separate case, attackers reached administrator accounts at the reservation service Tribeau and accessed data on about 19,000 people. The operator states that email and residential addresses, card data, passwords and electronic medical records were not part of that incident.

SBC Medical Group says both incidents are remediated. It isolated the affected server, removed the attackers and rotated passwords for all clinics it manages on Tribeau. It is still assessing the business and financial impact.

Why it matters for Saudi institutions

The case shows how a management platform, a reservation vendor and employee records can all become exposure points at once. Healthcare providers and their service partners in the Kingdom hold similar data and should review their own controls.

What to do now

1. Inventory online platforms and third-party booking or patient-engagement services that hold patient or customer data, and confirm their owners.
2. Review administrator accounts on vendor platforms: enforce MFA, remove unused accounts and rotate credentials after any vendor incident.
3. Check that passwords are stored with strong hashing and that staff and customer credentials are not reused across systems.
4. Limit retention of sensitive HR documents, such as bank and tax records, and restrict access to them.
5. Confirm that your incident response plan covers PDPL breach assessment and notification, including vendor-originated incidents.
6. Require vendors to notify you promptly of incidents and to share root-cause findings.