A Brief Chronology of Cyberattacks on Plastic Surgery Practices

- DataBreaches.net

The following is a partial chronology of cyberattacks on plastic surgery practices. It does not include leaks of data due to human error or other types of incidents.

2017

- **Plastic Surgery Associates of South Dakota** reported a ransomware attack that affected more than 10,000 patients. In October 2024, HHS OCR settled charges against the entity for violating the HIPAA Security Rule for a $500,000 monetary penalty and a corrective action plan.
- Lithuanian plastic surgery clinic **Grožio Chirurgija** was hacked, and sensitive patient data was posted online. Individual files were listed for sale between €50 and €2,000 each, or €344,000 for all of the data.
- **London Bridge Plastic Surgery** in the U.K. was attacked by thedarkoverlord (TDO). The clinic reportedly negotiated a payment, but it wasn't enough to satisfy TDO, who later tried to extort the patients directly.

2018

- TDO attacked the **AZ Plastic Surgery Center** in Arizona. When Dr. Spies refused to pay them, they started leaking identifiable patient data, including photos. HHS records indicate that 5,524 patients were affected.

2019

- **The Center for Facial Restoration** in Florida received an extortion demand from the threat actor(s) who had exfiltrated patient data. When the doctor didn't pay, the threat actor(s) started contacting patients directly. The incident affected 3,600 patients.

 Last Updated October 27, 2025

2020

- The plastic surgery center of **Dr. Kristin Tarbet** in Washington was reportedly hit by ransomware on May 1.
- On the same day, Maze Team also reportedly hit **Nashville Plastic Surgery Institute, LLC**, dba **Maxwell Aesthetics**. Maze leaked data from both practices.

2021

- **JEV Plastic Surgery & Medical Aesthetics** in Maryland disclosed that an unauthorized actor accessed their systems and may have viewed or acquired certain patient information between April 30, 2021, and June 14, 2021. JEV reported that 1,620 patients were affected, but because JEV was not a covered entity, HHS closed its investigation without further action.

2023

- The plastic surgery practice of **Roberto Polizzo** in Brazil was attacked, and data was leaked by "The Snake." Many of the files appeared to have been encrypted.
- **Beverly Hills Plastic Surgery** (BHPS, Dr. David Kim) was attacked by AlphV (aka BlackCat). The notification letter didn't inform patients that patient data was leaked on the dark web.
- The practice of **Gary Motykie, M.D.** in California was attacked in May by an unnamed group or individual. A leak site displayed nude photos of patients as well as their full medical records. Videos of the surgeon in not-safe-for-work videos were also leaked. Patients were told they could pay the hackers directly to get their data removed. Later, the attackers removed the listing and claimed the videos of the doctor were fake news. Dr. Motykie reported that 3,400 patients were affected. He never publicly confirmed nor denied that he had paid extortion to get the listing removed.
- **Hankins & Sohn Plastic Surgery Associates** in Nevada was attacked by the same threat actor(s) who attacked Gary Motykie, M.D. The breach reportedly occurred in February 2023 and was disclosed in March and April. The threat actors created a leak site on the clearnet with nude photos, personal information, and medical records of named patients. The information on the leak site was indexed by Google. Multiple class action lawsuits were consolidated in the Nevada District Court: *Tausinga v. Hankins &*

Sohn Plastic Surgery Associates et al, 2:2023cv00824. As of June 2025, the threat actors continue to add more patients' data to the leak site.

- **Jaime S. Schwartz, M.D.**, in California, was attacked by Hunters International, who announced the attack on their darkweb leak site in October. Allegedly getting no response from Dr. Schwartz despite having leaked sensitive nude photos and files, they reportedly leaked more patient data that consisted of more than 1 TB of files and more than 250,000 files. A lawsuit filed against Dr. Schwartz claimed that he had told patients that only a few patients were affected by the breach. Multiple lawsuits against him have been consolidated in the Central District of California as *In re Jaime S. Schwartz, MD, Data Security Litigation*, Case No.: CV 25-898-GW-SSCx
- **Aesthetic Plastic Surgery, PC**, doing business in New York as **NYBRA Plastic Surgery** ("NYBRA") was attacked between August 28, 2023, and September 4, 2023. They discovered the breach on September 4, 2023.
- **Columbus Aesthetic and Plastic Surgery** ("CAPS") in Ohio discovered in September that they had been hacked. The incident was reported to HHS as affecting 16,598 patients.

2024

- **Long Island Plastic Surgical Group/New York Plastic Surgical Group** was attacked by what was reportedly a collaborative attack involving BlackCat (AlphV) and Radar. The attack allegedly occurred on January 7, 2024, and became publicly known in March 2024 when it was added to a clearnet leak site. The incident was reported to HHS as affecting 161,707 patients. Data was leaked on a darkweb leak site.
- **Jaime S. Schwartz, M.D.**, was attacked for a second time in March 2024. This time, it was not by Hunters International but by the same threat actors who had attacked Dr. Motykie and Drs. Hankins and Sohn. Once again, the threat actors created a leak site with nude pictures of patients with their documents and personal information, and once again, they created a clearnet leak site. In February 2025, Dr. Schwartz notified patients that they had discovered a breach in June 2024. Once again, DataBreaches could find no notification on HHS's public breach tool, even though the threat actors involved in the second breach claim to have data on 1,700 patients. This incident is part of the consolidated class action lawsuit referenced above.
- **SSK Plastic Surgery** was also attacked in March 2024. In March 2025, they notified patients but did not disclose when the breach occurred or when it was first discovered. Their letter stated that the attacker attempted to extort them, but did not disclose whether any data had been exfiltrated or leaked.

2025

- **Hand and Plastic Surgery Centre** dba **Elite Plastic Surgery** in Michigan discovered they were the victim of a cyberattack on January 29, 2025. A total of 19,846 patients were reportedly affected.
- **Vitenas Cosmetic Surgery**, **Mirror Mirror Beauty Boutique**, and the **Houston Surgery Center** in Texas are owned by Paul Vitenas, Jr., M.D., F.A.C.S. On March 5, the threat actor(s) known as Kairos listed Dr. Vitenas's site on their darkweb leak site with proof of claims. They subsequently leaked much of what they claimed was 1.34 GB of files.
- **Michael R. Schwartz, MD, FACS** in California discovered they were the victim of a hacking with exfiltration incident between January 20, 2025 and August 26, 2025. Their notification letter of October 23, 2025 does not state whether there was any ransom or extortion demand. No group publicly claimed responsibility for the attack as of October 27, 2025.

If you are aware of any additions to this chronology or corrections to it, please contact plasticsurgery[at]databreaches[dot]net.

