



Data Breach at Polish Dental Software Vendor FELG Software (FELG Dent)

Oct 02, 2026

[View Alert](#)

☐ WHITE

On October 1, 2026, FELG Software sp. z o.o., the Polish developer of FELG Dent, a cloud-based practice management application for dental practices, [confirmed a cybersecurity incident affecting its platform](#). The incident became public when a threat actor using the alias *Horus* contacted Polish cybersecurity news outlets claiming access to data stored in FELG Dent. According to the company's website, more than 16,000 dentists use its tools.

FELG Software became aware of the incident on September 28, 2026, and the threat actor demanded a ransom in exchange for not disclosing the stolen data. Because FELG Dent serves many independent dental practices from a single platform, a compromise of the vendor may affect patients across a large number of unrelated health sector organizations.

This incident represents the third attack in the last three months against health sector software vendors in Poland, following MyDr in August 2026, where the Ministry of Digital Affairs estimated that data on 18.8 to 19 million people may have been affected, and [Medyc \(Qbusoft\) in September 2026](#). Unlike the two earlier incidents, the FELG Dent breach involves a different threat actor pursuing ransom and the sale of stolen data.

Additional Info

Analysis

FELG Software's CEO confirmed that the incident occurred and stated that its scope is still being determined. Based on preliminary estimates, partly drawn from the threat actor's own claims, **the incident may cover about 2 million patient records.** The potentially affected data includes names, PESEL numbers (Poland's national personal identification number), addresses, medical data, and information related to e-prescriptions, e-ZLA (electronic sick leave certificates) and eWUŚ, the national health insurance eligibility verification system. The company noted that the number of records does not necessarily correspond to the number of individuals affected, and that log analysis results are expected within a few days.

FELG Software has informed all of its clients of a possible breach, filed a report with the prosecutor's office, and remains in contact with UODO, Poland's data protection authority. A detailed technical analysis is underway with external forensic specialists. The company states it has identified how the incident occurred but is not disclosing technical details at this stage.

Threat Actor Claims

The threat actor claims to hold data on 2.4 million patients, including PESEL numbers, names, addresses, phone numbers and associated practices, as well as 1.2 million prescriptions, visit records, e-ZLA, eWUŚ data, and files and photos from the platform. They initially claimed data on 712,000 staff members, but after FELG Software disputed this figure, they lowered it to 28,000, citing duplicate records. **None of the threat actor's figures have been confirmed by FELG Software.**

Claimed Attack Vector

According to the threat actor claims, they began extracting data on September 6, 2026, through poorly secured API endpoints, retrieving successive patient, prescription and staff records by incrementing a request parameter. This describes an insecure direct object reference (IDOR) vulnerability. They further claim that the endpoints required authentication, but that a demo account was sufficient, and that this account could access other users' production data because the interface did not verify data permissions. **FELG Software has not confirmed these technical details.**

Attribution

FELG Software's statement refers to a hacker claiming membership in *fingerprint*, the actor that claimed the MyDr and Medyc breaches. Zaufana Trzecia Strona, a leading Polish cybersecurity news outlet, reports that the threat actor admitted referencing those attacks during ransom negotiations to increase pressure on the victim, and that [fingerprint confirmed it was not responsible for the FELG Dent breach](#). Following the end of negotiations, **the threat actor stated they intend to offer the database for sale on Cebulka, a Polish-language dark web forum.**

Recommendations:

If your organization uses FELG Dent

- Request written confirmation from FELG Software of whether your practice's patient data is affected and which data categories are involved.
- Assess your obligations to notify UODO within 72 hours under GDPR Article 33, and to notify patients under Article 34, together with your data protection officer. Article 33(4) allows information to be provided in

phases, so an initial notification does not need to wait for full scope confirmation from the vendor.

- Reset passwords for all FELG Dent user accounts, remove inactive accounts, and revoke any tokens or integrations linked to the platform. Review available access logs from September 6, 2026, onward.
- Brief reception staff on phishing, SMS and phone scams impersonating your practice or FELG Software, and advise patients to reserve their PESEL number in the mObywatel app.

Health-ISAC recommends that all members, whether or not they use the affected platforms, review their third-party and SaaS vendor security against the following guidance. Priority areas are supplier risk assessment, security requirements in procurement and contracts, vendor incident notification, and protection of sensitive patient data.

- HHS 405(d) and HSCC, *Health Industry Cybersecurity Practices (HICP)*, 2023 Edition - <https://405d.hhs.gov/Documents/HICP-Main-508.pdf>

- HSCC, *Health Industry Cybersecurity Supply Chain Risk Management Guide v2.0* (October 2023) - https://healthsectorcouncil.org/wp-content/uploads/2023/10/HIC-SCRiM_2023-2.pdf

- ENISA, *Procurement Guidelines for the Cybersecurity of Hospitals and Healthcare Providers* (July 2026) <https://www.enisa.europa.eu/sites/default/files/2026-07/Procurement%20guidelines%20for%20the%20cybersecurity%20of%20hospitals%20and%20healthcare%20providers.pdf>

- ENISA, *Cyber Hygiene in the Health Sector* <https://www.enisa.europa.eu/sites/default/files/2025-09/ENISA%20Cyber%20Hygiene%20in%20the%20Health%20Sector.pdf>

Alert Id c98e8b9a

Category Threat Bulletins

Reference [zaufanatrzeciastrona healthsectorcouncil cyware europa hhs europa 1 zaufanatrzeciastrona 1 sekurak money niezalezna](#)

Tags Extortion, Poland, EHR, Third-party Access, PHI, Europe, Supply Chain Attack, Data Exfiltration, Data breach

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Access the Health-ISAC Threat Intelligence Portal

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments

Please email us at toc@h-isac.org

Please provide your feedback



Download the App

Available on iOS, Android and Web



For more updates and alerts, visit: <https://health-isac.cyware.com/webapp/>

Health-ISAC is an invite only platform. Please DO NOT forward this email to anyone. If you are not supposed to receive this email, please report to toc@h-isac.org