Medical reports exposed by changing a URL: GDPR fines for controller and processor

27 November 2026 · 4 min read · blogs.iictp.org/url-id-medical-report-exposure-gdpr-processor-fine

Short answer: a GDPR controller and processor fine followed a platform on which other patients' medical reports could be opened without login by changing a number in the web address, and Italy's data protection authority fined a radiology centre EUR 16,000 and its IT provider EUR 12,000. The European Data Protection Board published the summary on 18 November 2026, and the decision is dated 7 October. It matters because outsourcing a system does not remove the controller's duty to oversee its security.

TL;DR The short version

- Italy's data protection authority fined a radiology centre EUR 16,000 and its IT provider EUR 12,000 after patients' reports could be opened by changing a number in the URL.
- The reports were reachable without login, and both the controller and the processor were held responsible.
- Outsourcing a system does not remove the controller's duty to oversee its security, so test processors' access controls.

Read online, listen to it, or change the text size: https://blogs.iictp.org/url-id-medical-report-exposure-gdpr-processor-fine

What happened?

A complaint reported that reports on the online platform of Centro Radiologico Madonna della Bruna could be viewed by changing the numerical identifier at the end of a link. The documents held identifying details and health data. The centre was the controller, and MedStore Saronno was the processor running the platform.

How the failure worked

Security engineers call this broken object-level access control: the server returns a record because the identifier exists, without checking that the requester is entitled to it. The authority also found that reports dating back to 2020 remained available because automatic deletion had malfunctioned.

What the authority found

- Anyone with an ordinary browser could reach other patients' reports.
- The centre had not adequately overseen security of processing it entrusted to the provider.

- The provider had not promptly installed an available security patch and had not ensured adequate protection against unauthorised access.
- Centre: infringements of Articles 5(1)(e) and (f), 25 and 32.
- Provider: infringements of Articles 5(1)(f) and 32.

Sanctions reported by the source

- EUR 16,000 on the radiology centre.
- EUR 12,000 on the IT provider.
- No further corrective measure on the provider, since the patch was installed after the report.

Limitations and open questions

- We read a summary, not the Italian decision.
- It does not state how many people were affected or how fines were calculated.
- A single national decision shows an approach, not a fixed tariff.
- This is not legal advice.

Sources were read on 27 November 2026. Products, rules and data change, so check the linked originals before you rely on any detail.

How to tighten processor oversight

1. Put patch deadlines, access control testing and retention duties into the processing agreement.
2. Ask for dated evidence of penetration tests that try other users' identifiers.
3. Require reports when scheduled deletion fails, and check deletion yourself on samples.
4. Keep a right to audit and use it.
5. Rehearse breach assessment and notification with the processor.
6. Document these checks, because oversight must be shown.

What it means for lawyers advising healthcare and software clients

Each side had its own findings. A processor cannot rely on the controller to notice an unpatched system, and a controller cannot rely on the contract alone. Include retention in security reviews, since data kept too long increased what was exposed. US readers handling patient records should also see the HIPAA final rule changes.

Frequently asked questions

- **Who paid the GDPR controller and processor fine?** Both: EUR 16,000 for the centre and EUR 12,000 for the provider.
- **What was the technical flaw?** Reports could be opened by changing an identifier in the address, without authentication.
- **Why was retention an issue?** Automatic deletion had failed, leaving reports from 2020 available.
- **Did later patching avoid the fine?** No, although no further corrective measure was imposed on the provider.

Related reading

- HIPAA Privacy Rule final rule
- Onward transfers and model clauses
- What is least privilege?
- Certified Technical Practitioner

Related credential: Certified Technical Practitioner. Explore the exam facts and syllabus.

Sources and further reading

1. European Data Protection Board (national news). Italian DPA fines radiology centre and IT provider a combined EUR 28 000 for exposing patient health data. 18 November 2026. edpb.europa.eu/news/italian-dpa-fines-radiology-centre-and-it-provider-a-combined-eur-28-000-for-exposing-patient_en

Published by IICTP, an independent technical credential body, on 27 November 2026. The current version of this post is at https://blogs.iictp.org/url-id-medical-report-exposure-gdpr-processor-fine. More guides: blogs.iictp.org.