Personal Data Breach Notification

Published: 23 June 2025

Public communication pursuant to Article 34(3)(c) of Regulation (EU) 2016/679 – General Data Protection Regulation (GDPR)

Issued by Azienda USL Toscana sud est – Data Controller, concerning the malfunction of the laboratory software at the Campostaggia and Nottola hospitals between 26 May and 5 June 2025.

What happened?

The laboratory services of the Campostaggia and Nottola hospitals, managed by Azienda USL Toscana sud est, recently experienced a malfunction in the IT system responsible for processing blood samples for haematochemical analyses and for generating and transmitting the related reports to the Electronic Health Record (FSE).
As a result of this malfunction, approximately **1,300 laboratory reports** concerning around **1,200 patients**, generated between **26 May and 5 June 2025** and referring to **samples taken between 15 May and 4 June 2025** at various blood collection points in the province of Siena, were **erroneously uploaded to the FSEs of other patients**.
The incident came to the Company's attention following reports starting from 3 June, some regarding missing reports in a patient's own FSE, and others concerning the presence of a laboratory report belonging to another person.

What personal data were breached?

The breach involved data contained in approximately 1,300 laboratory reports of samples taken at company-operated collection points in the province of Siena. The data included:

- **Health data**: haematochemical values
- **Identification data**: full name, date of birth, tax code
- **Contact details**: address
  These reports account for approximately one-third of the total produced by the two laboratories during the period.
  The incident led to a **loss of confidentiality** and **temporary unavailability** of data. However, **no data loss** occurred.

What has the Company done?

Upon receiving the first reports, the Company immediately activated a response protocol with ESTAR (the Regional Technical and Administrative Support Entity that manages the Company's IT systems) to reconstruct the incident and implement the most advanced technical measures available to resolve the issue.

In particular, by **5 June**:

- the source of the malfunction was eliminated
- a corrective action was applied to the IT system
- the transmission of reports within the Company and to the FSE was restored

By **9 June**, following completion of the analysis:

- the approximately 1,300 misdirected reports were deleted from the incorrect patients' FSEs
- the same reports were retransmitted to the correct patients' FSEs

In relation to the incident, the Company has notified the Italian Data Protection Authority in accordance with Article 33 of the GDPR.

What can I do?

This was a completely accidental incident, with no intentional action involved. Therefore, the likelihood of any concrete harm to affected individuals is objectively **low**.
Given the prompt corrective measures and the fact that each report was potentially visible to only **one unauthorized person**—and even then, it is not certain the report was actually viewed—the **potential impact** on individuals is considered **minimal**.

Nevertheless, we advise potentially affected individuals (i.e., those who had blood drawn at one of the Company's collection points in the province of Siena during the indicated period) to be **especially cautious** if contacted by unknown persons requesting personal information or making other unusual requests.

Who can I contact for more information?

For further clarification, you can contact the Company's Data Protection Officer through the following channels:

- By phone: +39 0577-536890
- By email: **privacy@uslsudest.toscana.it** for general inquiries
- For personal inquiries: **privacy@uslsudest.toscana.it** (please attach a copy of a valid ID)