AXIOMATIC

Responsible disclosure

If you find a weakness in Inora, on axiomatic.digital or in the infrastructure we operate, report it to us. We confirm every report and keep you informed until it is closed.

Updated on 9 November 2026

Why this matters

Care organisations put their protocols, work agreements and quality handbook into Inora. Their staff type questions and reports into it that can concern clients, and so can contain health data. A weakness in Inora therefore affects not only us, but care organisations, their staff and their clients. We would rather hear about it from you than from someone who abuses it.

How we protect Inora and that data is on the Security page.

What this policy covers

- Inora's web application, in which the staff of care organisations ask questions and write reports.
- Inora's APIs.
- This website, axiomatic.digital.
- The infrastructure Axiomatic itself operates for Inora and for this website.

What it does not cover

- Services and integrations run by others, such as a care organisation's identity provider (for example Microsoft Entra ID) or its electronic client record. Report a vulnerability there to that organisation or to its maker. If it also affects Inora, tell us as well.
- Social engineering and phishing of Axiomatic's staff or of care organisations' staff.
- Attacks that overload or take down the service (DoS and DDoS).
- Automated scanning or testing that makes the service slower or unavailable for others.

- Physical attacks on offices or data centres.
- Software and systems that are not Axiomatic's.

How to report

Email security@axiomatic.digital with "Security" in the subject line.

In your report, include:

- what the vulnerability is and what someone could do with it;
- the steps to reproduce it;
- what shows it, such as screenshots, a proof of concept or requests and responses;
- how we can reach you with questions.

Do not send us other people's data you came across. Describe what you saw, not the data itself.

The address and this policy are also in security.txt on axiomatic.digital, following RFC 9116.

What we do, and when

- **Receipt.** We confirm receipt of your report within three working days.
- **Assessment.** We investigate the report, set its severity by the classes below and tell you what we find.
- **Fix.** We fix a critical vulnerability within 72 hours and others within 30 days. If we cannot, we tell you why and when we will.
- **Keeping you informed.** Until the vulnerability is fixed, we keep you informed of our progress.
- **Care organisations.** If the vulnerability let a care organisation's data be viewed, changed or lost, we notify that organisation without undue delay, no later than 24 hours after we become aware of it, as the Security page describes.
- **Credit.** With your permission, we credit you once the vulnerability is fixed.

What we ask of you

- Do not access, change or delete data that is not yours.
- If you come across data of a care organisation, a member of staff or a client, stop at once, tell us and keep no copy.
- Do not disrupt the service. It is used at night too, when there is no colleague to fall back on.
- Test only with accounts you own or have explicit permission to use. Inora has no public sign-up: every account is created by a care organisation, through its own sign-in. If you want to test Inora yourself, ask us for access.
- Use a vulnerability no further than needed to show it.
- Publish nothing before the vulnerability is fixed, and give us 90 days from your report for that. If it is fixed sooner, we agree together when you publish.
- Do nothing beyond what this policy allows.

What we commit to

If you follow this policy and act in good faith, we will not report you to the police or take legal action against you. If someone else holds you to account, we will state that you acted within this policy. We cannot waive action on behalf of others, such as the Public Prosecution Service or a care organisation.

We treat your report and your details as confidential, and share your name only with your permission.

How we set severity

Class	Examples
Critical	Remote code execution; bypassing sign-in; access to another organisation's environment; viewing conversations, reports or documents at scale; obtaining keys or secrets.
High	Gaining more rights within an organisation than one's own account gives; viewing another member of staff's conversations; stored cross-site scripting; SQL or command injection; making Inora answer outside the organisation's sources or judge a client.

Class	Examples
Medium	Cross-site request forgery; leaking data without sensitive content; access-control faults with limited impact.
Low	Verbose error messages, missing security headers and other departures from good practice with little impact.

We look at what an attacker can achieve in practice, not only at the type of fault. Where client data is involved, we weigh the report more heavily.