AXIOMATIC

Security overview

Axiomatic B.V. and Inora

Version 1.4, 9 November 2026

1. Introduction

Axiomatic B.V. designs, builds, implements and operates Inora. Care workers ask Inora questions in ordinary language and get answers from the sources their organisation has designated; one tap on a marker shows the organisation's source a sentence rests on. The organisation's own documents are internal, and the questions can concern clients. This overview describes how we protect that data: who can reach it, where it is, how it is separated, encrypted, backed up and monitored, and how we recover.

This document is meant for the privacy officer, information security officer and IT staff of a care organisation that is assessing Inora. It is part of the security measures referred to in Annex 2 of our data processing agreement. The proposed periods and measures become commitments only after confirmation and signature of the data processing agreement.

2. Organisation and people

2.1 The team

The people who build, implement and operate Inora:

- Engineering builds and operates Inora. The director is responsible for security and privacy at Axiomatic.
- Implementation and partnerships work with care organisations during implementation, without access to organisation data or to production.
- The advisors have no access to organisation data or to production.

Only named engineers have access to the production environment, listed in the processing agreement. We do not use contractors with access to production or to organisation data.

2.2 Confidentiality and screening

Everyone at Axiomatic has signed a confidentiality agreement that continues after they leave. This agreement is also what the Dutch GDPR Implementation Act requires of people who process health data without a professional duty of secrecy of their own (Article 30(4) UAVG). Everyone with access to production holds a certificate of conduct (VOG).

Everyone reads and signs our security rules when they start, and again each year.

2.3 Devices

We work on laptops with full-disk encryption, automatic security updates, a firewall and a screen lock after a few minutes. Organisation data is never stored on laptops. A lost or stolen laptop is reported the same day, and its access is revoked.

2.4 Accounts and access

- Personal accounts only. No shared accounts, no shared passwords.
- Multi-factor authentication on every account that gives access to code, infrastructure, email or documents. Administrative access to production uses a hardware security key.
- Access to production is limited to the named engineers, and to what they need.
- Every access by Axiomatic staff to an organisation's environment is logged. We review access rights every quarter.
- When someone leaves, their access ends the same day.

3. Architecture

3.1 One environment per organisation

Each organisation has its own environment in Inora: its own database, its own document storage and its own search index. There is no shared database in which organisations are separated only by a column. A question asked in one organisation can only reach that organisation's documents.

3.2 Sign-in

Inora connects to the organisation's own single sign-on, usually Microsoft Entra ID, through OpenID Connect or SAML 2.0. With single sign-on Inora stores no passwords; multi-factor authentication and password rules are set by the organisation in its own identity provider. When the organisation disables an account there, that person can no longer sign in to Inora. An existing session may remain active until revoked or expired. A session ends no later than eight hours after it starts.

The consent in Entra ID gives Inora only openid, profile, email and User.Read, delegated and read-only; the organisation's groups arrive as a claim in the sign-in token. No access to mail, files, Teams or SharePoint. Inora reads only the groups the organisation assigns to the app, so the claim never overflows. The organisation's administrator disables those accounts in Inora.

Inora has two roles. Administrators manage documents, settings and the report register. Users ask questions and draft reports. The organisation decides which groups of staff get which role.

3.3 How a question is answered

1. A user asks a question in Inora.
2. Inora searches the organisation's own index for the passages that concern the question.
3. The question and those passages go to the language model, within the European Union.
4. The model writes an answer from the passages. Inora shows the answer with a marker after each sentence that rests on one of the organisation's sources; one tap shows the document and the passage. If no passage answers the question, Inora says so, and where it looked.
5. The question, the answer and the sources are stored in the user's conversation history in the organisation's environment, for the retention period the organisation has set.

For reports, the headings come from a register the organisation maintains. The model writes only the content beneath them.

The organisation's sources stay in its own document system; Inora works with a copy that its handbook manager supplies and keeps up to date. There is no connection to that document system.

The client record stays in the organisation's own EHR. Inora reads it with the care worker's own login and rights, in a microVM of its own per user, so the pilot needs no connection. Connections come after the pilot, and the organisation's IT turns them on.

Building the search index also sends document passages to the embedding model in the EU. Answering sends the question and retrieved passages to the language model, which in the same step sorts the conversation by topic for the team reports (section 6).

4. Hosting and location

Component	Provider	Location
Application, database, document storage, search index	Amazon Web Services (Amazon Web Services EMEA SARL)	Europe (Ireland) Region, eu-west-1
Backups	Amazon Web Services	Europe (Ireland) Region, eu-west-1
Language model	Amazon Bedrock, EU inference profile	Amazon Web Services Regions in the EU
Language models through Azure OpenAI; the system picks the model	Microsoft Ireland Operations Limited (Azure OpenAI)	An Azure region in the EU
Website axiomatic.digital (no organisation data)	Amazon S3 and Amazon CloudFront	Files in the Europe (Ireland) Region; delivered through CloudFront's global network

All Inora data is processed and stored in the European Union. Processing outside the EU first requires a written amendment to the arrangements with the organisation. Transfers outside the EEA also require a valid basis under Chapter V GDPR; the organisation's authorisation alone is insufficient. Remote access and support are included in this assessment. Article 3.5 of the data processing agreement sets this out.

The physical security of the data centres is the responsibility of Amazon Web Services. AWS publishes its own certifications and audit reports. Those cover AWS's services, not Axiomatic.

The parent companies, Amazon.com, Inc. and Microsoft Corporation, are American; both take part in the EU-US Data Privacy Framework. Storage in the EU does not rule out a request from a foreign government; section 13 describes what we then do.

5. Encryption

- **In transit.** All traffic to and from Inora, and between its components, uses TLS 1.2 or higher. Older protocols are refused.
- **At rest.** Databases, document storage, search indexes and backups are encrypted with AES-256.
- **Keys.** The encryption keys sit in AWS Key Management Service, in the EU, with access restricted and every use logged.
- **Secrets.** Passwords for services, API keys and certificates are kept in a key vault, never in source code.

The limit. While a question is answered, the question and the passages are decrypted only for as long as the answer is being made; the model does not keep them. This happens on our servers and at the language model. Encryption in transit and at rest does not prevent that processing of readable text. This is not end-to-end encryption in which only the user can read the text. Staff with production access could, in principle, see content at that moment; section 2 describes who they are and how their access is logged.

6. Artificial intelligence

- **Model.** Inora uses language models in Amazon Bedrock, through the EU inference profile. Prompts and answers are processed only in Regions within the EU. Amazon Bedrock does not store the question or the passages and does not pass them to the model's maker.
- **Azure OpenAI.** The system picks the language model for each task; through Azure OpenAI it runs in an EU region. Axiomatic runs it with the modified abuse monitoring Microsoft approves for sensitive data: Microsoft stores no questions or answers, and no Microsoft employee reads them (https://learn.microsoft.com/en-us/azure/ai-foundry/openai/concepts/abuse-monitoring).
- **Team reports.** For the team reports the language model that writes the answer sorts the conversation by topic in the same step, in the EU. No person reads along, and the model keeps nothing. The sorting stays in the environment and is deleted with the conversation.
- **Training and storage.** Neither Axiomatic nor the model provider uses organisation data to train or fine-tune models.
- **Search index.** To make documents searchable, Inora converts passages into numerical representations with an embedding model in the same EU deployment. These are stored in the organisation's own index and deleted with the documents.

- **Source on one tap.** Each sentence that rests on one of the organisation's sources carries a marker; one tap shows the document and the passage. A language model can be wrong; the source lets the care worker check it.
- **Boundary.** Inora supports professionals with their organisation's knowledge. It does not diagnose, decide on treatment or assess photos of skin or wounds; in triage the nurse triages, and Inora puts the organisation's protocol beside them and flags what is missing. The professional decides. Its intended use keeps Inora outside the scope of the medical device rules.

7. Logging and monitoring

Inora records sign-ins, administrative actions and every access by Axiomatic staff, for 12 months. On request an organisation receives its environment's security logging, totalled per team of at least five people and per day, and every access by Axiomatic; a day with fewer than five sign-ins shows as '<5'. The sign-in times and IP addresses of one member of staff never go to the organisation. In a security incident Axiomatic investigates the log itself and reports a finding about the system, naming no care worker.

- Inora also records changes to documents and settings.
- We receive alerts for repeated failed sign-ins, unusual traffic, errors and unavailability.
- The logs stay in the EU and cannot be changed by the application.

8. Backups and recovery

- We back up every organisation's environment daily; at most 24 hours of data is lost. A restore from back-up takes at most 8 hours.
- Backups: daily, encrypted, kept for 30 days, in the Europe (Ireland) Region, across several availability zones.
- Every quarter we restore a backup to a separate environment to check that it is complete.
- Built for 99.9% availability, with the target of 95% of outages resolved within 4 hours and a response within an hour, day and night. The organisation reports an outage to support@axiomatic.digital, day and night. During an outage the organisation's contact gets notices by email until it is resolved.

- Each of the named engineers can restore the service alone. The recovery procedure is written down.

9. Development and change

- Every change to Inora is reviewed by a second engineer before it reaches production.
- Development and testing use a separate environment with no organisation data.
- We monitor the libraries Inora depends on for known vulnerabilities. Security updates for critical vulnerabilities are applied within 72 hours, other security updates within 30 days.
- We follow the OWASP Top 10 as the checklist for web application risks.

10. Testing

- **Penetration test.** An independent specialist tests Inora every year, the application and the infrastructure, against the OWASP Top 10 and the separation between organisations. We fix critical findings within 72 hours, others within 30 days. The summary of the latest test is available on request.
- **Continuous scanning.** Code, dependencies, containers and cloud configuration are scanned automatically on every change and every day.
- **Security researchers.** Anyone can report a vulnerability to us, under the policy below.

To report a vulnerability, email security@axiomatic.digital with “Security” in the subject line. We confirm receipt within three working days. We ask researchers not to access or change others’ data, not to disrupt the service and to give us 90 days before publication. We take no legal action against research done in good faith within these rules.

11. Incident management

We follow a written incident procedure:

1. **Detect.** Alerts, reports from users, organisations or researchers.
2. **Contain.** Stop the cause and limit the damage.
3. **Assess.** Establish which organisations, data and people are involved.

4. **Notify.** We notify a personal data breach or suspected breach without undue delay, no later than 24 hours after becoming aware. This is a contractual maximum, not a waiting period. A breach can also involve loss of availability, destruction or unauthorised disclosure. We share what is known about its nature, affected data and people, likely consequences and measures. Notices name the kinds of data and the number of people affected, never data from Inora. Further information follows as it becomes available.
5. **Support.** The care organisation is the controller. It must notify the Dutch Data Protection Authority, the Autoriteit Persoonsgegevens, without undue delay and, where feasible, within 72 hours of becoming aware of a personal data breach, unless a risk to people's rights and freedoms is unlikely. Where a high risk is likely, it informs affected people without undue delay, unless an exception under Article 34(3) GDPR applies. It documents every breach, even where notification is not required. We assist it. The 72-hour period does not wait for our final report. A late notification must explain the delay.
6. **Report.** We send a written report within ten working days of becoming aware. If the investigation is ongoing, we say so and supplement the report. This does not postpone earlier notifications.
7. **Learn.** We change the system or the procedure to prevent recurrence.

12. Retention and deletion

Data	Retention
Conversations (questions, answers, drafted reports, the topic sorting)	90 days, or the period the organisation sets; a conversation the function in annex 3 to the data processing agreement asked for, until the investigation is complete (art. 5.5)
Documents	As long as the organisation keeps them in Inora; removed from backups within 30 days of removal
User accounts	While the user has access and up to 30 days afterwards
Logs	12 months, unless the agreement ends sooner
Service metrics (numbers of questions and response times per user)	Per user 30 days; after that only totalled per team of at least five people
Competence record	As long as the member of staff works for the organisation, plus 30 days; in those 30 days the organisation exports it to its own personnel file

Data	Retention
Test set, only on the organisation's written instruction	Until the organisation withdraws the instruction, at the latest until the end of the agreement; then gone within 30 days
Answer record (sources, versions, model, check and date per answer, and a reference the member of staff sees with the answer)	2 years, at Axiomatic; then out of backups within 30 days
Backups	30 days
All data after the agreement ends	Return or deletion at the organisation's choice; available for return up to and including day 30 unless return is completed or earlier deletion requested; active systems, including logs and search indexes, cleared by day 30; backups cleared by day 60

Only a retention requirement under Union or Dutch law can justify an exception to deletion. We then state the data, legal basis and period concerned, unless the law prohibits this. The data remains protected for as long as we hold it. After deletion during the agreement, copies may remain in backups for up to 30 further days. We reapply deletions after a restore. On request, we confirm deletion in writing.

13. Government requests

We disclose organisation data to a government authority only when Union or Dutch law obliges us to, for example under a court order, and then no more than required. Unless the law forbids it, we tell the organisation first. We object to requests that do not have a valid legal basis.

If the law demands a conversation, Axiomatic gives only what the demand asks, logs it, and the member of staff is told, unless the law forbids it.

14. Assurance

For the organisation's assessment:

- this security overview;
- the data processing agreement, covering subjects from the Brancheorganisaties Zorg model but using its own provisions;

- the list of sub-processors;
- the control matrix in section 15: every control of ISO 27001 and NEN 7510 and how we built it, the basis for your statement of applicability;
- a description of the processing, for the organisation's data protection impact assessment (DPIA).

We cooperate with audits and inspections by the organisation or its mandated auditor covering all obligations under the data processing agreement. Routine audits normally take place once a year. Additional audits remain possible where needed under Article 28 GDPR, including after an incident, indications of non-compliance, a material change or a supervisory authority request. The organisation bears the cost of its own auditor, unless the audit reveals a material failure on our part.

15. Control matrix

Built to NEN 7510 and ISO 27001: every control of Annex A of ISO/IEC 27001:2022 and the controls NEN 7510 adds for healthcare, with how Axiomatic built it for Inora and the status of each row.

Organisational (37)

No.	Control	How we built it	Status
5.1	Policies for information security	The security policy and the security overview set out how Inora is secured, and both are public. Everyone at Axiomatic reads and signs the security rules at the start and every year after. The director approves the policy and reviews it every year and after every serious security incident.	▪ In place
5.2	Information security roles and responsibilities	The director is responsible for security and privacy at Axiomatic. The security overview names who can reach production and who cannot.	▪ In place
5.3	Segregation of duties	No change reaches production without review by a second engineer. Whoever guides organi-sations through implementation has no access to production or to their data.	▪ In place

No.	Control	How we built it	Status
5.4	Management responsibilities	Management requires everyone to sign the security rules at the start and every year, and carries the responsibility for security and privacy itself.	▪ In place
5.5	Contact with authorities	In a data breach we help the organisation notify the Autoriteit Persoonsgegevens. We answer a request from an authority only where Union or Dutch law obliges us, with no more than necessary and, unless the law forbids it, after the organisation knows.	▪ In place
5.6	Contact with special interest groups	We follow the security advisories of the NCSC and Z-CERT and the security notices of every building block Inora runs on.	▪ In place
5.7	Threat intelligence	With the advisories from 5.6 we review every month which threats bear on Inora, and record it. Known vulnerabilities in the libraries are tracked automatically.	▪ In place
5.8	Information security in project management	Every implementation and every new feature starts with its security questions answered in writing: which data, who can reach it, which supplier.	▪ In place
5.9	Inventory of information and other associated assets	A register lists every system, supplier, data store and laptop, each with an owner, checked every quarter.	▪ In place
5.10	Acceptable use of information and other associated assets	The security rules everyone signs say how information and laptops may be used. Organisation data never sits on a laptop.	▪ In place
5.11	Return of assets	When someone leaves, the laptop comes back on the last working day and is wiped. Access ends the same day.	▪ In place
5.12	Classification of information	Everything users type into Inora is classed as health data and protected as such. The organisation's documents are classed as internal.	▪ In place
5.13	Labelling of information	Every environment, store and search index carries the label of its organisation and its data class in the infrastructure.	▪ In place

No.	Control	How we built it	Status
5.14	Information transfer	All traffic to and from Inora, and between its parts, is encrypted with TLS 1.2 or higher. What we do with data, and with whom, is set down in the data processing agreement.	▪ In place
5.15	Access control	The organisation decides which groups of staff get access and who administers. Only the engineers who build Inora can reach production, each by name.	▪ In place
5.16	Identity management	Staff sign in with their own account through the organisation's identity provider, by SAML or OpenID Connect; SCIM creates and closes accounts. When the organisation disables an account there, that person can no longer sign in. There are no shared accounts.	▪ In place
5.17	Authentication information	With single sign-on Inora stores no passwords. Administrative access to production needs a physical security key, and service keys and certificates sit in a key vault, never in the source code.	▪ In place
5.18	Access rights	Every quarter we review access rights. When someone leaves, their access ends the same day.	▪ In place
5.19	Information security in supplier relationships	We work with as few sub-processors as we can: for Inora Amazon Web Services, and Microsoft (Azure OpenAI, EU). We remain responsible for what our suppliers do.	▪ In place
5.20	Addressing information security within supplier agreements	Every sub-processor has signed an agreement with obligations no weaker than those in our data processing agreement.	▪ In place
5.21	Managing information security in the ICT supply chain	Inora runs on open building blocks and its language model can be exchanged, so it depends on no single vendor. The libraries it runs on are checked for known vulnerabilities.	▪ In place
5.22	Monitoring, review and change management of supplier services	We announce a new sub-processor 30 days ahead. The organisation can object. If we find no solution together, it may end the agreement for the part that cannot be delivered without the new sub-processor, at no cost.	▪ In place

No.	Control	How we built it	Status
5.23	Information security for use of cloud services	Inora runs at Amazon Web Services EMEA SARL in the Europe (Ireland) region, its language model through Amazon Bedrock's EU inference profile or through Azure OpenAI in the EU; the system picks the model. No one trains models on this data. Amazon Bedrock does not store the question or the passages and does not pass them to the model's maker, and Azure OpenAI runs with the modified abuse monitoring Microsoft approves for sensitive data, so Microsoft stores no questions or answers and no Microsoft employee reads them.	▪ In place
5.24	Information security incident management planning and preparation	A written incident procedure in seven steps: detect, contain, assess, notify, support, report and learn.	▪ In place
5.25	Assessment and decision on information security events	Every event is assessed for the organisations, data and people it touches, and placed in one of four severity classes, critical to low, as Responsible disclosure describes them.	▪ In place
5.26	Response to information security incidents	We notify the organisation of a breach, or a suspected one, no later than 24 hours after becoming aware, with what is known. A written report follows within ten working days.	▪ In place
5.27	Learning from information security incidents	We investigate every incident without blame, with the cause sought in the system, and change the system or the procedure so it does not recur.	▪ In place
5.28	Collection of evidence	In an incident we capture a snapshot of the affected environment before anything changes, with who took it and when. The logging is immutable (5.33).	▪ In place
5.29	Information security during disruption	The restore procedure is written down, so any engineer can run it alone. After a restore we apply deletions again.	▪ In place
5.30	ICT readiness for business continuity	A backup every day, a restore test every quarter, at most 24 hours of data lost. A restore from back-up takes at most 8 hours. Built for 99.9% availability, with the target of 95% of outages resolved within 4 hours and a response within an hour, day and night.	▪ In place

No.	Control	How we built it	Status
5.31	Legal, statutory, regulatory and contractual requirements	The GDPR, the Dutch UAVG and the AI Act are worked through for Inora in the published policies. The data processing agreement follows Article 28 GDPR.	▪ In place
5.32	Intellectual property rights	Protocols and handbooks stay the property of the organisation that wrote them. For sources from others, such as national guidelines, their publisher's licence applies.	▪ In place
5.33	Protection of records	Logs are kept for 12 months in the EU and cannot be changed by the application. Invoices and the records behind them are kept for seven years, as Dutch tax law requires.	▪ In place
5.34	Privacy and protection of PII	The organisation is the controller, we are the processor. No one in the organisation reads a member of staff's conversation, and no model trains on the data.	▪ In place
5.35	Independent review of information security	The organisation or its auditor audits every obligation in the data processing agreement, in principle once a year.	▪ In place
5.36	Compliance with policies, rules and standards for information security	Every year we check this matrix against what runs in production; a deviation is fixed or recorded.	▪ In place
5.37	Documented operating procedures	The incident procedure and the restore procedure are written down, so any engineer can run them alone.	▪ In place

People (8)

No.	Control	How we built it	Status
6.1	Screening	Everyone with access to production holds a Dutch certificate of conduct (VOG).	▪ In place
6.2	Terms and conditions of employment	Everyone signs a confidentiality agreement that holds after they leave, and the security rules, at the start and every year after.	▪ In place

No.	Control	How we built it	Status
6.3	Information security awareness, education and training	Twice a year the team trains on phishing and on handling care data. Everyone signs the security rules at the start and every year.	▪ In place
6.4	Disciplinary process	The security rules state what follows a breach of them, from a conversation to withdrawn access and dismissal.	▪ In place
6.5	Responsibilities after termination or change of employment	Confidentiality continues after someone leaves, and their access ends the same day.	▪ In place
6.6	Confidentiality or non-disclosure agreements	Everyone at Axiomatic has signed a confidentiality agreement, as Article 30(4) UAVG asks of anyone who processes health data without a professional duty of secrecy.	▪ In place
6.7	Remote working	Work laptops have full-disk encryption, a firewall and automatic security updates, and lock after a few minutes. Organisation data never sits on a laptop.	▪ In place
6.8	Information security event reporting	A lost or stolen laptop is reported the same day. Researchers report a vulnerability by email and hear back within three working days.	▪ In place

Physical (14)

No.	Control	How we built it	Status
7.1	Physical security perimeters	Inora runs only in Amazon Web Services data centres in the EU; their physical security lies with AWS, under its own ISO/IEC 27001 and SOC 2 reports. Axiomatic's office holds no organisation data.	▣ In place at AWS
7.2	Physical entry	Axiomatic has no server room of its own; no one from Axiomatic enters a data centre. We reach Inora only remotely, with a personal account and a physical security key (the data centres themselves: 7.1).	▪ In place
7.3	Securing offices, rooms and facilities	The rooms that hold organisation data are AWS's. No Axiomatic office holds organisation data.	▣ In place at AWS

No.	Control	How we built it	Status
7.4	Physical security monitoring	AWS monitors its data centres, as its own audit reports describe.	▣ In place at AWS
7.5	Protecting against physical and environmental threats	Fire, water, power and climate in the data centres are AWS's responsibility. Backups are kept apart from production, encrypted, in the EU.	▣ In place at AWS
7.6	Working in secure areas	Work inside the data centres' secure areas is done by AWS; Axiomatic does not work there.	▣ In place at AWS
7.7	Clear desk and clear screen	Laptops lock after a few minutes unattended. Organisation data never sits on a laptop, so it never sits on a desk either.	▪ In place
7.8	Equipment siting and protection	Inora's servers are AWS's, sited and protected by AWS.	▣ In place at AWS
7.9	Security of assets off-premises	Laptops have full-disk encryption. A lost or stolen laptop is reported the same day, and its access is withdrawn.	▪ In place
7.10	Storage media	Storage holding organisation data is AWS's, encrypted with AES-256. Laptop disks are fully encrypted.	▣ In place at AWS
7.11	Supporting utilities	Power, cooling and network in the data centres are AWS's responsibility.	▣ In place at AWS
7.12	Cabling security	Cabling in the data centres is AWS's responsibility. All of Inora's traffic is encrypted, over those cables too.	▣ In place at AWS
7.13	Equipment maintenance	AWS maintains the equipment in its data centres. Laptops install security updates automatically.	▣ In place at AWS
7.14	Secure disposal or re-use of equipment	Disks that held organisation data are AWS's, which wipes or destroys them under its own audited procedure. Laptops hold no organisation data.	▣ In place at AWS

Technological (34)

No.	Control	How we built it	Status
8.1	User endpoint devices	Work laptops: full-disk encryption, a firewall, automatic updates and a screen lock. The organisation's staff use Inora in the browser, signed in through the organisation's own identity provider.	▪ In place
8.2	Privileged access rights	Only the engineers who build Inora have administrative access to production, each with a personal account, multi-factor authentication and a physical security key. Every access is logged.	▪ In place
8.3	Information access restriction	A question in one organisation can reach only that organisation's documents. No one in the organisation reads a member of staff's conversation. Axiomatic reads a conversation only on a written request from the function the organisation names, for an incident or a complaint, or on a legal demand (art. 5.6); every access is logged and the member of staff is told, unless the law forbids it. In an outage or security incident Axiomatic examines the system logs and the answer record, never a conversation. For the team reports the language model that writes the answer sorts the conversation by topic in the same step, without names; no person reads along (art. 5.6).	▪ In place
8.4	Access to source code	The source code is reachable only through a personal account with multi-factor authentication, and every change to it is reviewed by a second engineer.	▪ In place
8.5	Secure authentication	Sign-in runs through the organisation's own identity provider, by SAML or OpenID Connect, under its own multi-factor rules; SCIM creates and closes accounts. With Entra ID the consent gives Inora only openid, profile, email and User.Read, delegated and read-only; no access to mail, files, Teams or SharePoint. Inora reads only the groups the organisation assigns to the app, so the claim never overflows. A session ends no later than eight hours after it starts.	▪ In place

No.	Control	How we built it	Status
8.6	Capacity management	Load, storage and model capacity are measured per environment, with an alert before a limit is reached.	▪ In place
8.7	Protection against malware	Every document that enters Inora is scanned for malware before it reaches the search index. Laptops run the operating system's malware protection.	▪ In place
8.8	Management of technical vulnerabilities	Inora's libraries are checked automatically for known vulnerabilities. Critical security updates are applied within 72 hours, others within 30 days.	▪ In place
8.9	Configuration management	The infrastructure is defined as code and reviewed like software, by the same second engineer as a change to Inora.	▪ In place
8.10	Information deletion	Conversations are deleted after 90 days, or after the period the organisation sets; a conversation the function in annex 3 to the data processing agreement asked for stays until the investigation is complete (art. 5.5). After the agreement, active systems are empty by day 30 and backups by day 60, confirmed in writing.	▪ In place
8.11	Data masking	Development and testing use no organisation data. The measurements Axiomatic sees contain no names and no content of documents, questions or answers.	▪ In place
8.12	Data leakage prevention	A question can reach only its own organisation's documents. Organisation data never goes onto a laptop or into the AI tools we use to write software.	▪ In place
8.13	Information backup	A backup of every environment every day, encrypted, kept for 30 days, in the Europe (Ireland) region. Every quarter we restore one to check that it works.	▪ In place
8.14	Redundancy of information processing facilities	Inora runs across several availability zones of the Europe (Ireland) region, so the loss of one data centre does not stop it. The stored data also sits across several zones at AWS.	▪ In place

No.	Control	How we built it	Status
8.15	Logging	Inora records sign-ins, administrative actions and every access by Axiomatic staff, for 12 months. On request an organisation receives its environment's security logging, totalled per team of at least five people and per day, and every access by Axiomatic; a day with fewer than five sign-ins shows as '<5'. The sign-in times and IP addresses of one member of staff never go to the organisation. In a security incident Axiomatic investigates the log itself and reports a finding about the system, naming no care worker.	▪ In place
8.16	Monitoring activities	We are alerted to repeated failed sign-ins, unusual traffic, errors and unavailability.	▪ In place
8.17	Clock synchronization	Every server takes its time from the cloud provider's time service, so the logs of every part line up to the second.	▪ In place
8.18	Use of privileged utility programs	Administrative tools that can bypass the application reach production only through the engineers' personal accounts, with a physical security key. Every access is logged.	▪ In place
8.19	Installation of software on operational systems	Software reaches production only as a reviewed release through the deployment pipeline; no one installs anything on a running server by hand.	▪ In place
8.20	Networks security	All traffic to Inora and between its parts uses TLS 1.2 or higher; older protocols are refused.	▪ In place
8.21	Security of network services	Inora is reachable only through AWS's load balancer, behind a web application firewall that blocks known attack patterns.	▪ In place
8.22	Segregation of networks	Each organisation has its own environment, separated in the infrastructure and not only in the software. Development and testing run apart from production.	▪ In place
8.23	Web filtering	Work laptops filter web traffic at DNS level and block known malicious domains.	▪ In place

No.	Control	How we built it	Status
8.24	Use of cryptography	TLS 1.2 or higher in transit, AES-256 at rest for databases, document storage, search indexes and backups. The keys sit in AWS Key Management Service, in the EU; every use is logged. Secrets sit in a key vault.	▪ In place
8.25	Secure development life cycle	Every change is reviewed by a second engineer, with the OWASP Top 10 as checklist. If the organisation gives a written instruction for it, after the consent of its works council where it has one, every new version is tested on its test set, its own questions and flagged answers stripped of names, before its staff see that version.	▪ In place
8.26	Application security requirements	Beside the OWASP Top 10, what is particular to Inora counts as a security fault: an answer outside the organisation's sources, or one organisation reaching another. The severity classes on Responsible disclosure name them.	▪ In place
8.27	Secure system architecture and engineering principles	Each organisation has its own database, document storage and search index; no shared database with organisations told apart by a column. The language model can be exchanged, and processing stays in the EU.	▪ In place
8.28	Secure coding	The OWASP Top 10 is the checklist at every review. Secrets never sit in the source code, and libraries are checked for known vulnerabilities.	▪ In place
8.29	Security testing in development and acceptance	If the organisation gives a written instruction for it, after the consent of its works council where it has one, every new version is tested on its test set, its own questions and flagged answers stripped of names, before it goes live.	▪ In place
8.30	Outsourced development	Inora is built by Axiomatic's own engineers. No outside contractor has access to production or to organisation data.	▪ In place
8.31	Separation of development, test and production environments	Development and testing happen in a separate environment, without organisation data.	▪ In place

No.	Control	How we built it	Status
8.32	Change management	Every change is reviewed by a second engineer before it reaches production. Planned maintenance is announced in advance, and a function the organisation relies on is never removed unannounced.	▪ In place
8.33	Test information	Test data contains no organisation data; development and testing happen without it.	▪ In place
8.34	Protection of information systems during audit testing	Audits and tests on production are agreed in advance, read-only where possible and outside the busiest hours.	▪ In place

Healthcare (NEN 7510) (8)

No.	Control	How we built it	Status
5.38	Analysis and specification of information security requirements	Every feature is held in advance to the OWASP Top 10 and to the faults particular to Inora: an answer outside the sources, or one organisation reaching another.	▪ In place
5.39	Uniquely identifying subjects of care	Inora keeps no register of care recipients, so it has no duplicates; unique identification and merging happen in the organisation's ECD. Inora asks for no citizen service number.	▪ In place
5.40	Validation of displayed or printed data	Inora keeps no register of care recipients. A report about a client goes, on the care worker's approval, into the record of the client they have open in the ECD, where the organisation identifies the client. Every sentence that rests on a source of the organisation carries a marker that shows the document and the passage.	▪ In place
5.41	Publicly available health information	Public sources the organisation designates, such as national guidelines, are read as published, under their publisher's licence, and every answer shows the source it rests on.	▪ In place

No.	Control	How we built it	Status
5.42	Communication in emergencies	The organisation reports an outage that makes Inora unusable to support@axiomatic.digital, day and night; a response within an hour. In a breach its contact hears no later than 24 hours after we become aware. We test the channel and a second contact every year with the organisation's contact.	▪ In place
5.43	Reporting incidents externally	We notify the organisation of a breach no later than 24 hours after becoming aware and help it notify the Autoriteit Persoonsgegevens, which it must do within 72 hours where feasible.	▪ In place
6.9	Management training	Management takes training every year in the duties the Cyberbeveiligingswet and NEN 7510 place on it.	▪ In place
8.35	Zero trust principles	No access rests on a network location: every user signs in through the organisation's own identity provider, every administrative access takes a personal account and a physical key, and every access is logged.	▪ In place

16. Contact

Axiomatic B.V., Delft. security@axiomatic.digital.