AXIOMATIC

# Control matrix

Inora, built to NEN 7510 and ISO 27001

Version 1.3, 9 November 2026

Every control of Annex A of ISO/IEC 27001:2022, as NEN 7510 takes it over, and the eight controls NEN 7510 adds for healthcare, with how Axiomatic built it for Inora. “With AWS” means the cloud provider carries out the control, with its own audit reports as the evidence. This document is the basis for your statement of applicability in your own assessment of Inora as a supplier.

Physical controls in the data centres lie with the cloud provider, Amazon Web Services EMEA SARL, in the Europe (Ireland) Region. Who else processes data is at axiomatic.digital/en/trust/sub-processors.

## 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 |

Questions about this matrix: security@axiomatic.digital.