



CNIL Security Appendix for reference methodologies (MR) Compliance Assessment

Version Date 2026-09-22

©2026 Viedoc Technologies AB

Disclaimer

No part of this document may be modified, copied, or distributed without prior written consent from Viedoc Technologies AB. The information contained herein is subject to change without notice. Viedoc Technologies AB shall not be liable for technical or editorial errors or omissions contained herein.

Document History

Version	Author	Date	Change
1	Predrag Gaic	2026-09-22	Initial version

Contents

1	BACKGROUND	3
1.1	Abbreviations.....	3
1.2	Scope.....	4
2	TECHNICAL AND ORGANISATIONAL REQUIREMENTS	4
2.1	Robust Access Controls & Identification	4
2.2	Traceability and Quality Control	5
2.3	Data Protection Technical Measures.....	5
2.4	Vulnerability & Operations Management.....	5
3	SECURITY REQUIREMENTS FROM CNIL SECURITY APPENDIX.....	5
3.1	General Security measures	6
3.2	Security measures for delivering the information notice in electronic format	12
3.3	Security measures for the review and publication of results	15
3.4	Non-identifying code	16
4	APPENDICES.....	18

1 BACKGROUND

France's CNIL updated its Reference Methodologies MR-001 (consent-based health research) and MR-003 (non-consent research) on May 23–26, 2026, introducing mandatory security and quality control annexes and streamlined compliance self-declarations.

Core Scope and Updates:

- MR-001 Application: Governs interventional clinical research involving human participants where informed consent is collected.
- MR-003 Application: Covers health research studies that do not require patient consent under specific legal exemptions.
- New Binding Annexes: Both frameworks now require strict adherence to companion [MR-003 annotated - CNIL](#) security and quality control annexes governing data accuracy and audit trails.
- Clarified Roles: Research sites are no longer classified as data processors, and joint controllership is formally acknowledged with individual declarations required.
- Territorial Scope: Explicitly applies to non-French sponsors if data subjects are located in France.
- Operational Modernization: Permits electronic disclosures for transparency under reinforced technical safeguards and mandates compartmentalized access barriers for data recipients.

1.1 Abbreviations

CNIL - (Commission Nationale de l'Informatique et des Libertés) is the independent data protection authority for France. Established by law in 1978, its primary mandate is to ensure that data privacy laws are correctly applied to the collection, storage, and use of personal data, which includes enforcing the European Union's General Data Protection Regulation (GDPR) within France.

GDPR - European Union's General Data Protection Regulation.

MR-001 - CNIL's MR-001 is a pre-approved compliance framework under the GDPR for interventional health research and clinical trials in France that require participant consent.

MR-003 - CNIL's MR-003 is the simplified, pre-approved compliance framework under the GDPR for health research and non-interventional studies in France where explicit participant consent is not required.

1.2 Scope

The official text of the **Security Annex (MR-SEC)** is not issued as a standalone document, but rather integrated directly by the [French Data Protection Authority \(CNIL\)](#) as a mandatory, binding extension of both the [MR-001 Reference Methodology](#) and [MR-003 Reference Methodology](#). Compliance with this annex is a strict condition for filing a simplified self-declaration.

Viedoc Technologies is a Software as a Service provider for the primary purpose of collecting research data from research sites in a clinical trial. In addition to data collection, Viedoc contains several supporting features used to perform data verification, site monitoring, randomization, supply management, medical coding, adverse event reporting, user training, and certification.

Viedoc customer can either be a so-called sponsor—the financier of the project—or a subcontractor of the project sponsor. A sponsor is typically a pharmaceutical company, a biotechnology or medical device company, or an academic institution. A subcontractor is typically a Contract Research Organization (CRO).

Our interpretation is that the CNIL Security Annex for security reference (MR) is written as a requirement for the Sponsor so the compliance analysis in this document is from the angle of does our product support the sponsor in the requirements that apply to our role in the clinical.

2 TECHNICAL AND ORGANISATIONAL REQUIREMENTS

The core technical and organizational security requirements detailed in the CNIL Security Annex for security reference (MR) include:

2.1 Robust Access Controls & Identification

- **Stricter Access Segregation:** Compartmentalized access barriers must ensure that only authorized personnel can view specific tranches of health data.
- **Multi-Factor Authentication (MFA):** Implementing MFA is mandatory. The CNIL outlines specific rolling deadlines:
 - January 1, 2027: Mandatory for all web-based applications and remote interfaces.

- January 1, 2028: Mandatory for all other internal systems and endpoints processing the study data.
- Least Privilege: System rights must strictly reflect the user's role in the protocol (e.g., separating investigators, monitors, and statisticians).

2.2 Traceability and Quality Control

- Enhanced Logging (Audit Trails): Every action taken on the data (creation, modification, extraction, deletion) must produce an unalterable, non-significant, automatically generated log event.
- Alignment with Quality Annex: Data entry and audit modifications must map precisely to verification workflows so remote quality controls can be safely conducted.

2.3 Data Protection Technical Measures

- Data Encryption: Health data must be encrypted both at rest and in transit across network layers using state-of-the-art cryptographic standards.
- Pseudonymization Rules: Compliance codes must use non-significant identifiers generated in strict alignment with guidelines MR-CNS-01 to 04 within the security framework to avoid re-identification vectors.
- Secure Backups & Redundancy: Processes must detail the isolation and protection of system backups to guarantee resilience against ransomware or physical data loss.

2.4 Vulnerability & Operations Management

- Penetration Testing: Regular, documented penetration and vulnerability assessments are required on infrastructure hosting the research databases.
- Vendor & Subcontractor Compliance: Formal data processing agreements must legally bind your providers to the exact technical requirements detailed under this security annex.

3 SECURITY REQUIREMENTS FROM CNIL SECURITY APPENDIX

The security requirements described in the CNIL Security Annex for security reference (MR) are listed in the tables below. The table also lists Viedoc's assessment of how the Viedoc platform meets each requirement.

NOTE: The original Security Annex (MR-SEC) is published only in French and the terms in the tables below have been translated to English from the original document.

3.1 General Security measures

Number	Title	Security requirement	Viedoc Status
Preparation and Design			
MR-SEC01	Steering data protection	Identify the stakeholders competent in data protection and information security, including the data protection officer and the information systems security manager. Ensure that the research project complies with the organization's general data protection policy.	Implemented
MR-SEC02	Security by design	Integrate data protection and security measures from the design phase of the research. Involve stakeholders competent in data protection and information security in the design of research protocols and in the ongoing monitoring of the project.	Implemented
MR-SEC03	Risk assessment	Minimize the data processed (filtering, transformation, reduction, aggregation, purging, etc.) as early as possible and at every stage of the research.	Implemented
Minimization and pseudonymization			
MR-SEC04	Data minimization	Minimize the data processed (filtering, transformation, reduction, aggregation, purging, etc.) as early as possible and at every stage of the research.	Implemented
MR-SEC05	Separation by data type	Where research requires individual follow-up of persons participating in the research, separate administrative data (surname, first name, permanent patient identifier, etc.) from health data concerning these persons.	Implemented
MR-SEC06	Pseudonymization	Index research data using a non-identifying code, applying requirements MR-CNS-01 to 04.	Implemented

Number	Title	Security requirement	Viedoc Status
		Define the procedures for re-identifying persons participating in the research.	
MR-SEC07	Medical images	Pseudonymize medical images by masking identifying data and removing identifying metadata. Take into account, in the risk assessment, the presence of visual features that could allow re-identification of individuals (for example, tattoos, prostheses, malformations), and implement appropriate measures to reduce the possibility of re-identification (for example,	Implemented
MR-SEC08	Data purging	Erase data from the active database upon expiry of its retention period.	Implemented
Data protection			
MR-SEC09	Data encryption	Secure data at rest and in transit, using encryption or equivalent security measures. Use state-of-the-art, recognized and secure cryptographic algorithms. Define a secret key management policy. Protect secret keys with restrictive access rights and strong passwords.	Implemented
MR-SEC10	User identification	Define a unique identifier for each user and prohibit accounts shared between several users.	Implemented
MR-SEC11	Passwords	Comply with the CNIL recommendation on passwords.	Implemented
MR-SEC12	Multi-factor authentication	Make access to the personal data of persons participating in the research conditional on multi-factor authentication, involving at least two distinct authentication factors.	Implemented
MR-SEC13	Access management	Define access profiles by separating tasks and areas of responsibility, so as to limit users'	Implemented

Number	Title	Security requirement	Viedoc Status
		access to only the data strictly necessary for carrying out their duties. Have any request for an access profile validated by a line manager. Limit access to functional administration tools and interfaces to authorized persons only. Modify users' access profiles in the event of a change of assignment or position, or at the end of their contract. Carry out a regular review, at least annually, of access rights.	
MR-SEC14	Logging	Implement a system for logging users' business activities, technical interventions, anomalies, and security-related events. Identify any health data that may be present in the logs, minimize it, and secure the logs accordingly. Proactively analyze the collected logs, in real time or in the short term, so as to be able to detect the occurrence of an incident.	Implemented
MR-SEC15	Paper documents	Secure existing paper documents (storage, transmission, destruction).	Not applicable
Securing tools and equipment			
MR-SEC16	Securing the IT estate	Enable automatic device locking and require a secret to unlock devices. Encrypt devices. Disable automatic program execution. Limit administration rights to the strict operational need.	Implemented
MR-SEC17	Physical security	Restrict and control physical access to premises hosting the data.	Implemented

Number	Title	Security requirement	Viedoc Status
MR-SEC18	Protection against malicious software	Install and regularly update antivirus software, firewalls, and intrusion detection systems on all servers and workstations controlled by the data controller. Deploy security updates promptly, particularly when they fix publicly known critical vulnerabilities.	Implemented
MR-SEC19	Segregation of health data	Segregate the processing of health data from the rest of the organization's information system. Use software dedicated to the research (electronic case report forms, questionnaires, etc.) hosted on servers dedicated to the research.	Implemented
MR-SEC20	Management of removable media	Prohibit the use of removable media (USB drives, external hard drives, etc.) not controlled by the data controller. Where controlled removable media are used, encrypt the data on such media and delete it after use. Deploy solutions to inspect the content of media as soon as they are connected.	Implemented
MR-SEC21	Uncontrolled equipment	Prohibit the use of personal equipment ("bring your own device") to access research data. Where uncontrolled professional equipment is used, assess the associated risks, define specific risk-reduction measures, and limit accordingly the data and applications accessible on those devices. Formally document in writing the responsibilities and precautions to be observed.	Implemented
Collaboration and subcontracting			

Number	Title	Security requirement	Viedoc Status
MR-SEC-22	Governing subcontractors (processors)	Set out the parties' obligations regarding the security of the processing in the contract with subcontractors. Ensure that subcontractors are contractually required to notify the data controller of any anomaly or security incident as soon as possible.	Implemented
MR-SEC-23	Remote exchanges	Protect flows and recordings during teleconsultations and remote interviews. Verify the identity of the persons contacted. Secure the electronic sending of documents, in particular information notices and remote quality control.	Implemented
MR-SEC-24	Data transmission	Secure data exchanges (for example, transfers from investigating centers). When sending over a public network (for example, the internet, e-mail), encrypt the data using state-of-the-art, recognized, and secure cryptographic algorithms. Ensure the confidentiality of the encryption key by transmitting it via a separate channel.	Implemented
Documentation and awareness			
MR-SEC-25	Documentation	Document data operating procedures. Keep them up to date and make them available to all users concerned, in language that is clear and suited to each category of user.	Implemented
MR-SEC-26	User awareness	Raise awareness among all users (internal and external) working with personal data of the risks to individuals' freedoms and privacy, as well as of the obligations relating to medical confidentiality and the processing of health data.	Implemented

Number	Title	Security requirement	Viedoc Status
		Inform them of the measures taken to address these risks and of the potential consequences of non-compliance. Ensure that they have absorbed the good practices for personal data protection to be applied on a day-to-day basis.	
Incident management and backups			
MR-SEC-27	Incident management	Distribute to all users, internal and external, the procedure to follow and the list of persons to contact in the event of a data breach, security incident, or the occurrence of an unusual event affecting the organization's information and communication systems. Raise users' awareness of the importance of reporting any suspicious event.	Implemented
MR-SEC-28	Regular backups	Perform frequent backups of data. Protect backed-up data with security measures appropriate to a level of risk equivalent to that of operational data. Regularly check their integrity and the ability to restore them. Delete backups once their retention period has expired.	Implemented
End of lifecycle			
MR-SEC-29	Data management after publication	Define a secure archiving policy for the data after publication, specifying in particular the retention periods, the access conditions, and the procedures for purging or transferring to the National Archives.	Not applicable
MR-SEC-30	Secure destruction of data	At the end of the research project, securely erase the data present on all IT equipment (for	Not applicable

Number	Title	Security requirement	Viedoc Status
		example, workstation, server, hard drive) and retain only the data provided for by the archiving policy defined (MR-SEC-29). In the event of reassignment or disposal of IT equipment during the project, securely erase the data present on it beforehand.	

3.2 Security measures for delivering the information notice in electronic format

Number	Title	Security requirement	Status
MR-INF01	Dematerialized information notice	Individual information for persons participating in the research is delivered in electronic format, in compliance with the conditions set out in requirements MR-INF-02 to 04.	Not applicable
MR-INF02	Information by simple e-mail	Where the information notice does not reveal any information about the state of health of the person participating in the research, it may be sent by simple e-mail, provided that the data controller ensures that the e-mail address is a personal, individual address that is actually used by the person participating in the research or by their legally authorized representatives.	Not applicable
MR-INF03	Information by e-mail with an access code	Where the information notice is likely to reveal information about the state of health of the person participating in the research, it may be sent by e-mail provided that the	Not applicable

Number	Title	Security requirement	Status
		following cumulative conditions are met: - the body and subject line of the message must not contain any information likely to reveal information about the state of health of the person participating in the research; - access to the information notice must be conditional on possession of a knowledge factor (for example, the information notice may be an encrypted attachment, or the message may contain a link to a secure download platform requiring a secret code); - the decryption or download code must be transmitted via a separate trusted channel (for example, hand delivery, a phone call or SMS to a verified phone number, or secure postal mail); - where a secure download platform is used, a limited availability period must be configured.	
MR-INF04	Information via a secure platform	Where the information notice is likely to reveal information about the state of health of the person participating in the research, it may be transmitted via a secure platform for which the person participating in the research has an authenticated connection, ensuring that the message will be read only by its intended recipient.	Implemented

Number	Title	Security requirement	Status
		A notification must be sent by the platform to the recipient inviting them to log in. This notification must not contain any information likely to reveal information about the state of health of the person participating in the research.	

3.3 Security measures for the review and publication of results

Number	Title	Security requirement	Status
MR-PUB01	Data minimization for the review of results	For the review of results, the data made available to independent experts must consist solely of minimized (MR-SEC-04) and pseudonymized (MR-SEC-06) data used to obtain the published results and strictly necessary for their review.	Not applicable
MR-PUB02	Secure solution for the review of results	The solution used to make data available for review must ensure: - the granting of authorizations offering differentiated access to data; - authentication of users; - the use of encrypted communication channels; - the use of state-of-the-art encryption algorithms and secret management procedures; - the implementation of measures to trace access to data.	Not applicable
MR-PUB03	Restrictions on the ability to copy data	Persons accessing the data made available must not be able to copy or extract it (for example, by blocking screen captures, copy/paste, or downloads).	Not applicable

3.4 Non-identifying code

Number	Title	Security requirement	Status
MR-CNS-01	Indexing data using a non-identifying code	Where it is necessary to link together data relating to the same person participating in the research, within a set of pseudonymized data or between several sets of pseudonymized data, indexing must be carried out solely by means of a non-identifying code meeting requirements MR-CNS-02 to 04.	Not applicable
MR-CNS-02	Non-identifying code	A non-identifying code must not reveal any information about the data subject or about pre-existing identifiers linked to that person. It must not contain pre-existing identifiers, nor a truncation or concatenation of them. In particular, it must not contain information relating to the identifying traits of data subjects (for example, initials, date of birth), to care (national health identifier/NIR-INS, permanent patient identifier/IPP, stay identifier/IEP), to the data collection phase (inclusion number, biological sample tube number), or to the identifier used in a source dataset. It must be generated specifically for the dataset.	Not applicable
MR-CNS-03	Methods for generating the non-identifying code	A non-identifying code must be generated using one of the following two methods:	Not applicable

Number	Title	Security requirement	Status
		- the use of a random value generator (for example, a pseudo-random number generator, "PRNG"); - derivation from a pre-existing identifier by means of a hash function keyed with a secret key. The hash function used must be a state-of-the-art cryptographic function. The secret key must be governed by a key management policy.	
MR-CNS-04	Governing the means of re-identification	The data controller must ensure that it is not possible to link a non-identifying code to other identifiers concerning persons participating in the research without access to additional information — namely, the correspondence table between the non-identifying code and a pre-existing identifier, or the secret key used to generate the code by means of a hash function. This additional information must be retained only where it is strictly necessary to be able subsequently to link the non-identifying code to other identifiers concerning persons participating in the research. Access to it must be strictly controlled and limited to a restricted number of duly authorized persons.	Not applicable

4 APPENDICES

- COMDOC58 Data Protection Impact Assessment
- COMDOC22 Information Security SOA
- ISO27001:2022 Certificate
- SOC 2 Type 2 Report