Deliberation 2022-107 of September 22, 2022National Commission for Computing and LibertiesNature of the deliberation: Referential/standard regulation/standardLegal status: In force Date of publication on Légifrance: Friday December 02, 2022NOR: CNIL2231479XDeliberation n° 2022-107 of September 22 2022 adopting a reference system relating to the processing of personal data implemented by the laboratory holding the rights to use a medicinal product benefiting from an early access authorizationThe National Commission for Computing and Liberties (CNIL), Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (regulation General on Data Protection), in particular its Article 58; Having regard to the public health code; Considering the modified law n° 78-17 of January 6, 1978 relating to data processing, files and freedoms, in particular its articles 8 I 2° b and 66; After having heard the report of Mrs Valérie PEUGEOT, commissioner, and the observations by Mr. Benjamin TOUZANNE, Government Commissioner; Adopts a standard relating to the processing of personal data implemented by the laboratory holding the rights to use a medicinal product benefiting from an early access authorisation.APPENDIX THE LABORATORY HOLDING THE RIGHTS TO USE A MEDICINE BENEFITING FROM AN EARLY ACCESS AUTHORIZATIONYou can consult the full text with its images from the authenticated electronic Official Journal extract;1. Definitions Within the meaning of this standard, the following terms are thus defined, as provided for in the General Data Protection Regulation (GDPR): 1.1. Personal data: any information relating to an identified or identifiable natural person (hereinafter referred to as "data subject"); is deemed to be an "identifiable natural person" a natural person who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier, or to one or more specific elements specific to his physical, physiological, genetic, psychological, economic, cultural or social identity.1.2. Processing: any operation or set of operations carried out or not using automated processes and applied to data or sets of personal data, such as the collection, recording, organization, structuring, storage, adaptation or modification, extraction, consultation, use, communication by transmission, dissemination or any other form of making available, reconciliation or interconnection, limitation, erasure or destruction.1.3. Data controller: the natural or legal person who, alone or jointly with others, is responsible for an early access authorization, manages it, monitors patients, checks that its funding is provided and who determines the purposes and means of the processing necessary for it.1.4. Representative: a natural or legal person established in the Union, designated by the controller or processor in writing, pursuant to Article 27, who represents them with regard to their respective obligations under the General Regulation on data

protection.1.5. Processor: the natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. These include, for example, providers of electronic platforms, establishments within which the collection of personal data is ensured, or a provider of health data hosting services.1.6. Recipient: the natural or legal person, public authority, service or any other body that receives communication of personal data, whether or not it is a third party.1.7. Third party: a natural or legal person, a public authority, a service or an organization other than the data subject, the controller, the processor and the persons who, placed under the direct authority of the controller or the -processor, are authorized to process the personal data.1.8. Genetic data: personal data relating to the hereditary or acquired genetic characteristics of a natural person which give unique information on the physiology or the state of health of this natural person and which result, in particular, from an analysis of a biological sample of the natural person in question.2. Who is this reference for? 2.1. This reference framework exclusively governs the processing of personal data: implemented by the company which ensures the exploitation of the medicinal product having an early access authorization, hereinafter the data controller; and whose purposes are the availability of the medicinal product under early access authorization and monitoring of patients treated with a medicinal product within the framework of such authorisation.2.2. This reference document covers the processing of personal data relating to the monitoring of patients treated with a medicinal product with an early access authorization implemented from the date of entry into force of this reference document.2.3. This standard concerns data controllers established in France or who use the services of a subcontractor established in France or who implement the processing of personal data relating to persons residing in France (patient, person affected, healthcare professional), regardless of their place of establishment. In the event that the data controller is not established on the territory of the European Union, he is required to designate by written mandate a representative established in the European Union in accordance with Article 27 of the General Regulation on the data protection (GDPR).2.4. This standard is not applicable: to the processing of personal data implemented by health professionals and health care systems or services (e.g.: health establishments, health agencies, etc.) in application of the provisions of 1° of article 65 of the "data-processing and freedoms" law (for example: medical file, computerized patient file); to the processing of personal data implemented by pharmaceutical companies for traceability purposes medicines; to the processing of personal data implemented by pharmaceutical companies for pharmacovigilance management purposes (1); to the processing of personal data implemented for the performance of the compensation agreement mentioned in Article R. 5121-70 of the Public Health Code (CSP); to the processing of personal data implemented within the framework of a

compassionate access authorization or a compassionate prescription framework provided for in Article R. 5121-70 of the Public Health Code (CSP); article L. 5121-12-1 of the CSP.3. Scope of the standard3.1. This standard specifies the legal framework, resulting from the GDPR and national provisions, applicable to the processing of personal data constituted for the provision of the medicinal product under early access authorization, as well as the monitoring of patients treated with a medicinal product under authorization. early access.3.2. Data controllers who make a declaration of compliance with this standard to the CNIL are authorized to implement the processing of personal data for the purpose of providing a medicinal product under authorization for early access and monitoring. of patients if it strictly complies with the reference system.3.3. Any processing of personal data for the purpose of making a medicinal product available under early access authorization and monitoring patients that does not comply with all the requirements defined by these standards must be subject to a request for specific authorization, in accordance with the provisions of article 66 III of the law "data-processing and freedoms".3.4. Data controllers must implement all appropriate measures (technical and organizational) to guarantee the protection of the personal data processed, both from the design of the processing and by default. They must also demonstrate this compliance throughout the life of the treatments. The processing of personal data implemented within the framework of this standard must also be recorded in the register of processing activities provided for in article 30.1 of the GDPR.3.5. The principles set out by the CNIL, in this reference document, constitute an aid to carrying out the impact analysis relating to data protection (AIPD) that the data controllers concerned must carry out (article 14 of this reference document). Data controllers will thus be able to define the measures allowing them to ensure the proportionality and necessity of their processing, to guarantee the rights of individuals and to control the risks presented by their processing.4. Controllers and processors4.1. In the context of this standard, the organization or establishment within which the collection of personal data is carried out acts as subcontractors for the collection and transmission of personal data to the controller. These establishments and, where applicable, the health professionals involved in the care of the patient, remain responsible for the processing for which they define the purposes and means, in particular for the purposes of keeping and managing medical records.4.2. Also qualified as a subcontractor is any organization involved in the processing and meeting the definition of article 1.5 of these standards, in particular the supplier of an electronic platform for entering personal data relating to the follow-up of patients treated by a medicinal product with early access authorisation.4.3. In the event of recourse to a subcontractor, the service must be carried out under the conditions provided for in Article 28 of the GDPR. A subcontracting contract must be concluded between the service provider and the

data controller. This contract must in particular: specify the distribution of responsibilities relating to security measures and the management of data breaches between the various actors; provide for the conditions for the restitution and destruction of data; provide the procedures for the data controller to ensure the effectiveness of the guarantees provided (security audits, visits, etc.); specify the terms and conditions under which the subcontractor helps, as far as possible, the data controller to fulfill his obligation to follow up to requests to exercise the rights of data subjects.4.5. Each subcontractor must keep a record of the processing activities carried out on behalf of a data controller under the conditions of article 30.2 of the GDPR.4.6. In the event that the data controller uses the services of a subcontractor for the hosting, storage or retention of health data, this subcontractor must be an approved or certified health data host according to the provisions of CSP.5. Objective(s) pursued by the processing (Purposes)5.1. The processing of personal data implemented within the framework of an early access authorization is intended to allow the verification of the patient's eligibility for the drug and the monitoring of the patients benefiting from it.5.2. To do this, the processing of personal data aims to allow: the collection, recording, analysis, monitoring, documentation, transmission and storage of data relating to access, initiation, monitoring and discontinuation of drug prescriptions within the framework defined by Article L. 5121-12 of the CSP; management of contacts with healthcare professionals involved in the monitoring of patients receiving early access drugs and the personnel acting under their responsibility or authority; with regard to the summary reports, mentioned in article R. 5121-70-1 of the CSP, and only if they contain personal data, the evaluation of the medicinal products having benefited from early access authorization by the French National Authority for Health (HAS).5.3. The personal data collected for these purposes may be reused only under the conditions provided for by the GDPR and the "Informatique et Libertés" law applicable to the processing of personal data implemented for research, study or information purposes. assessment in the field of health, and subject to the completion of the prior formalities required with the CNIL. In addition, the storage of personal data with a view to their reuse for the purposes of research, study or evaluation in the field of health (health data warehouse) is also subject to compliance with the conditions laid down by the GDPR and the law "Informatique et Libertés", as well as the completion of the prior formalities with the CNIL, except in the case of collection of the express consent of the person.5.4. These subsequent reuses constitute data processing distinct from that implemented for the purposes defined in Article 5.2.6. Legal basis(s) of the processing6.1. In the context of this reference system, the legal obligations imposed on the data controller, in particular in article L. 5121-12, as well as in articles R. 5121-68 and following of the CSP, are retained as legal bases for the processing of personal data in accordance

with the provisions of Article 6.1.c of the GDPR.6.2. The collection of sensitive data for the purposes mentioned in article 5 of this standard is necessary for reasons of public interest in the field of public health; its main objective is to guarantee compliance with high standards of quality and safety of health care and medicines, in accordance with the provisions of Article 9.2.i of the GDPR and Article 66 of the "Informatique et Libertés" law. ".7. Personal data concerned7.1. Only data that is adequate, relevant and limited to what is necessary for the purposes pursued may be processed, namely the provision of the medicinal product with an early access authorization, as well as the monitoring patients treated with a medicinal product concerned by the early access authorization, under the conditions and according to the specificities provided for in article L. 5121-12, as well as in articles R. 5121-68 and following of the CSP.7.2 . As such, depending on the objective pursued by the processing of personal data, the medicinal product concerned and the situations, in accordance with the therapeutic use and data collection protocol (PUT-RD) defined by the HAS and drawn up , where applicable, in conjunction with the National Agency for the Safety of Medicines and Health Products (ANSM), the data controller may collect and process: a) data relating to patients: patient identification data: three first letters of the surname and first two letters of the first name, number, alphanumeric code or alphabetic code, identifying information (sex, weight, height, age or year and month of birth or full date of birth if necessary in a pediatric context), exclusion of the registration number in the national personal identification directory (NIR) and the national health identifier (INS); data relating to the characteristics of the population benefiting from the medicinal product under early access authorization involving the information on the health of the patient, in particular the history of the disease, the personal or family history, the pathologies or associated events; data relating to the conditions of use of the drug involving in particular the concomitant treatments, information relating to the mode of prescription, dispensation and use of the medicinal product as well as the therapeutic behavior of the prescriber; data relating to the efficacy of the medicinal product; data relating to the quality of life involving in particular the questionnaires and their results; data relating to the safety of the medicinal product: nature and frequency of adverse effects. In addition to this data, the data controller may also collect and process the following data provided that it is strictly necessary with regard to the product prescribed and the pathology in question: ethnic origin; data genetic data, excluding the complete genome; sex life; consumption of tobacco, alcohol and drugs; b) where applicable, the data collected concerning persons related to the patient, only if taking the drug has affected them (partner, offspring), in particular the identification data including the link with the patient, the efficacy data and the data relating to adverse effects as described in article 7.a; c) the data relating to health professionals involved in the monitoring of

patients benefiting from early access medicines (in particular prescribing doctors and dispensing pharmacists) and staff acting under their responsibility or authority: surname, first name, specialty, registration number in the shared directory of healthcare professionals (RPPS), professional contact details.7.3. The media allowing the collection of the aforementioned data must exclude the use of free entry areas, for example in the form of "notepads". Concerning, more particularly, data relating to quality of life collected via questionnaires directly from patients, only questionnaires validated by the competent authorities may be used.8. Accessors and recipients of data8.1. The personnel of the establishments involved in the care of the person may collect the data, within the strict limits of the missions entrusted to them.8.2. The authorized personnel of the data controller may, under the latter's responsibility, access the personal data processed, within the limits of their respective powers and as far as they are concerned, in particular: the pharmacist in charge or his representative as well as any person duly authorized and placed under his responsibility; the person in charge of pharmacovigilance as well as the collaborators placed under his responsibility; the members of the departments in charge of medical affairs, research and development, regulatory affairs, market access; the members of the service in charge of managing orders, the supply and the distribution of medicines; the members of the service in charge of audits can, on an ad hoc and motivated basis, have access to this data to check compliance with the requirements regulations and internal procedures.8.3. May be recipients of the data, under the responsibility of the data controller: the authorized personnel of the subcontractors acting on behalf of the data controller, within the limits of their functions, their respective attributions and under the conditions defined by the subcontract -contracting; the authorized personnel of other companies in the group to which the data controller belongs who participate in the implementation of the early access authorization or who set up an early access program for the medicinal product at national or European level or international, within the limits of their respective attributions; national or foreign public bodies in charge of the regulation, evaluation and monitoring of medicinal products, within the framework of the exercise of their missions as defined by the texts , in particular the ANSM, the HAS, the regional pharmacovigilance centers and the poison control centres, or the organizations in charge of monitoring medicinal products benefiting from early access authorisation.9. Storage periods9.1. The data processed are kept in an active database for a maximum of two years following the publication by HAS, if necessary after consulting the ANSM, of the summary of the last summary report provided for in Article R. 5121-70-1 of CSP.9.2. The data is then archived in an intermediate database for the duration of the marketing authorization (MA) relating to the therapeutic indication having been the subject of an early access authorization. They may not be stored, depending on the

medicinal product concerned, the therapeutic indication targeted and the legislative and regulatory provisions in force, beyond a period of seventy years from the date of withdrawal from the market of the medication.9.3. If no Marketing Authorization is granted to the pharmaceutical specialty concerned or if the early access authorization is suspended or withdrawn, the data cannot be archived in an intermediate database beyond a period of seventy years from of: the expiration of the HAS decision granting the non-renewed early access authorization or the last HAS decision authorizing its renewal; the date of the HAS decision pronouncing the suspension or withdrawal of the early access authorization.9.4. At the end of these periods, the data is deleted or archived in an anonymous form.9.5. The storage and archiving of data must be carried out under security conditions in accordance with the provisions of article 32 of the GDPR.10. Information of persons10.1. Processing of personal data must be implemented in full transparency vis-à-vis the persons concerned (patients undergoing treatment with a medicinal product under early access authorization and/or their legal representatives, professionals involved in the care of patients, people who may be affected by taking the drug). The data controller takes the appropriate measures to provide data subjects and/or their legal representatives with concise, transparent, understandable and easily accessible information, in clear and simple terms.10.2. With regard to patients and/or their legal representatives, the methods of information are as follows: in accordance with article L. 5121-12 of the CSP, the prescribing doctor must inform the patient and/or his legal representatives that the prescription of the medicinal product is not carried out within the framework of an MA but within the framework of an early access authorization, the risks incurred, the constraints and the benefits likely to be provided by the medicinal product; access to treatment, the prescribing doctor provides the patient and/or his legal representatives with an information note, in accordance with the provisions of Articles 13 and, where applicable, 14 of the GDPR, as well as Articles 69 and 70 of the law "data-processing and freedoms"; it is recalled that the patient and/or his legal representatives are free to accept or refuse the treatment by a drug prescribed under authorization of early access. If treatment is accepted, Articles L. 5121-12 et seq. and R. 5121-70 of the CSP et seq. require the collection of personal data relating to patient monitoring; the patient may be assisted by the trust he has designated pursuant to Article L. 1111-6 of the CSP.10.3. With regard to persons in contact with the patient and who are affected by taking the medicine, the information procedures are as follows: if the healthcare professional has collected this data directly from the person, he gives them, within the respect for medical secrecy, an information note in accordance with the provisions of article 13 of the GDPR as well as articles 69 and 70 of the law "Informatique et Libertés"; if the health professional has indirectly collected this data, he to the patient an information note intended for the person affected

by taking the medicine, in accordance with the provisions of article 14 of the GDPR as well as articles 69 and 70 of the "data-processing and freedoms" law. On this occasion, the professional informs the patient and/or his legal representatives of the consequences that this information will have with regard to the secrecy of the information concerning him.10.4. In addition, the data controller is required to make available on its website the information notices relating to the processing of personal data implemented which must comply with the provisions of the GDPR.10.5. With regard to healthcare professionals involved in the care of the patient, the information media include the information provided for in Articles 13, where applicable, 14 of the GDPR.10.6. If an electronic platform is used to collect the data mentioned in article 7, healthcare professionals must be informed when they first connect to this platform.10.7. In the event that personal data collected in accordance with these standards are reused for the purposes of research, study or evaluation in the field of health, new individual information for the persons concerned is required, unless: the data subject already has the information provided for in Articles 13 or 14 of the GDPR concerning this further processing; the information provided during the collection of the data within the framework of an early access authorization provides for the possibility of reuse the data, and refers to a specific information system (for example: a transparency portal available on a website) to which the persons concerned can refer prior to the implementation of each new data processing operation.11. Rights of persons11.1. The persons concerned by the processing and/or their legal representatives (patients, persons affected by the taking of the processing in connection with the patient and healthcare professionals) have the following rights: right of access; right of rectification; right of limitation (for example, when the person disputes the accuracy of their data, they can ask the data controller to temporarily freeze their data while the latter carries out the necessary checks).11.2. In accordance with article L. 1111-6 of the CSP, the patient may be accompanied in his steps by the trusted person he has designated.11.3. Insofar as the processing of personal data is based on compliance with a legal obligation and pursues an objective of public interest in the field of public health, the persons concerned have neither the right of opposition nor the right to erasure, or the right to data portability. The persons concerned are informed beforehand.11.4. With regard to the patient, his rights are exercised at any time with the health professional involved in his care or through the doctor of his choice. He can also exercise his rights directly with the data controller. In this case, the patient is informed of the consequences on the confidentiality of his data.11.5. With regard to persons in contact with the patient and who are affected by the taking of the medicinal product, these rights are exercised under conditions compatible with the provisions relating to medical and professional secrecy. More specifically, the exercise of the rights of these persons must not lead the laboratory to

communicate information covered by medical secrecy. If the exercise of the rights of the person in connection with the patient and who is affected by taking the medicine requires the data controller to reveal confidential information concerning the patient, the data controller must inform the person in connection with the patient and may not respond to his request to exercise his rights.11.6. With regard to healthcare professionals involved in patient care, their rights are exercised directly with the data controller.12. Transfer of data outside the European Union (2)12.1. Indirectly identifying data of patients, persons related to the patient who are affected by taking the medicine and directly identifying data of healthcare professionals may only be transferred outside the European Union if the following conditions are met: the provisions of article 8 relating to the recipients of the data are respected; the transfer is strictly necessary for the provision of the medicinal product under early access authorization and the monitoring of patients treated with a medicinal product object of such authorisation.12.2. In addition, the transfer can be carried out within the framework of the declaration of conformity with this standard only if one of the following conditions, provided for in Chapter V of the GDPR, is met: the transfer is made to a country or an international organization recognized by the European Commission as providing an adequate level of protection, in accordance with Article 45 of the GDPR (adequacy decision); the transfer takes place subject to appropriate safeguards, listed in Article 46.2, of the GDPR (in particular: standard contractual clauses approved by the European Commission, binding corporate rules, code of conduct, certification mechanism) and, where applicable, additional measures if the legislation of the country to which the data is exported is an obstacle compliance with contractual guarantees (3); in the absence of an adequacy decision or appropriate guarantees, the transfer may be based on one of the exceptions provided for in Article 49 of the GDPR provided that the specific conditions , of strict interpretation, set out in this article apply (4).12.3. The data controller must have previously informed the persons concerned of the transfer of their personal data to countries outside the European Union, of the existence or absence of an adequacy decision or appropriate guarantees, and finally the means to obtain a copy in accordance with articles 13.1.f and 14.1.f of the GDPR.12.4. Any remote access to data from outside the territory of the European Union (viewing) is considered a transfer.13. Security13.1. In general, the data controller and his or her subcontractor(s), including the establishments responsible for collecting the data, must take all the necessary precautions with regard to the risks presented by the processing, to preserve the security of the data. personal data and, in particular, at the time of their collection, during their transmission and their storage, to prevent them from being altered, damaged, lost or that unauthorized third parties have access to them. 13.2. The controller defines, implements and monitors the application of a

security policy which must in particular describe the measures meeting the processing security requirement provided for in Article 32 of the GDPR.13.3. In particular, in the context of this standard, the data controller and its subcontractors must adopt the following technical and organizational measures, measures which must be read in the light of the other regulations applicable to the security of information systems in health, in particular the general security policy for health information systems (PGSSI-S): Requirement numbers Security requirements Educate users SEC-SEN-1 Inform and educate people handling data Each person authorized to access the data concerned by this framework must be trained to respect professional secrecy and be regularly made aware of the risks and obligations inherent in the processing of personal data, and in particular health data and special categories of personal data (such as genetic data or data revealing ethnic origin of the patient). SEC-SEN-2Draft an IT charter and give it binding forceEach person authorized to access the data processed within the framework of processing governed by this standard must undertake to respect a confidentiality charter specifying in particular the sanctions in the event of non-compliance.Authenticate usersSEC-AUT-1Define a unique identifier (login) for each userEach person authorized to access the data processed within the framework of processing governed by this standard must have a unique and individual identifier. Accounts shared between several users are to be avoided.SEC-AUT-2Set up user authenticationThe data controller sets up strong multi-factor authentication involving at least two distinct authentication factors for all users and administrators, for example by using an identifier coupled with a password and a one-time password generated via a cryptographic protocol. Authentication of healthcare professionals, in the event that data collection is carried out by means of he interface allowing the electronic entry of data is provided by the dematerialized service provided for in II of article R. 5121-70 of the CSP. In any case, this authentication must comply with the requirements of the PGSSI-S, in its section relating to the electronic identification of actors in the health, medico-social and social sectors, applicable to natural persons.SEC-AUT-3 Adopt a user password policy that complies with the recommendations of the CNIL a recommendation relating to passwords and other shared secrets and repealing deliberation no. 2017-190 of June 22, 2017, or any other subsequent update of this recommendation.SEC-AUT-4Require the user to change his password password after resetThe user must change any password assigned by an administrator or automatically by the system during account creation or a reset.SEC-AUT-5Limit the number of attempts to access an accountThe responsible for processing must provide for a limit on the number of access attempts to any electronic platform used to collect the data processed in the context of processing governed by this standard and set up a temporary blocking of access when the limit is reached .Manage

authorizationsSEC-HAB-1Define authorization profilesDifferent authorization profiles must be provided in order to manage access to data as needed and exclusively, for a fixed and limited period.Granularity of data access must be provided for each type of profile, for example access only to aggregated data, access to pseudonymised data or access to directly identifying data. Access to health data should also be distinguished from access to other data. Privileged access with extended rights, in particular for administration and maintenance, must be reserved for a restricted team and be limited to what is strictly necessary.SEC- HAB-2Remove obsolete access permissionsAccess permissions must be withdrawn as soon as authorizations are withdrawn, for example after the departure of an employee.SEC-HAB-3Perform an annual review of authorizationsA review of authorizations must be carried out regularly and at least annually.Secure exchanges with other bodiesSEC-ÉCH-1Secure the collection of information via an electronic platformIf the collection of personal data is done in electronic format using a dedicated platform, the person in charge of processing provides for the data to be sent in encrypted form: either by directly encrypting the data; or by using an encrypted communication channel (via protocols such as HTTPS, SFTP). In all cases, the encryption algorithms used must meet the SEC-CRY-1 requirements. The confidentiality of secrets (encryption key, password, etc.) must be ensured by transmitting them via a separate communication channel (for example, deposit of the encrypted file on the platform and communication of the password by telephone or SMS). SEC-ÉCH-2 Securing email transmissions With regard to data transmissions by email, these must be secured, for example by encrypting personal data using an asymmetric encryption algorithm with a private key held solely by the recipient of the data .The confidentiality of the secrets (encryption key, password, etc.) must be ensured by transmitting them via a separate channel (for example, sending the encrypted file by email and communicating the password by telephone or SMS). When transmitting by e-mail, the sender must ensure that it is the correct recipient, in order to prevent personal data from being accidentally disclosed to an unauthorized third party.SEC-ÉCH-3Secure the sending by fax If the paper format is used and transmissions are made by fax, the following security measures must be implemented: the fax must be located in a physically controlled room and accessible only to authorized personnel; the printing of messages must be subject to the introduction of a personal access code; when messages are sent, the fax machine must display the identity of the recipient fax machine in order to be sure of the recipient's identity; fax addresses must pre-register, as far as possible, the potential recipients in order to avoid any recipient error. , including those listed in the requirements SEC-EXH-1, SEC-EXH-2 and SEC-EXH-3, in order to transmit the summary reports to the competent authorities. The use of a secure electronic document exchange platform is preferred.SEC-ÉCH-5Secure the

collection of quality of life data from patientsConcerning questionnaires allowing the collection of quality of life data directly from patients patients, the data controller provides a procedure to guarantee the intervention of a health professional according to the following cases, listed in order of preference: The questionnaire is completed online by the patient and the platform only allows a deposit or online data entry: The platform provides for simple identification of the patient, namely by means of a meaningless and random pseudonym generated by the laboratory for this purpose and transmitted by the healthcare professional to the patient. It is not necessary to create an account or a personal patient space. The questionnaire is completed online by the patient and the platform also allows the data entered to be consulted later: the healthcare professional sends the patient the connection details communicated by the laboratory. The collection is done through the intermediary of the healthcare professional via a paper questionnaire: The professional gives the paper questionnaire to the patient; the latter completes it and gives it to the healthcare professional who is responsible for concealing the directly identifying data and transmitting the answers to the data controller. The questionnaire is completed online by the healthcare professional: The healthcare professional connects on an electronic platform put online by the data controller (or its subcontractor) in order to enter the answers to the questionnaire, during or after the consultation with the patient. This platform must meet the requirements of this standard. If the collection of quality of life data is carried out by post, the completed questionnaire must be returned by the patient by post, using a "T envelope", to the person in charge of processing at a dedicated address.Use SEC-CRY-1 cryptographic functionsUse recognized algorithms, software and librariesPersonal data must be encrypted at rest using algorithms and key sizes compliant with appendix B1 of the general security reference system ("RGS"). An operational key management procedure must be formalized. The backups of this data must also be encrypted in accordance with Annex B1 of the RGS. All data transmissions are carried out via encrypted communication channels and ensuring source and recipient authentication (HTTPS type, with the most up-to-date version of TLS possible). SEC-CRY-2Keep secrets and cryptographic keys securelyThese secrets must be protected, at least by the implementation of restrictive access rights and a secure password.Trace accessSEC-JOU-1Provide a system logging (logs)User actions must be the subject of logging measures, in particular, at a minimum, user accesses, the timestamp of their accesses as well as the details of the actions carried out (such as read or write operations). writing) as well as the reference of the record concerned.Logging traces must be kept for a period of between six months and one year.SEC-JOU-2Inform users of the implementation of the logging systemUsers participating in processing covered by this standard must be informed of the implementation of the logging

system, the nature of the data collected and the retention period of these traces.SEC-JOU-3Protect logging equipment and logged informationThe architecture of logging must be centralized and the logs must be subject to special protection measures. Access to the logs is restricted to only people who have obtained specific authorization based on strict necessity.SEC-JOU-4Checking the tracesAn automatic or semi-automatic check of the traces must be carried out regularly and at least every two months, in order to detect any anomalies.Manage incidents and data breachesSEC-VIO-1Predict procedures for security incidentsA security incident management policy is implemented in order to immediately respond to any possible security incident and identify if the incident leads to a breach of the personal data processed by the data controller. The policy provides in particular for a procedure aimed at implementing remedial actions in order to reduce the seriousness of the harm for a person affected by the data breach and to correct the vulnerabilities caused by security incidents.SEC-VIO-2Provide procedures for personal data breach notificationsThe data controller provides a procedure to determine the seriousness of a data breach (i.e. i.e. any breach, even temporary, of the confidentiality, availability or integrity of the data) for the persons concerned. If necessary, if there is a risk for the persons concerned, the data controller must proceed the notification of the breach to the authority in charge of the protection of personal data competent in the territory in which the data controller has his main establishment and, in the event that the data controller is not established on the territory of the European Union, to the CNIL under the conditions provided for in Article 33 of the GDPR. If this risk is deemed to be high, the data controller must communicate the violation to the persons concerned under the conditions provided for in Article 34 of the GDPR. The data controller must internally document any data breach regardless of its level of severity. Backup and plan for business continuitySEC-SAU-1 Perform frequent data backups Whether the data is in paper or electronic form , full backups should be scheduled at regular intervals. The process of restoring data from backups should also be tested regularly.SEC-SAU-2Store backup media in a safe placeBackup media (external hard drive, USB key, etc.) should be kept in a safe place different from the place where the data is stored. The media to be favored are those with sufficient longevity.SEC-SAU-3Provide security means for the transport of backupsWhen backups are transmitted by the network, it is advisable to encrypt the backup transmission channel when they are transmitted via a public network.SEC-SAU-4Regularly plan and test business continuityThe data controller provides an IT business recovery and continuity plan, even a summary one. He must ensure that users and subcontractors know who to contact in the event of an incident. This continuity or disaster recovery plan as well as the restoration of backups must be regularly tested. Archive in a secure mannerSEC-ARC-

1Implement specific access procedures for archived data The data controller defines an archiving and archive management process, which includes specific access procedures for archived data, given that the use of archived data must take place on an ad hoc and exceptional basis.SEC-ARC-2Destroy obsolete archives in a secure mannerThe data controller implements an operating procedure guaranteeing that the entire archive has been destroyed.13.4. More generally, the data controller or its subcontractor, if the data controller uses IT service providers in the context of the processing covered by this standard, must implement and document the following measures:CategoriesMeasuresSecuring workstations of work Provide an automatic session locking procedure Use regularly updated antivirus software Install a software "firewall" Collect the user's agreement before any remote maintenance intervention on his workstation Secure mobile computing Provide resources encryption of mobile equipment storage media Make regular data backups or synchronizations Require secrecy for unlocking smartphones Protect the internal computer network Limit network flows to what is strictly necessary Secure remote access for mobile computer devices by VPN Implement the WPA2 or WPA2 protocol -PSK for Wi-Fi networksSecure serversLimit access to administrative tools and interfaces to authorized personsDefine and implement a policy for updating software tools and install critical updates without delaySecure websitesUse the TLS protocol and check its implementation Check that no password or identifier is transmitted via URLs Check that user entries correspond to what is expected Put a consent banner for tracers (cookies) not necessary for the service Supervise the maintenance and destruction of dataRecord maintenance interventions in a daybookSupervise maintenance interventions carried out by third parties by a person in charge of the organizationErase the data of any equipment before its disposalProtect the premisesRestrict access to the premises by means of locked doors whatsoever to paper files or computer equipment, in particular serversInstall anti-intrusion alarms and check them periodicallySupervise IT developmentsPropose settings that respect the privacy of end usersAvoid comment areas or strictly supervise themPerform tests and acceptance tests on fictitious or anonymized data13 .5. These measures are not exhaustive and must be supplemented by any measures deemed necessary during the performance of the data protection impact assessment carried out, as detailed in article 14 of these standards.13.6 . The data controller may usefully refer to the Personal Data Security Guide (5) published by the CNIL.13.7. Articles 5.1.f and 32 of the GDPR require the updating of security measures with regard to the regular reassessment of the risks, so that they comply with the state of the art.14. Data protection impact assessment14.1. In accordance with Article 35 of the GDPR, the data controller must carry out and document a data protection impact assessment (DPIA).14.2. To carry out and document its impact analysis, the data controller

may refer to: the principles contained in this reference system; the methodological tools offered by the CNIL on its website.14.3. If necessary, the data controller may draw up a procedure relating to the DPIA allowing the involvement of the relevant actors and persons for its implementation, in particular the data protection officer (DPD/DPO), who must be consulted. 14.4. The DPIA will have to be reviewed and updated regularly, in particular if significant changes are planned in the processing or if the risks for the data subjects have evolved (such as the pursuit of an additional purpose, the use of a new processor , new data collected, data leak allowing re-identification, etc.).14.5. In accordance with Article 36 of the GDPR, the data controller must consult the CNIL prior to the implementation of the processing if, following the impact analysis, he is unable to identify and set up sufficient measures to reduce the risks to an acceptable level (residual risk remaining too high).(1) See deliberation no. for health vigilance management purposes.(2) Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR.(3) Recommendations 01/2020 on the measures that complement the transfer instruments intended to ensure compliance with the EU level of personal data protection.(4) Recourse to the derogations referred to in Article 49 must be limited to specific situations. Guidelines 2/2018 of the European Data Protection Board on derogations from Article 49 under Regulation 2016/679, adopted on May 25, 2018.(5) https://www.cnil.fr/sites /default/files/atoms/files/cnil_guide_securite_personnelle.pdf.The PresidentM.-L. Denis