Deliberation 2022-067 of June 2, 2022 National Commission for Computing and Liberties Legal status: In force Date of publication on Légifrance: Wednesday July 20, 2022 of personal data intended for the management of pharmaciesThe National Commission for Data Processing and Liberties, Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 relating to the protection of natural persons at with regard to the processing of personal data and the free movement of such data (General Data Protection Regulation), in particular Article 58 thereof; Considering the law n° 78-17 of January 6, 1978 modified relating to data processing, files and freedoms, in particular its article 8-I-2°-b; ;After having heard the report of Mrs Valérie PEUGEOT, Commissioner, and the observations of Mr Damien MILIC, Deputy Government Commissioner, Adopts a reference system relating to the processing of personal data intended for the management of pharmacies. The President Marie- Laure DENISANNEXEREFERENTIAL RELATING TO THE PROCESSING OF PERSONAL DATA INTENDED FOR THE MANAGEMENT OF PHARMACY PHARMACIES>>> You can consult the full text with its images from the authenticated electronic Official Journal extract1. Who is this reference for? This repository, taken pursuant to the provisions of Article 8-I-2-b of Law No. 78-17 of January 6, 1978 relating to data processing, files and modified freedoms (hereinafter Data Protection Act liberties), aims to facilitate compliance with the processing of personal data implemented within pharmacies in the context of the health care and administrative management of their patients/customers. holders of self-employed pharmacies and their service providers (subcontractors). Are not affected by this standard, because of their specificities, the treatments implemented: within the framework of the supply of the pharmaceutical file (DP) provided for by article L. 1111-23 of the public health code (CSP); during the deployment of telecare in pharmacies; in the context of the online sale of medicines; in the context of the fight against the Covid-19 epidemic (SI-DEP); within pharmacies for interior (PUI).2. Scope of the standard Processing aimed at enabling health care and administrative management within pharmacies, whether implemented using internal tools or outsourced to a service provider, leads to the collection of data relating to to identified or identifiable individuals (patients, healthcare professionals, etc.). As such, they are subject to the provisions of the General Data Protection Regulation (GDPR), the Data Protection Act and the provisions of the CSP. The person responsible for processing implemented in the context of pharmacies is either the pharmacist who owns the pharmacy when he exercises his activity as an individual entrepreneur, or the legal entity through which he exercises his activity. On the other hand, a pharmacy intern or a salaried pharmacist cannot be considered as being responsible for a processing implemented within the framework of the management of the pharmacy. The processing manager must implement

all the technical measures and organizational measures in order to guarantee a high level of protection of personal data from the design of processing and throughout its life. He must also be able to demonstrate this compliance at any time. Processing carried out in pharmacies must be entered in the register provided for in Article 30 of the GDPR. For more information: consult the register of processing activities on the cnil.fr website This reference document is not binding. Compliance with the recommendations it contains makes it possible in principle to ensure the compliance of the data processing implemented within pharmacies with the principles relating to data protection and professional secrecy, in a context of changing practices. in the digital age. Pharmacies wishing to deviate from the standard with regard to the particular conditions relating to their situation must be able to justify the existence of such a need, then take all appropriate measures to guarantee the compliance of the processing with the regulations on the protection of personal data. The reference document is not intended to interpret the rules of law other than those relating to the protection of personal data. It is up to the actors concerned to ensure that they comply with the other regulations that may apply. if this is required. For more information: consult the page Impact analysis relating to data protection: publication of a list of processing operations for which an analysis is requiredThe CNIL regularly publishes practical guides to support professionals in the implementation the obligations provided for by the regulations on the protection of personal data, which the latter are invited to consult in addition to this reference document. For more information: consult in particular the page Compliance tools3. Objectives pursued by the processing (PURPOSES) The processing implemented must meet a specific objective and be justified with regard to the missions and activities carried out within the pharmacy. They allow in particular: the dispensing of drugs and other products, articles, objects and devices provided for by the decree of February 15, 2002 as amended; cooperation between health professionals in application of 2o of article L. 5125-1-1 A of the CSP; contribution to health monitoring and protection actions organized by the authorities; participation in therapeutic education and support actions for patients/customers defined in Articles L. 1161-1 to L. 1161-5 of the CSP; the exercise of the role of corresponding pharmacist, in application of 7° of article L. 5125-1-1 A of the CSP; the proposal of advice and services intended to promote the improvement or maintenance of the state personal health pursuant to 8° of article L. 5125-1-1 A of the CSP; the vaccines that pharmacists are authorized to administer pursuant to 9° of article L. 5125-1-1 A of the CSP; the management of appointments. The processing operations allow, in particular, for the needs of the dispensation administration of medicines: keeping the prescription book and dispensing registers; managing and keeping the files necessary for monitoring the patient/client (excluding the Pharmaceutical File (DP)); communication and coordination between

professionals identified participating in the care of the person concerned; the establishment and electronic transmission of documents intended for the payment of health costs by the health insurance (prescriptions, etc.); the keeping of the accounts. The data personal data must be processed with respect for the privacy of individuals and with respect for the secrecy of information concerning them, in accordance with article L. 1110-4 of the CSP. They can be reused for research, studies or evaluations carried out by the staff monitoring the patient/client and intended for their exclusive use (internal research), without requiring authorization from the CNIL. Failing this, this reuse must be subject to subject to formalities pursuant to Articles 66 and 72 et seq. of the Data Protection Act relating to processing for the purposes of research, study or evaluation in the field of health. For more details on research in the field of health: Medical research sheet: what is the legal framework? 4. Legal basis(s) of the processing Each purpose of the processing must be based on one of the legal bases set by the regulations. It is up to the data controller to determine these legal bases before any processing operation, after having carried out a reflection, which he will be able to document, with regard to his specific situation and the context. Having consequences on the exercise of certain rights, these legal bases are part of the information that must be brought to the attention of the persons concerned. choice of legal basis in the table below.PurposesPossible legal bases (1)Dispensing of medicines, products or objectsContract or, where applicable, legal obligationCooperation between healthcare professionalsLegitimate interestsContribution to health monitoring and protection actions organized by the authoritiesMission of public interestProcessing implemented in the context of participation in therapeutic education and support actions for patients/clients defined in Articles L. 1161-1 to L. 1161-5 of the CSPLegitimate interestsExercise of the role of corresponding pharmacistLegitimate interestsProposal of advice and services intended to promote the improvement on or maintaining people's state of health, in accordance with article R. 5125-33-6 of the CSPLegitimate interestsVaccinationLegal obligation (2)Managing appointmentsLegitimate interestsKeeping the prescription book and dispensing registersObligation legalThe establishment and electronic transmission of documents intended for compulsory health insuranceLegal obligationFor more information: consult the page Lawfulness of processing: the essentials on the legal bases provided for by the GDPR5. Personal data concernedIn order to minimize the personal data processed, the data controller must ensure that he only collects and uses the relevant and necessary data with regard to his own needs for processing, health care and administrative management of the pharmacy. of pharmacy. The following data are in principle considered relevant for the purposes mentioned above: the identity and contact details of the patient/client (such as surname, first name, date of birth, postal address, e-mail address and telephone number); the identity and contact details of the health

professionals involved in the patient's care; the national health identifier (INS) for the health care of a patient/customer in the context of the delivery of reimbursed products; the social security number (NIR) for billing purposes and financial support of health expenses in the context of the delivery of reimbursed products; health data (such as weight, height, history medical conditions, medical diagnoses, treatments prescribed, treatments delivered, products sold, information likely to influence the reaction of the patient/client to his medical care and any element of a e to characterize the health of the patient/customer when providing advice, medication, products or medical devices); information relating to lifestyle habits depending on the context, when it is collected with the patient's consent and 'they are necessary for the health care of the patient; functional traces (those which report on the business actions of users or machines within the information system) and technical traces (those which report on the activity of the components software and hardware used by the information system to ensure the functionality requested by a user or a machine). For more details on the management of functional traces: AIPD Guide Knowledge bases After ensuring the necessity and relevance of the personal data that he uses, the data controller must also check, throughout the duration of the processing, the quality of the data processed. In practice, this means that the data must be accurate and updated in accordance with the regulations.6. Recipients of the dataPersonal data should only be made accessible to persons authorized to know it with regard to their attributions. In general, access authorizations should be documented by the organizations, and access to the various treatments must be subject to traceability measures. their missions and by virtue of legislative provisions the following persons:6.1. Persons accessing data on behalf of and under the authority of the data controller Only persons authorized by virtue of their missions or functions may access the personal data processed, in compliance with the provisions on professional secrecy and in the strict limit of their respective attributions and the accomplishment of these missions and functions. This may be, for example, pharmacy staff involved in the dispensing of medicines and other products, articles, objects and devices or in the delivery of advice.6.2 Recipients of dataThe GDPR defines recipients as any organization that receives data reporting. Before any communication of information, the data controller must, on the one hand, question the purpose of the transmission to ensure its relevance and legitimacy and, on the other hand, check that the data communicated is adequate, relevant and not excessive with regard to the purpose pursued. The recipients of the data may in particular be (non-exhaustive list): health professionals and professionals contributing to prevention and care, in order to ensure the continuity of care in the compliance with the provisions of Articles L. 1110-4 and L. 1110-12 of the CSP; in order to allow the reimbursement of acts, services and their control, the personnel of the compulsory

health insurance bodies, who are aware, within the framework of their functions and for the duration necessary for the accomplishment of these, the identity of their insured persons and beneficiaries, their social security number and the code numbers of the acts performed and pr stations served under the conditions defined in Article L. 161-29 of the Social Security Code (CSS); organizations conducting studies, research and assessments in the field of health, which may be recipients of personal health data under the conditions defined by the GDPR and the Data Protection Act (in particular in compliance with the principle of data minimization).6.3 SubcontractorsThe GDPR defines the subcontractor as the natural or legal person, the public authority, the service or other body which processes personal data on behalf of the data controller. This may be, for example, IT service providers (e.g. maintenance of software and workstations used in the pharmacy) or any organization offering a service or provision involving the processing of personal data on behalf of another organization (eg. : the technical concentrator organization (OCT) responsible for transmitting the data to the health insurance). The data controller who wishes to use a service provider to process personal data on his behalf (maintenance company, online platform, approved or certified health data host) must ensure that he only uses organizations presenting sufficient guarantees. A contract defining the characteristics of the processing, as well as the different obligations of the parties in terms of data protection must be established between them (article 28 of the GDPR). This contract must mention that the service provider, as a subcontractor: only processes personal data on the instructions of the data controller; ensures that staff sign confidentiality agreements; takes all the security measures required with regard to the security objectives set for it by the data controller; does not recruit a subcontractor without the prior written authorization of the data controller; cooperates with the data controller to comply with its obligations, in particular when patients/customers have requests concerning their data; deletes or returns to the data controller all personal data at the end of the services; provides the data controller with all the information necessary to demonstrate compliance with the obligations to enable audits to be carried out. The service provider must, in its capacity as subcontractor, keep a register of processing activities under the conditions of Article 30.2 of the GDPR. The service provider must, in the event of incident related to the data it manages on behalf of the data controller (security breach, hacking, loss, etc.) inform it within the s as soon as possible, so that the latter can comply with its own obligations to manage and notify the incident. The contract signed between the data controller and its subcontractor should provide for the procedures for notifying the subcontractor to the data controller. For more details on subcontracting: > Section Working with a subcontractor > Guide to support for subcontractors Example: maintenance of the software and workstations used in the pharmacy Dispensary -ci

accesses personal data in compliance with professional secrecy. Data security must be guaranteed and confidentiality preserved. As such, physical and logical measures must be implemented, such as encryption, in order to allow the technician to carry out his missions without being able to read this data. Storage periods7.1. Retention of personal data A precise retention period for the data must be set according to each purpose: this data cannot be retained for an indefinite period. The retention period for the data or the criteria used to determine this duration form part of the information that must be communicated to the persons concerned. Under these conditions, it is the responsibility of the data controller to determine this period before the processing is carried out. In the context of the delivery of specific products, certain regulatory retention periods must be applied. Thus, in accordance with article R. 5132-35 of the CSP, copies of prescriptions for drugs classified as narcotics or subject to narcotics regulations must be kept for a period of three years. Moreover, in accordance with articles R. 5125-45, R. 5132-10 and R. 5132-59 of the CSP, data from the registers of magistral or officinal preparations, medicines falling within lists I, II and narcotics and registrations of substances or preparations intended for a non-therapeutic use of products classified as very toxic, toxic, carcinogenic, teratogenic or mutagenic must be kept for a period of ten years. Finally, the registers or records relating to medicinal products derived from blood must be kept for a period of forty years, in accordance with article R. 5121-195 of the CSP.Duplicate electronic care sheets must be kept for at least three months, in accordance with article R. 161-47 of the CSS.For donations data whose retention period is not fixed by the texts, it is up to the data controller to determine and justify the appropriate period (see section For more information below). At the end of these periods, the data is deleted or archived in an anonymized form. It is up to service providers providing software solutions to integrate automatic archiving functionalities on the expiry date. Failing this, the data controller should do so manually. Similarly, the traces (technical and functional) of the software solutions should be kept for a minimum of six months; this period may be extended if necessary to deal with certain risks weighing on individuals. The storage and archiving of data must be carried out under security conditions in accordance with the provisions of Article 32 of the GDPR. To find out more In addition, you can refer to the CNIL guides: > Security: Secure archiving > Limiting the retention of data > Practical guide to retention periods > Guidelines for health retention periods (excluding research)7.2. Retention of anonymized data The regulations relating to the protection of personal data do not apply, in particular with regard to retention periods, to anonymized data. These are data which can no longer, by the use of means reasonably available to individuals, be linked to the identified natural person to whom they initially related (e.g. statistics). Anonymization must be distinguished from pseudonymization, for which it is

technically possible to trace the identity of the data subject using third-party data. Indeed, the pseudonymization operation is reversible, unlike anonymization. Thus, the data controller can keep the anonymized data for an indefinite period. In this case, the data controller must guarantee the anonymized nature of the data in a sustainable way. For more information: see the G29 Guidelines on anonymization8. Informing people The processing of personal data must be implemented in complete transparency vis-à-vis the people concerned. Thus, from the stage of the collection of personal data, people must be informed of the methods of processing their data in the conditions provided for in Articles 12, 13 and 14 of the GDPR. Data subjects must also be informed of how to exercise their rights. Persons whose data are recorded and stored in the processing of personal data of the controller treatment are informed by posting in the pharmacy or by the delivery of a specific document, in particular in the context of home visits (such as a leaflet given to the patient/customer or made available to him at the counter) .9. Rights of persons The persons concerned have the following rights, which they exercise under the conditions provided for by the GDPR (see the section dedicated to rights): right to oppose the processing of their data, subject to the conditions for exercising this right pursuant to the provisions of Article 21 of the GDPR: for example, the right of opposition will not apply to mandatory dispensing registers or to the transmission of their prescription for the delivery of prescription drugs; right of access to all data concerning them in general; right to rectify data concerning them, if they are inaccurate; right to erase data concerning them subject to the conditions for exercising this right pursuant to the provisions of Article 17 of the GDPR; right to restriction of processing. For example, when the person disputes the accuracy of their data, they can ask the healthcare professional to temporarily freeze the processing of their data, while the latter carries out the necessary checks concerning their request. It should be noted that the choice of a legal basis for the processing conditions the existence of certain rights (3). Thus, keeping a dispensation register meets a legal obligation. The patient/customer cannot therefore object in principle to the processing of his personal data, in accordance with the provisions of Article 21 of the GDPR.10. Security The data controller must take all necessary precautions with regard to the risks presented by its processing to preserve the security of personal data and, in particular at the time of their collection, during their transmission and their storage, to prevent them from being distorted, damaged or that unauthorized third parties have access to it.10.1. The security obligations imposed by the GDPR In order to meet his obligations in terms of security, the data controller may usefully refer to the Guide to the security of personal data. In particular, in the specific context of this reference system, the pharmacist is invited to adopt the following measures, to justify their equivalence or the fact that their implementation is not necessary:CategoriesMeasures Raise awareness among

usersInform and raise awareness among pharmacy staff accessing the dataFor a pharmacy pooling IT resources, draft an IT charter and give it binding force Authenticate users Define an identifier (login) specific to each user Adopt a user password policy in accordance with CNIL recommendations (4) For users accessing health data, use strong authentication based on: cards CPx, in particular: a professional card (CPS), which must remain strictly personal, without communication of the secret code to the other members of the staff of the pharmacy; a professional in training card (CPF for pharmacy students) or any alternative two-factor means (for example, a password supplemented by the sending of a unique code at each connection). Manage authorisations, track access and manage incidents Assign an authorization profile adapted to each user (distinguishing in particular between administrative data and medical data) Delete obsolete access permissions Set up a system for logging access to health data Inform users of the implementation of the logging systemProvide procedures for personal data breach notificationsSecure workstations and mobile computingProvide an automatic locking procedure for the computer session, with a trigger after one five-minute inactivity timeout for workstations located in areas open to the publicProtect workstations that can easily be taken away, such as laptops, with a physical security cableEncrypt storage media for computer equipment used in places accessible to the publicAllows re the regular updating of antivirusesCollect the user's agreement before any intervention on an individual workstationLimit the storage of health data on tablets and smartphones (because of the consequences for patients/customers in the event of theft or loss of material). If this equipment is used, its level of data security must be equivalent to that of the other equipment (encryption, access codes, etc.) Require secrecy for unlocking smartphones or tablets Protect screens from prying eyes (orientation, optical filter) Provide a confidentiality zone around dispensing stations, with markings and information encouraging compliance Limit the use of storage media removable media (USB keys, external hard drives) and systematically encrypt the sensitive data stored there Do not lend or use smartphones and tablets for professional use for personal use Protect the internal computer network Prohibit connections of non-professional devices on the network In the event of provision of public Wi-Fi access to pharmacy customers, this must not allow access to the pharmacy's internal network (partitioning) Securing the servers Limiting access to administration tools and interfaces to only people empoweredAllow critical updates to be installed without delayBackup and plan for continuity of activityPerform or allow the execution of regular backupsStore backup media in a safe placeArchive in a secure mannerImplement specific access procedures for archived dataDestroy obsolete archives in a secure mannerSupervise the maintenance and destruction of dataRecord the interventions of maintenance in a daybookSupervise interventions by third

parties by a pharmacy managerErase the data of any equipment before its disposalManage subcontractingProvide specific clauses (5) in subcontractor contractsProvide conditions for return and destruction of data Ensure the effectiveness of the guarantees provided (security audits, visits, etc.) Secure exchanges with other healthcare professionals and with patients/customers Authenticate recipients before sending any healthcare data Use messaging secure health electronics for exchanges between healthcare professionals For exchanges with other professionals involved in the care of the patient/client or with the patients/clients themselves:encrypt the documents before sending them via standard electronic messaging (6) and transmit the secret by a separate transmission and via a different channel; use a transfer protocol guaranteeing the confidentiality of the messages and the authentication of the mail server; choose a mail service hosting the data in a country or with a service provider guaranteeing the data protection in accordance with European rules.Protect the premisesRestrict access to the premises by means of locked doorsInstall anti-intrusion alarms and check them periodicallySecure the storage of files in paper format (secure premises, lockable cabinet)Recover printed documents containing data immediately after they are printed or made, when possible, secure printingDestroy paper documents containing data that are no longer useful using an appropriate shredder (certified at least class 3 of the DIN 32757105 standard)Service providers responsible for developing, maintain the software and workstations managing patient/client files or offering an appointment platform are invited to implement the following measures, or be able to justify the implementation of equivalent measures or their lack of necessity or possibility, under the control of the data controller:CategoriesMeasures Raising awareness among usersInforming and raising awareness among their staff having access to health data or participating in the development or maintenance of IT tools handling health dataAuthenticate usersDefine an identifier (login) specific to each userIntegrate a password policy ut user complies with CNIL recommendations (7)Require the user to change their password after resettingLimit the number of attempts to access an accountFor users accessing health data, require strong authentication via their health professional card health (CPS) or establishment (CPE) or any alternative two-factor means (eg. sending a single-use code)Manage authorizationsIntegrate authorization profiles distinguishing in particular between administrative data and medical dataRemove obsolete access permissionsCarry out an annual review of authorizationsLimit the distribution of paper documents containing health data to people with need to have it as part of their activity Trace access and manage incidents Provide a logging system Inform users of the implementation of the logging system Protect logging equipment and logged information Provide procedures for data breach notifications to personal character Secure workstations Provide an automatic locking procedure for

the computer session, with a trigger after a period of inactivity of five minutes for workstations located in areas open to the public Protect workstations likely to be easily taken devices, especially laptops, using a physical security cable Implement regularly updated antivirus software Install a software firewall Encrypt stored data Collect user consent before any intervention on their computer Secure mobile computingFor remote access to patient/client files, comply with the interoperability and security standards provided for in article L. 1110-4-1 of the CSPProtect screens from prying eyesLimit the use of storage media removable media (USB keys, external hard drives) and systematically encrypt the sensitive data stored there Plan backup measures and regular synchronization of data Protect the internal computer network Limit network flows to what is strictly necessary (block protocols and ports that are not used)Limit connections of non-professional devices on the networkSecure remote access of devices mobile computers using a VPNImplement the WPA2 or WPA2-PSK protocol for Wi-Fi networksSecure serversLimit access to administrative tools and interfaces to authorized personsEncrypt stored dataInstall critical updates without delayEnsure data availabilitySecure websitesUse the TLS protocol in accordance with ANSSI recommendations and verify its implementationVerify that no passwords or resource identifiers containing personal data are embedded in URLsBackup and plan business continuityPlan regular stored backups in a separate site Plan the storage of backup media in a safe place sufficiently distant from the main system Provide security means for the transport of backups if necessary Plan and regularly test business continuity Archive in a secure manner Implement access procedures specific to archived dataDestroy obsolete archives in a secure mannerSupervise the maintenance and destruction of dataRecord maintenance interventions in a daybookPhysically erase the data from any equipment before it is scrappedManage subcontractingProvide for specific clauses (8) in the contract with the data controller Provide conditions for the restitution and destruction of data Allow the data controller to ensure the effectiveness of the guarantees provided (security audits, visits, etc.) Secure exchanges with other organizations Facilitate the exclusive use of secure electronic health messaging for exchanges between healthcare professionals a standard electronic mail and foresee the trans mission of the secret code by sending it separately and via a different channel; using a transfer protocol guaranteeing the confidentiality of messages and the authentication of the messaging server; allowing and facilitating the use of messaging hosting the data in a country or with a service provider guaranteeing data protection in accordance with European rules Supervise IT developments Offer privacy-friendly settings by default to end users Avoid free comment areas or strictly supervise them Test on fictitious or anonymized data (and not only pseudonymised)Use cryptographic functionsUse state-of-the-art algorithms, software and

libraries and comply with the recommendations of the general security repository of the National Information Systems Security Agency (ANSSI)Keep secrets and cryptographic keys securely10.2 . The security obligations imposed by the CSP In addition to the general obligations arising from the GDPR (article 32) and the Data Protection Act, the processing of health data in the context of health care is subject to specific security obligations. . Articles L. 1470-1 and following of the CSP provide that the data controller must ensure that the information systems, services or digital tools that he uses comply with the security (9) and interoperability (10) drawn up by the Digital Health Agency (ANS) (11). He must also respect the security instructions concerning him provided by the latter which correspond to the state of the art. In the event of outsourcing of the hosting of health data, the IT service providers must be approved or certified for the hosting, storage, retention of health data in accordance with the provisions of Article L. 1111-8 of the CSP (so-called "HDS" certification, hosting of health data). To find out more: > ANS list of certified hosts> ANS list of approved hosts Example of outsourcing data hosting: When the pharmacy management software (LGO) is accessible remotely and is hosted by a service provider (generally the software publisher, an online appointment booking platform) or if the storage of patient/customer health data is entrusted to a service provider responsible for ensuring its storage in remote servers (for example, a backup service provider), this service provider must be HDS.11.Additional measures: Impact analysis anddata protection officerThe CNIL considers that the completion of a DPIA and the appointment of a data protection officer (DPD/DPO) should in principle be necessary for pharmacies declaring an overall annual activity of more than 2,600,000 euros excluding tax. The assessment of the amount of the activity is carried out in application of article L. 5125-15 of the CSP and according to the methods of article R. 5125-37-1 of the same code. To carry out an impact study, the data controller may refer to: the principles contained in this reference system; the methodological tools offered by the CNIL on its website.(12) In accordance with Article 28 of the GDPR, the sub- processor must provide the data controller with all the information necessary to carry out this analysis._____(1) Subject to different choices justified by a specific context.(2) Legal and regulatory obligations are assimilated.(3) https://www .cnil.fr/fr/la-liceite-du-traitement-lessentiel-sur-les-bases-legales-prevues-par-le-rgpd(4) https://www.cnil.fr/fr/authentication-par -password-elementary-security-measures(5) Precise description of the processing (data, location, operations, access, duration, restitution, etc.), security objectives adapted to the risks, incident management and notification data breaches.(6) Instant messaging (ch at) must be used with the utmost care and in a secure manner.(7)

https://www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires (8) Precise description of the processing (data, location, operations, access, duration, restitution, etc.), security objectives adapted to the risks, incident management and notification of data breaches.(9) https://esante.gouv. fr/securite(10) https://esante.gouv.fr/interoperabilite(11) See the PGSSI-S standards: https://esante.gouv.fr/securite/pgssi-s/espace-de-publication(12) https://www.cnil.fr/fr/RGPD-analyse-impact-protection-des-donnees-aipd