ADMINISTRATIVE DIRECTIVE WHAT ESTABLISHES THE TREATMENT OF THE PERSONAL INFORMATION RELATED WITH HEALTH OR DATA PERSONAL IN HEALTH

- **(Administrative Directive No. 294-MINSA/2020/OGTI, approved by RM N° 688-2020/MINSA)**

October, 2020

ADMINISTRATIVE DIRECTIVE ESTABLISHING THE PROCESSING OF RELATED PERSONAL DATA WITH HEALTH OR PERSONAL HEALTH DATA

(Administrative Directive No. 294-MINSA/2020/OGTI,
approved by RM N° 688-2020/MINSA)

General Information Technology Office

October 2020

Cataloging made by the Library of the Ministry of Health

Administrative directive that establishes the processing of personal data related to health or personal data in health / Ministry of Health. General Directorate of Information Technologies. Information Management Office - Lima: Ministry of Health; 2020. 40 p. illus.

HEALTH LEGISLATION / INFORMATION SYSTEMS / DATA REGISTRATION / PERSONAL INFORMATION / PANDEMICS / ANONYMIZATION OF INFORMATION / CONFIDENTIALITY

"Administrative Directive that establishes the Treatment of Personal Data related to Health or Personal Data in Health" (DA No. 294-MINSA/2020/OGTI approved by RM No. 688-2020/MINSA).

Ministry of Health. General Office of Information Technologies (MINSA/OGTI)

Team responsible for the preparation:
Lawyer Carmen Alicia Cedamanos Medina, OGTI
Dr. A.S. Paul Martin Vasquez Carbonell, OGEI/OGTI
Lic. Jorge Antonio Miranda Monsoon, OGEI/OGTI

Coordination and editing:
Lic. Alice Rivers Lumps, OGEI/OGTI

Design and layout:
Julie Guillen Ramos, THURSDAY/THUG

Revision:
Dr. A.S. Luis Robles Guerrero, Normative Coordination Unit/MINSA

Ministry of Health
Av. Salaverry N° 801, Lima 11, Lima-Peru
Tel.: (51-1) 315-6600
https://www.gob.pe/minsa/
Webmaster@minsa.gob.pe

Digital Version Available: http://
bvs.minsa.gob.pe/local/MINSA/5118.pdf

PERÚ Ministerio de Salud

PILAR MAZZETTI SOLER
Minister of Health

LUIS ANTONIO NICOLAS SUÁREZ OGNIO
Vice Minister of Public Health

VICTOR FREDDY BOCANGEL PUCLLA
Vice Minister of Health Benefits and Insurance

SILVIANA GABRIELA YANCOURT RUÍZ
General Secretariat

MIGUEL ANGEL GUTIÉRREZ REYES
General Director of the
General Information Technology Office

ALBERTICO QUISPE CRUZATTI
Executive Director of the
Information Management Office

Presentation

At the global level, the United Nations Organization proclaims the fundamental right to protection of personal data through the adoption, in 1948, of the Universal Declaration of Human Rights, which states in its Art. 12 that “No one shall be subject to arbitrary interference in his private life, his family, his home or his correspondence, nor of attacks on his honor or reputation.”

In Peru, the Political Constitution establishes that computer services, computerized or not, public or private, do not provide information that affects personal privacy; Law No. 29733 on the Protection of Personal Data guarantees the right to their protection with adequate treatment and; Emergency decree No. 007-2020 alludes to public entities and private organizations managing personal, biometric and spatial data as strategic assets.

In the field of health, Law No. 26842 – General Health Law, states that every user of health services has the right to the confidentiality of information related to the medical act and their clinical history; Likewise, Law No. 27806 - Law of Transparency and Access to Public Information, states that the right of access to public information cannot be exercised with respect to personal data whose publicity constitutes an invasion of personal and family privacy.

In accordance with the aforementioned laws, the Ministry of Health, as the governing body in health, has formulated, through the General Office of Information Technologies, the Administrative Directive that establishes the Treatment of Personal Data related to Health or Personal Data in Health, which aims to establish administrative criteria for the adequate treatment and protection of personal data related to health or personal health data.

Said regulatory document considers the following aspects: the classification of data in the Health Sector, personal data in or related to health (DPS), information in health or health matters (IS), generation and protection of the DPS, the treatment of the DPS and health information, the flow and assets of health information, the sending of personal health data to other entities, the rights of the owners of the DPS, the information security measures, the confidentiality criteria of the DPS, the treatment of the DPS in a state of health emergency or pandemic situations.

In this context, this Administrative Directive is made available that establishes the Treatment of Personal Data related to Health or Personal Data in Health, for observation and application by public and private entities in the Health Sector.

Miguel Angel Gutierrez Reyes
General Director of Information Technologies

Content

TABLE OF CONTENTS

MINISTERIAL RESOLUTION I.

PURPOSE..... 11

II. GOALS..... 11

III. SCOPE OF APPLICATION..... 11

IV. BASE LEGAL..... 12

V. GENERAL PROVISIONS..... 13

5.1 OPERATIONAL DEFINITIONS..... 13

5.2 ACRONYMS..... 17

5.3 OF THE CLASSIFICATION OF DATA IN THE HEALTH SECTOR 17

5.4 PERSONAL HEALTH DATA OR RELATED PERSONAL DATA WITH HEALTH – DPS..... 17

5.5 HEALTH INFORMATION OR HEALTH INFORMATION - IS..... 20

SAW. SPECIFIC PROVISIONS..... 21

6.1 OF THE GENERATION OF THE DPS..... 21

6.2 OF THE PROTECTION OF THE DPS 22

6.3 OF THE TREATMENT OF DPS AND HEALTH INFORMATION 22

6.4 THE FLOW OF HEALTH INFORMATION 23

6.5 OF INFORMATION ASSETS 24

6.6. OF THE SENDING OF PERSONAL HEALTH DATA TO OTHER ENTITIES OF THE PUBLIC OR PRIVATE ADMINISTRATION..... 24

6.7 THE RIGHTS OF THE DPS HOLDERS..... 25

6.8 INFORMATION SECURITY MEASURES 26

6.9 OF THE CONFIDENTIALITY CRITERIA OF THE DPS..... 27

6.10 OF THE TREATMENT OF DPS IN A STATE OF HEALTH EMERGENCY OR PANDEMIC SITUATIONS 27

VII. RESPONSIBILITIES..... 28

VIII.FINAL PROVISIONS..... 28

IX. ATTACHMENTS..... 28

ANNEX 01 – Data Classification Chart in the Health Sector..... 29

ANNEX 02 – Regulatory references that recognize and guarantee the right to the protection of personal health data..... 30

Annex 03 – Confidentiality commitment of personnel with an employment relationship..... 37

Annex 04 – Confidentiality commitment of personnel with a contractual relationship..... 38

Annex 05 – Characteristics of consent for the processing of personal data in accordance with the provisions of article 12 of the regulations of law No. 29733, personal data protection law..... 39

MINISTERIO DE SALUD

No. 688-2020/MINSA

REPUBLICA DEL PERU

Resolución Ministerial

Lima, 01 de SETIEMBRE del 2020

Visto, los Expedientes N° 19-152576-001 y 004, N° 20-069960-001 que contienen el Informe N° 013-2020-AL-OGTI/MINSA, de la Oficina General de Tecnologías de la Información, el Informe UCN-006-2020-SG/MINSA, de la Unidad de Coordinación Normativa de la Secretaría General; así como, el Informe N° 850-2020-OGAJ/MINSA, de la Oficina General de Asesoría Jurídica;

CONSIDERANDO:

Que, el numeral XIV del Título Preliminar de la Ley N° 26842, Ley General de Salud, dispone que la información en salud es de interés público. Toda persona está obligada a proporcionar a la Autoridad de Salud la información que le sea exigible de acuerdo a Ley. La que el Estado tiene en su poder es de dominio público, con las excepciones que establece la Ley;

Que, el artículo 25 de la Ley General de Salud, dispone que toda información relativa al acto médico que se realiza, tiene carácter reservado. El profesional de la salud, el técnico o el auxiliar que proporciona o divulga, por cualquier medio, información relacionada al acto médico en el que participa o del que tiene conocimiento, incurre en responsabilidad civil o penal, según el caso, sin perjuicio de las sanciones que correspondan en aplicación de los respectivos Códigos de Ética Profesional;

Que, el artículo 120 de la Ley en referencia señala que toda información en materia de salud que las entidades del Sector Público tengan en su poder es de dominio público. Queda exceptuada la información que pueda afectar la intimidad personal y familiar o la imagen propia;

Que, el artículo 2 de la Ley N° 29733, Ley de Protección de Datos Personales, define los Datos personales como toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados, y Datos sensibles, aquellos datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos; opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual;

Que, los numerales 13.5 y 13.6 del artículo 13 de la Ley de Protección de Datos Personales, señala que los datos personales solo pueden ser objeto de tratamiento con

Base Legal

consentimiento de su titular, salvo ley autoritativa al respecto. El consentimiento debe ser previo, informado, expreso e inequívoco. En el caso de datos sensibles, el consentimiento para efectos de su tratamiento, además, debe efectuarse por escrito. Aun cuando no mediara el consentimiento del titular, el tratamiento de datos sensibles puede efectuarse cuando la ley lo autorice, siempre que ello atienda a motivos importantes de interés público;

Que, el numeral 6 del artículo 14 de la Ley en referencia, dispone que no se requiere el consentimiento del titular de datos personales para los efectos de su tratamiento, cuando se trate de datos personales relativos a la salud y sea necesario, en circunstancia de riesgo, para la prevención, diagnóstico y tratamiento médico o quirúrgico del titular, siempre que dicho tratamiento sea realizado en establecimientos de salud o por profesionales en ciencias de la salud, observando el secreto profesional; o cuando medien razones de interés público previstas por ley o cuando deban tratarse por razones de salud pública, ambas razones deben ser calificadas como tales por el Ministerio de Salud; o para la realización de estudios epidemiológicos o análogos, en tanto se apliquen procedimientos de disociación adecuados;

Que, el numeral 1) del artículo 3 del Decreto Legislativo N° 1161, Ley de Organización y Funciones del Ministerio de Salud, dispone como ámbito de competencia del Ministerio de Salud, la salud de las personas;

Que, el artículo 4 de la del Decreto Legislativo precitado, contempla que el Sector Salud, está conformado por el Ministerio de Salud, como organismo rector, las entidades adscritas a él y aquellas instituciones públicas y privadas de nivel nacional, regional y local, y personas naturales que realizan actividades vinculadas a las competencias establecidas en la presente Ley, y que tienen impacto directo o indirecto en la salud, individual o colectiva;

Que, el artículo 4-A del mencionado Decreto Legislativo, modificado por la Única Disposición Complementaria Modificatoria del Decreto Legislativo N° 1504, Decreto Legislativo que fortalece al Instituto Nacional de Salud para la Prevención y Control de Enfermedades, establece a través de sus sub numerales que: La potestad rectora del Ministerio de Salud comprende la facultad que tiene para normar, supervisar, fiscalizar y, cuando corresponda, sancionar, en los ámbitos que comprenden la materia de salud. La rectoría en materia de salud dentro del sector la ejerce el Ministerio de Salud por cuenta propia o, por delegación expresa, a través de sus organismos públicos adscritos y, dentro del marco y los límites establecidos en la presente ley, la Ley Orgánica del Poder Ejecutivo, las normas sustantivas que regulan la actividad sectorial y, las normas que rigen el proceso de descentralización. Asimismo, que el Ministerio de Salud, ente rector del Sistema Nacional de Salud, y dentro del ámbito de sus competencias, determina la policía, regula y supervisa la prestación de los servicios de salud, a nivel nacional, en las siguientes instituciones: Essalud, Sanidad de la Policía Nacional del Perú, Sanidad de las Fuerzas Armadas, Instituciones de salud del gobierno nacional y de los gobiernos regionales y locales, y demás instituciones públicas, privadas y público-privadas;

Que, Los literales a), b) y e) del artículo 5 del Decreto Legislativo N° 1161, modificado por el Decreto Legislativo N° 1504, dispone entre otras que, son funciones rectoras del Ministerio de Salud: conducir, regular y supervisar el Sistema Nacional de Salud; formular, planear, dirigir, coordinar, ejecutar, supervisar y evaluar la política nacional y sectorial de promoción de la salud, prevención de enfermedades, recuperación, rehabilitación en salud y buenas prácticas en salud, bajo su competencia, aplicable a todos los niveles de gobierno; así como regular y dictar normas de organización para la oferta de salud, de los diferentes prestadores que brindan

MINISTERIO DE SALUD

No.688-2020/MINSA

REPUBLICA DEL PERU

Resolución Ministerial

Lima, 01 de SETIEMBRE del 2020

atenciones, para que en conjunto sean integrales, complementarias, de calidad, y que preste cobertura de manera equitativa y eficiente a las necesidades de atención de toda la población;

Que, el artículo 52 del Reglamento de Organización y Funciones del Ministerio de Salud, aprobado por Decreto Supremo N° 008-2017-SA, establece que la Oficina General de Tecnologías de la Información es el órgano de apoyo del Ministerio de Salud, dependiente de la Secretaria General, responsable de implementar el gobierno electrónico; planificar, implementar y gestionar los sistemas de información del Ministerio de Salud; administrar la información estadística y científica en salud del Sector Salud; realizar la innovación y el desarrollo tecnológico, así como del soporte de los equipos informáticos del Ministerio de Salud. Asimismo, es responsable de establecer soluciones tecnológicas, sus especificaciones, estándares; diseñar, desarrollar y mejorar las plataformas informáticas de información en el Sector Salud. De igual modo, establece requerimientos técnicos para la adquisición, aplicación, mantenimiento y uso de soluciones tecnológicas, en el ámbito de competencia del Ministerio de Salud;

Que, los literales a) y d) del artículo 53 del precitado Reglamento, establecen como funciones de la Oficina General de Tecnologías de la Información: proponer y supervisar la implementación de políticas, normas, lineamientos, planes, estrategias, programas y proyectos en materia de desarrollo de tecnologías de la información; estadística y gestión de la información; gobierno electrónico y su operatividad; así como políticas de seguridad de tecnologías de la información y comunicación del Ministerio de Salud, para asegurar la integridad, confidencialidad y la disponibilidad de la misma en el marco de la normativa vigente; y, conducir, promover y coordinar el proceso de integración y articulación de la infraestructura tecnológica del Ministerio de Salud y del Sector Salud para velar por la interoperabilidad de los sistemas de información;

Que, mediante el documento del visto, y en el marco de sus competencias funcionales, la Oficina General de Tecnologías de la Información ha elaborado la Directiva Administrativa que establece el tratamiento de los datos personales relacionados con la salud o datos personales en salud, con el objetivo de establecer los criterios administrativos para el adecuado tratamiento de los datos personales relacionados con la salud o datos personales en salud;

V. BOCANGEL
L. SUAREZ
S. YANCOBRO
G. REVILLA S.
M. GUTIERREZ
L. CUEVA
N. HUAMANÍ

Base Legal

Base Legal

L. SUAREZ

V. BOCANGEL

Estando a lo propuesto por la Oficina General de Tecnologías de la Información;

G. REVILLA S.

Con el visado del Director General de la Oficina General de Tecnologías de la Información, del Director General de la Dirección General de Aseguramiento e Intercambio Prestacional, de la Directora General de la Dirección General de Intervenciones Estratégicas en Salud Pública, de la Directora General de la Oficina General de Asesoría Jurídica, de la Secretaria General, del Viceministro de Salud Pública y del Viceministro de Prestaciones y Aseguramiento en Salud; y,

M. GUTIERREZ

De conformidad con lo dispuesto en la Ley N° 26842, Ley General de Salud, el Decreto Legislativo N° 1161, Ley de Organización y Funciones del Ministerio de Salud, modificado por la Ley N° 30895, Ley que fortalece la función rectora del Ministerio de Salud y el Decreto Legislativo N° 1504, Decreto Legislativo fortalece al Instituto Nacional de Salud para la prevención y control de las enfermedades; así como, el Reglamento de Organización y Funciones del Ministerio de Salud, aprobado por Decreto Supremo N° 008-2017-SA, modificado por Decreto Supremo N° 011-2017-SA y Decreto Supremo N° 032-2017-SA;

L. CUEVA

SE RESUELVE:

Artículo 1.- Aprobar la Directiva Administrativa N° 294 -MINSA/2020/OGTI, Directiva Administrativa que establece el tratamiento de los datos personales relacionados con la salud o datos personales en salud, que en documento adjunto forma parte integrante de la presente Resolución Ministerial.

N. HUAMANÍ

Artículo 2.- Encargar a la Oficina General de Tecnologías de la Información, en el marco de sus funciones, la difusión, monitoreo y supervisión de acciones para el cumplimiento de la presente Directiva Administrativa.

S. YANCOURT

Artículo 3.- Encargar a la Oficina de Transparencia y Anticorrupción de la Secretaría General la publicación de la presente Resolución Ministerial y el documento adjunto que forma parte del mismo, en el portal institucional del Ministerio de Salud.

Regístrese, comuníquese y publíquese.

PILAR ELENA MAZZETTI SOLER
Ministra de Salud

ADMINISTRATIVE DIRECTIVE Nº 294-MINSA/2020/OGTI

ADMINISTRATIVE DIRECTIVE THAT ESTABLISHES THE TREATMENT OF PERSONAL DATA RELATED TO HEALTH OR PERSONAL DATA IN HEALTH

I. PURPOSE

Contribute with full respect for the person and the Fundamental Right to protect their personal data1 related to health, as well as the Fundamental Right to personal and family privacy, and the secrecy or inviolability of private documents, recognized by the regulations. national, so that they are safeguarded in the health sector.

II. GOALS

2.1 GENERAL OBJECTIVE:

Establish the administrative criteria for the appropriate treatment of personal data related to health or personal health data.

2.2 SPECIFIC OBJECTIVES

2.2.1 Establish the criteria for the adequate treatment and protection of personal data related to health or personal health data, in accordance with Law No. 26842, General Health Law, Law No. 29733, Personal Data Protection Law and Law No. 27806, Law on Transparency and Access to Public Information.

2.2.2 Classify health-related personal data and information into health, derived from health care.

III. SCOPE OF APPLICATION

This Administrative Directive is mandatory in all bodies and organic units of the Ministry of Health, its deconcentrated bodies, assigned public bodies, and national programs; in the Regional Health Directorates, Regional Health Managements or those that take their place in the regions and their networks, micro networks and health establishments.

Likewise, this Administrative Directive is applicable to the Social Security of Health - EsSalud, the Health Directorate of the National Police of Peru, Health Directorate of the Peruvian Army, Health Directorate of the Peruvian Navy, Health Directorate of the Peruvian Air Force and its corresponding health establishments, and others

[1] Law No. 29733, Personal Data Protection Law

public and private entities that develop activities in the National System of Health.

IV. BASE LEGAL

- Political Constitution of Peru, article 2 paragraphs 6, 7 and 10.
- Law No. 26842, General Health Law, and its amendments. Preliminary title numeral XIV, Article 5, 15.2, 25, 29, 78, 117, 120, 128.
- Law No. 29414, Law that establishes the Rights of Users of Health Services.
- Law No. 29733, Personal Data Protection Law and its amendments.
- Legislative Decree No. 604, Law of Organization and Functions of the National Institute of Statistics and Informatics, Article 7.
- Legislative Decree No. 1246, Legislative Decree approving various administrative simplification measures, Article 2.
- Legislative Decree No. 1353, Legislative Decree that Creates the National Authority for Transparency and Access to Public Information, strengthens the Personal Data Protection regime and the regulation of interest management.
- Legislative Decree No. 1412, Legislative Decree that approves the Digital Government Law. Section 5.10, Article 5.
- Supreme Decree No. 021-2019-JUS, which approves the Single Ordered Text of Law No. 27806, Law on Transparency and Access to Public Information. Article 17.
- Supreme Decree No. 024-2005-SA, which approves the Standard Health Data Identifiers. Article 1.
- Supreme Decree No. 003-2013-JUS that approves the Regulation of Law No. 29733, Personal Data Protection Law and its amendment Supreme Decree No. 019-2017-JUS.
- Supreme Decree No. 027-2015-SA, which approves the Regulation of Law No. 29414, Law that establishes the Rights of Users of Health Services. Article 19.
- Supreme Decree 092-2017-PCM, which approves the National Integrity and Fight against Corruption Policy.
- Supreme Decree No. 044-2018-PCM, which approves the National Integrity Plan

and Fight against Corruption 2018-2021".

- Supreme Decree No. 004-2019-JUS, Supreme Decree that approves the Single Ordered Text of Law No. 27444, General Administrative Procedure Law.

- Ministerial Resolution No. 369-86-SA–DM, which approves the Directive on the Functioning and Operability of Emergency Services of Hospitals of the Ministry of Health. Numeral 3 and 10.

- Ministerial Resolution No. 1201-2006-MINSA, which approves Administrative Directive No. 105-MINSA/SG.V.01, Administrative Directive for the classification of Information of the Ministry of Health.

- Ministerial Resolution No. 431-2015/MINSA, which approves the Technical Document "Information Security Policy of the Ministry of Health - MINSA".

- Ministerial Resolution No. 004-2016-PCM, which approves the mandatory use of the Peruvian Technical Standard "NTP ISO/IEC 27001:2014 Information Technology.
Security Techniques. Information Security Management Systems.
Requirements. 2a. Edition", in all the entities that make up the National Information Technology System.

- Ministerial Resolution No. 120-2017-MINSA, which approves "Administrative Directive No. 230-MINSA-2017-OGTI, "Administrative Directive that establishes the standards and technical criteria for the development of health information systems."

- Ministerial Resolution No. 214-2018/MINSA, which approves NTS No. 139-MINSA/2018/DGAIN: "Technical Health Standard for the Management of Clinical History" and its amendment approved by Ministerial Resolution No. 265-
2018/ONCE.

- Directorial Resolution No. 019-2013-JUS/DGPDP that approves the Security Directive.

The aforementioned regulations include their respective extension, modification and related provisions, if applicable.

V. GENERAL PROVISIONS

5.1 OPERATIONAL DEFINITIONS

5.1.1 **Information Asset:** It is any information or element related to its processing (software, computing and telecommunications equipment, email service, internet service, file cabinets) that has value for the organization. Understands the resources that an Information Security Management System has, so that the organization functions and achieves its objectives.

Base Legal

raised by the driving levels2. These assets that have value to the organization include: • Pure information assets (digital data),

• Tangible assets, Intangible assets, Application software, Operating systems, • Physical assets (infrastructure, hardware).

5.1.2 **Medical act:** It is any action or disposition carried out by the doctor in the exercise of the medical profession. This includes the acts of prevention, promotion, recovery (diagnosis, therapy, prognosis) and health rehabilitation, carried out by the doctor in the comprehensive care of patients, as well as those that derive directly from this3.

5.1.3 **Health act:** It is any action or activity carried out by health professionals except the Surgeon, for health interventions of health promotion, prevention, recovery and rehabilitation, as appropriate; that are provided to the patient, family and community.

Recovery includes clinical evaluation, diagnosis, prognosis, therapy and follow-up, according to the competencies of each health professional.

5.1.4 **National Health Authority.-** The Ministry of Health is the national Health Authority. As an agency of the Executive Branch, it is responsible for the formulation, direction and management of health policy and acts as the highest regulatory authority in health matters. It is the highest governing authority in the health sector5 .

5.1.5 **Personal data bank:** It is the organized set of personal data, automated or not, regardless of the support, whether physical, magnetic, digital, optical or others that are created, whatever the form or modality of its creation, formation. , storage, organization and access6.

5.1.6 **Database.-** It is a set of data belonging to the same context and systematically stored for later use, whose scope refers to primary, administrative and analytical data7 .

5.1.7 **Confidentiality of Information.-** It is an attribute that is assigned to information due to the nature of its content or by the principles that govern who accesses that information, which means that the content can only be accessed by authorized persons or those who become aware of it. in the exercise of their work, who have the duty to reserve said information and not comment on or disclose it outside the strictly professional scope or for the provision of services. The organization or entity guarantees that the information

2Ministerial Resolution No. 431-2015-MINSA, which approves the Technical Document “Information Security Policy of the Ministry of Health – MINSA.

3Ministerial Resolution No. 214-2018/MINSA, which approves NTS No. 139-MINSA/2018/DGAIN: “Technical Health Standard for the Clinical History Management.

4Ministerial Resolution No. 265-2018/MINSA, which approves the modification of the operational definition “Health Act” contained in the first bullet of subnumeral 4.1 OPERATIONAL DEFINITIONS of NTS N° 139-MINSA/2018/DGAIN: “Technical Health Standard for the Management of Clinical History”, approved with Ministerial Resolution No. 214-2018/MINSA.

5Definition taken from Legislative Decree No. 1504, Legislative Decree that strengthens the National Health Institute for the prevention and control of diseases and the General Health Law.

6Law No. 29733, Personal Data Protection Law and its amendments.

7 Definition prepared by the OGTI technical team.

It will be protected so that it is known only by authorized users8.

5.1.8 **Consent for the Processing of Personal Data.-** It is a principle established in Law No. 29733, Personal Data Protection Law, which allows the processing of personal data to be lawful when the owner of the personal data has given their free consent. , prior, express, informed and unequivocal9.

5.1.9 **Informed Consent.-** It is the express consent of the patient or his legal representative when the patient is unable to do so (for example: minors, patients with mental disabilities or a state of unconsciousness, or another), with respect to medical care, surgical or some other procedure; freely, voluntarily and consciously, after the doctor or competent health professional who will perform the procedure has informed you of the nature of the care, including the real and potential risks, side effects and adverse effects, as well as the benefits thereof. , which must be recorded and signed in a document, by the patient or their legal representative and the professional responsible for care10.

5.1.10 **Administrative data.-** It is all information that is generated in the administrative management of institutions, bodies, organic units, public organizations, including the IPRESS, which are part of the Health Sector, but which do not include personal data of the users. Said administrative data are necessary to fulfill its functions11.

5.1.11 **Personal data.-** It is all information about a natural person that identifies him or her or makes him or her identifiable through means that can be reasonably used. Likewise, it is any numerical, alphabetical, graphic, photographic, acoustic information, about personal habits or any other type of a natural person that identifies him or her or makes him individually identifiable through means that can be reasonably used12.

5.1.12 **Sensitive data.-** These are personal data consisting of biometric data that by themselves can identify the owner; data referring to racial and ethnic origin; economic income; political, religious, philosophical or moral opinions or convictions; union membership; and information related to health or sexual life. Likewise, information related to personal data referring to physical, moral or emotional characteristics, facts or circumstances of your emotional or family life, personal habits that correspond to the most intimate sphere, information related to physical or mental health or other analogous that affect their privacy13.

5.1.13 **Fundamental right.-** It is that which the State must guarantee as expressed in article 1 of the Political Constitution of Peru, by virtue of its axiological dimension of inseparable union with human dignity, being a necessary instrument for the individual to develop in society with all its potential14.

8Definition prepared by the OGTI technical team 9Definition taken from Law No. 29733, Personal Data Protection Law, its regulations and its amendments.
10Ministerial Resolution No. 214-2018/MINSA, which approves NTS No. 139-MINSA/2018/DGAIN: “Technical Health Standard for the Management of Clinical History” and its amendments
11Definition prepared by the OGTI technical team.
12Law No. 29733, Personal Data Protection Law, its amendment and its Regulations.
13Law No. 29733, Personal Data Protection Law, its amendment and its Regulations.
14Definition taken from what is stated in foundation 1 of ruling No. 1417-2005-AA of the Constitutional Court, the same one that generates binding precedent.

Disposiciones Específicas

5.1.14 **Information Integrity.-** It is the attribute of the information being correct and not having been modified, maintaining its data exactly as it was generated, without manipulations or alterations by third parties. This integrity is lost when information is modified or when part of it is deleted15.

5.1.15 **Interoperability.-** Interoperability is the ability of diverse and disparate organizations to interact to achieve objectives that they have jointly agreed upon, resorting to the sharing of information and knowledge, through processes and the exchange of data between their respective systems. of information16.

5.1.16 **Anonymization procedure.-** It is the processing of personal data that prevents identification or does not make the owner of the data identifiable. The procedure is irreversible17.

5.1.17 **Dissociation procedure.-** It is the processing of personal data that prevents identification or does not make the owner of the data identifiable. The procedure is reversible18.

5.1.18 **Information Security.-** It is the set of actions established with the purpose of preserving the confidentiality, integrity and availability of information, in addition to other characteristics such as authentication, responsibility, non-repudiation and reliability19.

5.1.19 **Owner of the personal data bank.-** It is the natural person, legal entity under private law or public entity, responsible for determining the purpose and content of the personal data bank, its processing and security measures20.

5.1.20 **Data frame.-** It is a two-variable data structure, where the rows represent cases or observations and the columns represent attributes or variables21.

5.1.21 **Processing of personal data.-** It is any technical operation or procedure, automated or not, that allows the collection, registration, organization, storage, conservation, elaboration, modification, extraction, consultation, use, blocking, deletion, communication by transfer or dissemination. or any other form of processing that facilitates access, correlation or interconnection to personal data22.

5.1.22 **Electronic transmission.-** It is the process by which data is sent

14Definition taken from what is stated in foundation 1 of ruling No. 1417-2005-AA of the Constitutional Court, the same one that generates binding precedent.
15Definition prepared by the OGTI technical team.
16Legislative Decree No. 1412, Legislative Decree that approves the Digital Government Law.
17Law No. 29733, Personal Data Protection Law and its amendments.
18Law No. 29733, Personal Data Protection Law and its amendments.
19Definition prepared by the OGTI technical team.
20Law No. 29733, Personal Data Protection Law and its amendments.
21Definition prepared by the OGTI technical team.
22Law No. 29733, Personal Data Protection Law and its amendments.

from one place to another through the means of Information and Communication Technologies (ICT), such as email, links, internet, among others23.

5.1.23 **User of information assets:** These are the people, whether they are servers, managers, public officials or third parties who are part of the organizations and entities that are specified in the scope of application of this Administrative Directive.

5.2 ACRONYMS:

- •ANS: National Health Authority
- •ARS: Regional Health Authority
- •DIRESA: Regional Health Directorate
- DIRIS: Directorate of Integrated Health Networks
- •DPS: Personal Health Data
- EESS: Health Establishments
- •GERESA: Regional Health Management
- IAFAS: Health Insurance Fund Administrator Institution
- IPRESS: Institutions Providing Health Services
- IS: Health Information
- •MINSA: Ministry of Health
- •OGEI: OGTI Office of Information Management
- •OGTI: General Information Technology Office •OTRANS: Transparency and Anti-Corruption Office of the Ministry of Health
- •SMA: Medical Support Service
- •ICT: Information and Communication Technologies

5.3 OF THE CLASSIFICATION OF DATA IN THE HEALTH SECTOR

The Ministry of Health, like all entities whether public or private, has information assets to fulfill its objectives.

The Ministry of Health, in its capacity as National Health Authority, classifies the information related to the problems, situation or health condition of the population in the health sector, (See Annex No. 01), into:

a) Personal Health Data (DPS) or Personal Data Related to Health b) Health Information or Health Information (IS)

5.4 PERSONAL HEALTH DATA OR PERSONAL DATA HEALTH RELATED – DPS

5.4. Personal Health Data (DPS) or Personal Data related to Health are all those referring to the health or illness situation of a person, and that identifies them and makes them individually identifiable, said information corresponds to past health and illness, present or predicted, physical or mental, of a person, including the degree of

23Definition prepared by the OGTI technical team.

disability and its genetic information. DPS are generated in any medical act or health act, or any health care received in a health establishment or outside of it.

5.4.2 The DPS according to Law No. 29733, Personal Data Protection Law are considered sensitive data. (See annex No. 02)

5.4.3 The DPS are protected by the Political Constitution of Peru, and not only in the content of the Fundamental Right to the Protection of Personal Data, but also in the Fundamental Right to Privacy and the Inviolability or secrecy of private documents. people, therefore, cannot be disseminated, nor treated in a way that violates their due reserve and confidentiality. (See annex No. 02)

5.4.4 Limitations to the exercise of the fundamental right to the protection of personal data can only be established by law, respecting its essential content and as long as they are justified by respect for other fundamental rights or constitutionally protected assets. (See annex No. 02)

5.4.5 The DPS in accordance with Law No. 29733, Personal Data Protection Law and the Single Ordered Text that approves Law No. 27806, Law of Transparency and Access to Public Information approved by Supreme Decree No. 021-2019 -JUS are considered sensitive data, which means that for their treatment, written consent must be obtained from the owner of said DPS.

Even without the consent of the owner, the processing of sensitive data can be carried out when the law authorizes it, as long as it meets important reasons of public interest. (See annex No. 02)

5.4.6 The reasons of public interest in health refer to exceptional access to the DPS of a person, or possibly more, without their consent, when that information is necessary to protect the population; In no case can it be interpreted that this exceptionality can be extended to the entire population and access to the DPS of entire populations or groups of populations, since for this the written and express consent of each person must be required, according to the characteristics established in the Law. (See Annex No. 05)

The DPS are only accessed, regardless of the consent of the owner according to the Law, when they correspond for reasons of public interest provided for by Law, or when they must be treated for reasons of public health and the Ministry of Health has qualified them as such, through the corresponding resolutive act, in accordance with the provisions of Law 29733 Personal Data Protection Law (art. 14, paragraph 6).

5.4.7 All DPS have a owner to whom they belong and can exercise their rights of access, rectification, cancellation, opposition, right to protection, objective treatment, among others indicated in Law No. 29733, Data Protection Law Personal and its regulations.

5.4.8 DPS are generated during the care that people receive, whether in medical acts or health acts, in health establishments, in consultations, hospitalization, emergency, medical support services, telemedicine health services and others. care services, at home, in extramural care, in pre-hospital care, in demand care, in care of strategic health interventions, and any other form of health care. In addition, they can be generated in research, health surveys or other related activities in the field of health which generate personal data related to health or personal health data.

5.4.9 The DPS include information related to the medical act or health information that may affect personal and family privacy or self-image, national security and foreign relations, as well as those referring to aspects protected by the regulations. of industrial property, as provided by Law No. 26842, General Health Law. (See Annex No. 02)

5.4.10 The Ministry of Health in the exercise of its National Health Authority, regulating, supervising and sanctioning as appropriate, guarantees compliance with the constitutional and fundamental right of the protection of the DPS of users of public health services, private and mixed.

5.4.11 Officials, directors, servants of the Ministry of Health, or other person, whatever their employment or contractual relationship, who work or provide services in the administrative or healthcare areas, including officials, directors, servants and personnel who work or provide services in public, private and mixed health establishments, are responsible, as appropriate, for ensuring compliance with the provisions of this Administrative Directive.

5.4.12 As long as there is prior and explicit written consent from the owner of its DPS, the public, private and mixed EESS may share them with another EESS that provides direct health care to the aforementioned owner. The EESS must take the necessary measures to ensure compliance with this provision.

5.4.13 The consent of the holder of the DPS will be dispensed with when they are necessary in circumstances of risk, for the prevention, diagnosis and medical or surgical treatment of the holder of said DPS, provided that said treatment is carried out in health establishments or by professionals. of health, respecting professional secrecy.

5.4.14 The construction of nominal lists containing DPS is not permitted, whether of patients, sick people, whether or not they receive treatment from the State, nor as a benefit of social programs, since they violate the fundamental rights of people. The DPS are only available and properly protected in the public, private and mixed EESS, where each patient was treated, thereby respecting the purpose for which they were collected.

5.4.15 The interoperability that occurs between information systems must not violate the right of each user to the protection of their DPS.

5.4.16 The Ministry of Health regulates and supervises that all entities in the health sector, public, private and mixed as appropriate, that for reasons of their function participate in the treatment of DPS, must guarantee that their information assets protect and ensure the inviolability of the DPS to which they access. This provision applies to the ANS, ARS, the IPRESS, the IAFAS, the entities that train human resources in health, and any other entity that is authorized to participate in the treatment of DPS. (See Annex No. 01)

5.5 HEALTH INFORMATION OR INFORMATION ON THE SUBJECT HEALTH - IS

5.5.1 Health Information or health information – IS is that which arises from care in health establishments and services, and is made up of the set of statistical data, dissociated or anonymized data related to health, which They do not allow the individual identification of one or more people or users, therefore, it does not include DPS. It also includes the administrative and financial data of the management of the organization or entity in the health sector.

5.5.2 The DPS, when subjected to the due anonymization and dissociation procedures, become Health Information, of a statistical nature, where it is not possible to know the individual identity of the holders of the original DPS. Only in this condition can health establishments transmit, by the corresponding means, whether physical or electronic transmission, the health information of the establishment, related to the health of its users.

5.5.3 The SI is of public interest. Every person is obliged to provide the National Health Authority with the information required by law.

5.5.4 The SI, for its presentation or publication, must not contain items that allow the identification of the person from whom it was obtained, that is, the individual identification of one or more people or users. Health information refers to epidemiological, statistical, and population information, which is anonymized.

5.5.5 The SI that public sector entities have in their possession is public domain; with the exceptions established by Law.

5.5.6 Public health policies are formulated and evaluated with the availability of real, updated, true health information, and at the relevant level of detail. It is not necessary to violate the DPS for this purpose.

(See Annex No. 01)

SAW. SPECIFIC PROVISIONS

6.1 OF THE GENERATION OF THE DPS

6.1.1 All records of care provided in health facilities or in home and pre-hospital care (campaigns), or medical support services, generate information that corresponds to DPS.

6.1.2 The healthcare staff of the health establishment that participates in the various care is responsible for the proper use of the DPS, the physical or digital records that they generate or use, as well as their treatment that protects the confidentiality and privacy of people's information. attended.

6.1.3 The administrative staff who participate in the support processes for the care of people in the health establishment, or medical support services, also act responsibly to respect the confidentiality and privacy of the information of the people cared for.

6.1.4 Directors, managers, chiefs, chief doctors, or those who take their place in health establishments or medical support services, must arrange the corresponding measures to guarantee the protection of the DPS in the care processes carried out in the EESS. or SMA in charge, as well as supervising compliance.

6.1.5 The DIRESA / GERESA, or the DIRIS, if applicable, or the administrative bodies of the other public, private and mixed EESS or SMA of the National Health System, must take the necessary administrative measures so that the EESS have the relevant resources to ensure the protection of the DPS of the patients they care for.

6.1.6 The patients' DPS should not leave the EESS or SMA under any circumstances, except in cases contemplated by law, or when it has been expressly authorized by the owner of the DPS.

6.1.7 The public, private and mixed EESS or SMA are obliged to send health information, which is generated from the care they provide, according to what the ANS requires, with punctuality, quality, certainty, in the formats or reports. that establishes for that purpose. The health information that is reported or transmitted will always be statistical and anonymized, under responsibility. Patients' DPS may not be transmitted or transferred, except in cases contemplated by Law or written authorization of the owner of said data.

6.1.8 The EESS or SMA that generates the DPS may access that information and send it exceptionally as appropriate to the ANS at the time it requires it, taking into account what is stated in paragraph 6 of article 14 of Law No. 29733, Law of Personal data protection.

6.2 DPS PROTECTION

6.2.1 The public, private and mixed EESS or SMA must take the technical, organizational and legal information security measures necessary to ensure the protection of the DPS of the patients they serve.

6.2.2 The DPS recorded in storage media, based on the care provided, are subject to the provisions of the current Technical Health Standard for Clinical History Management, and to the regulations on documentary files in force in the State.

6.2.3 The MINSA arranges what is necessary and provides the computer support for the software it develops so that the public EESS and SMA can guarantee the DPS protection of the patients they care for.

6.2.4 The EESS or SMA guarantee that the DPS generated in health care will not be sent, transferred or shared with another healthcare or administrative entity outside the respective EESS or SMA, under any circumstances, except as indicated in current legal regulations.

6.2.5 The exception to the transfer or submission of personal data related to health only applies in situations provided for by law or when the owner has authorized, expressly and in writing, its submission or transfer.

6.2.6 The Ministry of Health, in its capacity as National Health Authority, may exceptionally request the DPS of certain users of health services as long as it is for public health reasons duly approved by the head of the Ministry of Health.

6.2.7 The DPS that is collected from people voluntarily, as a product of health-related surveys by health professionals or health personnel, is strictly confidential, and it is their obligation to keep the confidentiality that the case merits.

6.3 OF THE TREATMENT OF THE DPS AND THE INFORMATION IN HEALTH

6.3.1 The public, private and mixed EESS or SMA send statistical and anonymized information, according to what has been established by the ANS, through its regulatory documents.

6.3.2 The health information is sent to the micro network, network, DIRESA /GERESA or DIRIS, or the one that takes its place at the National Level, as appropriate and has been arranged, using the mechanisms established for that purpose.

6.3.3 Health Information must not transmit data that identifies the person, and will be disaggregated into the attributes of age, sex, residence

(locality, town center, district, province, department), diagnosis, treatment, and others, as appropriate and established by the ANS in the respective regulatory document; ensuring that there is no way to individually identify the people served in the transferred information. The ANS must have the necessary mechanisms so that the data produced in health facilities maintain the integrity and confidentiality contemplated by the Law. The ARS must apply the provisions of the ANS, under responsibility.

6.3.4 The EESS or SMA must have the capacity to individually identify the patients whose care is contained in the health information sent, in the event that, for reasons of public health protection, the ANS requires it directly or through the ARS.

6.3.5 The OGTI is responsible for designing and putting into service the computer platform that allows the periodic online reporting of health information from the EESS itself, and which must allow access for reading and analysis to authorized personnel of the micro network, Network, DIRESA /GERESA or DIRIS, or at the National Level, as appropriate. This platform is designed based on the requirements of the ANS, and in no case does it include DPS.

6.3.6 The ANS is the only entity responsible for defining, authorizing and providing health information to public and private entities, inside and outside the health sector, that is necessary for the evaluation and monitoring of compliance with public policies.

6.3.7 Officials or public servants are responsible for respecting the fundamental rights of all people, including the protection of personal data and privacy, therefore, they may not request or provide the DPS of one or more people, to any person or entity that requests it, under administrative, civil and criminal responsibility, except in the exceptions contained in the Law.

6.3.8 Tests that are sent for diagnosis or diagnostic confirmation purposes to the National Institute of Health, through NETLAB, must ensure DPS protection, using patient coding mechanisms, which allow them to only be identified by the doctor. trafficker

6.4 THE FLOW OF HEALTH INFORMATION

6.4.1 Each public, private and mixed EESS or SMA sends, through electronic transmission or any other means, the required health information with the characteristics and within the deadlines established in the regulatory documents for the information platform that the ANS establishes. available.

6.4.2 The EESS or SMA send it to the micro network in the computer platform, in cases where they have access to the internet, which must immediately make said information available on the network, in the DIRESA / GERESA or DIRIS, and in the Ministry of Health. This statistical and anonymized information must be able to be grouped and disaggregated at geographic levels: national, departmental,

Disposiciones Específicas

provincial, district and by EESS.

6.4.3 If the EESS or SMA do not have internet services, they will physically send health information to the micro network or EESS defined as a data entry point so that it can be entered into the corresponding computer platform.

6.4.4 When for reasons of public health protection, the ANS requires DPS, contained in the medical history of a patient or patients, it will request it through personnel authorized to the ARS or directly to the EESS.

6.4.5 The EESS or SMA that is requested to provide health information of special interest must provide it immediately and securely.

6.4.6 Natural or legal persons are obliged to provide the National Health Authority with epidemiological information and that which is required to protect the health of the population, within the terms of responsibility, classification, periodicity and destination indicated in this document. Administrative Directive or the laws that regulate the matter.

6.5 OF INFORMATION ASSETS

6.5.1 The information, together with the processes, systems, network equipment, technical personnel and services linked to its processing, make up the information assets of the organization or entity, which are of vital importance for the fulfillment of its mission, vision. , objectives, functions, and plans of the Ministry of Health.

6.5.2 It is the responsibility of the Ministry of Health, through its bodies, organic units, public organizations and programs, to adequately protect the integrity, security, confidentiality and availability of its information assets.

6.5.3 The DIRIS, DIRESA or GERESA, and the EESS and SMA are responsible for the information assets they manage, therefore, they must implement the information security mechanisms that are necessary.

6.6 OF THE SENDING OF PERSONAL HEALTH DATA TO OTHER PUBLIC ADMINISTRATION ENTITIES OR PRIVATE

6.6.1 The bodies, organic units, public organizations and programs of the Ministry of Health are not authorized, under administrative, civil or criminal responsibility, to send the DPS to any public or private institution or entity that requests it. Likewise, the EESS, SMA, DIRIS, DIRESA or GERESA are not authorized to send the DPS to any

public or private institution or entity that requests it with the exceptions described in this Administrative Directive and in current legal regulations.

6.6.2 The Ministry of Health may send the health information it manages to public or private institutions or entities, ensuring that the protection of the DPS is not violated in any case.

6.6.3 In the event that a person's medical history is requested, the information contained therein may only be delivered and sent outside the health establishment, as long as some of the exception requirements indicated in article 25 of Law No. 26842, General Health Law. (See Annex No. 02)

6.6.4 In response to the collaboration carried out with other entities of the public or private administration for the sending of health information, to meet the objectives, this may be sent only if they are DPS with the consent of the owner of said data. data, in writing and expressly, or if they are anonymized data, in accordance with the provisions of Law No. 29733, Personal Data Protection Law, art 13, paragraph 13.6, and article 14, paragraph 6.

6.6.5 The official and/or public servant or directors of private entities who deliver information containing DPS, contravening the provisions of this Administrative Directive, incurs serious misconduct, and will be liable to the administrative, civil and criminal sanctions established in the current legal framework. .

6.6.6 For cases of extra-institutional electronic transmission, that is, with other requesting State entities, in no case will databases or data frames containing Personal Health Data be included, under responsibility.

6.7 RIGHTS OF DPS HOLDERS

6.7.1 So that the owners of the DPS can exercise their rights of access, rectification, cancellation, opposition, protection and others established in Law No. 29733, Personal Data Protection Law, the General Directors, or Heads of the EESS, SMA, DIRIS, DIRESA or GERESA, officials and directors of the private entities referred to in this Administrative Directive must designate an area to respond to their requests, as established in the regulatory documents approved by the ANS.

6.7.2 The holders of the DPS may exercise their rights in the places where they consider that their DPS has been affected, in the EESS, DIRIS, DIRESAS / GERESAS, and the ANS as appropriate.

6.7.3 DPS holders must have the appropriate conditions to grant their consent to the processing of their DPS, by means of a handwritten signature or

Disposiciones Específicas

digital, or other authentication mechanism that guarantees the unequivocal will of the owner. The consent of the owner of the DPS must have the characteristics of being free, prior, express, informed and unequivocal, and formulas of consent in which this is not expressed directly should not be admitted, such as those in which it is required to presume or assume the existence of a will that has not been expressed.

(See Annex No. 05)

6.7.4 The owner of the DPS may revoke consent to the treatment of his DPS at any time, and the professional or health personnel or person who treats these must respect his will, under responsibility.

6.8 INFORMATION SECURITY MEASURES

6.8.1 The directors or heads of the EESS are responsible for designating personnel to implement the security measures of the DPS, avoiding the loss or destruction of these, both manually and through the use of ICT, and must adapt to the provided in the “Technical Health Standard for the Management of Clinical History”.

6.8.2 Users of the information assets of the Ministry of Health, its bodies, public organizations, the administrative bodies of the DIRESAS or GERESAS, and the IPRESS must apply or implement, as appropriate, the following security measures. the information, in addition to the security measures established in the

Regulations of Law No. 29733, articles 39 to 46 of Chapter V:

a) The user registration and cancellation process must be implemented to allow the assignment of access rights to personal health data.

b) The assignment and use of privileged access rights must be restricted and controlled, according to the assigned responsibilities and for a period of three months, requesting its renewal if warranted.

c) The Information Technology Offices, or those that take their place, designate responsible and competent personnel in their jurisdiction, with the purpose of reviewing user access rights at regular intervals at the national level.

d) Access to personal health data in information systems must be restricted and controlled by a secure entry procedure, carried out by the personnel who implement the security measures of the DPS.

6.8.3 The OGTI of the Ministry of Health is responsible for preparing the regulatory document that specifies the technical, organizational and legal security measures in the health sector, in accordance with the provisions of the Law.

No. 29733, Personal Data Protection Law and its regulations.

6.9 OF THE CONFIDENTIALITY CRITERIA OF THE DPS

Any duly authorized user of the information assets described in this Administrative Directive is obliged to:

a) Do not reveal or provide in any way, to any natural or legal person, and do not use for your own benefit or for the benefit of any other person, information related to the service you provide.

b) Manage and provide confidential information, if applicable, as indicated by the Law, with the care and reasonableness that it deserves and will take security measures for both DPS protection, management, and information technology, to prevent the confidential information is manipulated, changed, distorted, denatured in its form and substance by third parties.

c) Treat the DPS with the exclusive purpose of fulfilling the functions that correspond to it, under administrative, civil and criminal responsibility that may apply.

d) Sign the confidentiality commitment established in Annex No. 03 and 04. The Confidentiality Commitment must be signed by personnel with an employment relationship or contractual relationship.

6.10 TREATMENT OF DPS IN STATES OF HEALTH EMERGENCY OR PANDEMIC SITUATIONS

a) The information generated from the care of patients in health emergency or pandemic situations, as long as it corresponds to DPS, must receive the same treatment that DPS receive under normal conditions, in accordance with the provisions of this Directive. Administrative.

b) If, due to the conditions that care is provided in these circumstances, documentation files of a temporary nature are generated, and that contain DPS, they must be subject to the corresponding security measures, which guarantee the privacy, security, inviolability of the information. contained there.

c) As soon as it is operationally possible, or at the end of the state of health emergency, the files of a transitory nature, which contain DPS of the patients treated, must be relocated with the usual files of the health facility. This includes that the information of each patient is unified in their corresponding medical history.

d) In no case can documentation of patient care that contains DPS be eliminated during the health emergency period. The healthcare or administrative staff who have contact with documentation containing DPS of the patients treated are obliged to maintain the corresponding confidentiality and confidentiality, under responsibility.

Disposiciones Específicas

VII. RESPONSIBILITIES

7.1 The Ministry of Health, through the General Office of Information Technologies, is responsible for the dissemination of this Administrative Directive to the regional level; as well as technical assistance and supervision of compliance.

7.2 The organs and organic units of the Ministry of Health, its deconcentrated bodies, assigned public organizations, and national programs; the Regional Health Authority and its agencies (EESS and SMA); and public and private entities in the health sector are responsible for compliance with this Administrative Directive in their respective institutional and jurisdictional spheres.

7.3 The Regional Health Authority, and the DIRIS in Metropolitan Lima, is responsible for the dissemination, application, technical assistance and supervision of this Administrative Directive in their respective jurisdictional areas.

7.4 The assistance and administrative personnel who, due to their activities or work, come into contact with the DPS are responsible for acting in accordance with the provisions of this Administrative Directive.

VIII. FINAL PROVISIONS

8.1 In the case in which traffic, transmission is detected without the authorization of its owners, as well as the falsification, manipulation or modification of the DPS, the General Directors, or Heads of the EESS, SMA, DIRIS, DIRESA or GERESA, officials or servants are obliged to report this fact to the Anti-Corruption Transparency Office of the Ministry of Health (OTRANS), the National Police of Peru or the Public Ministry, under administrative, civil or criminal responsibility that may arise.

8.2 It is the responsibility of the General Directors, or heads of the EESS, SMA, DIRIS, DIRESA or GERESA, officials and public servants and directors of private entities that the DPS are stored and safeguarded for the established time and until the purpose for which they were collected. Its treatment and final disposal must be carried out with the same criteria established in NTS No. 139-MINSA/2018/DGAIN, Technical Health Standard for the Management of Clinical History approved by Ministerial Resolution No. 214-2018/MINSA, its amendment or the one that replaces it, and the legal regulations that apply to it.

IX. ATTACHMENTS

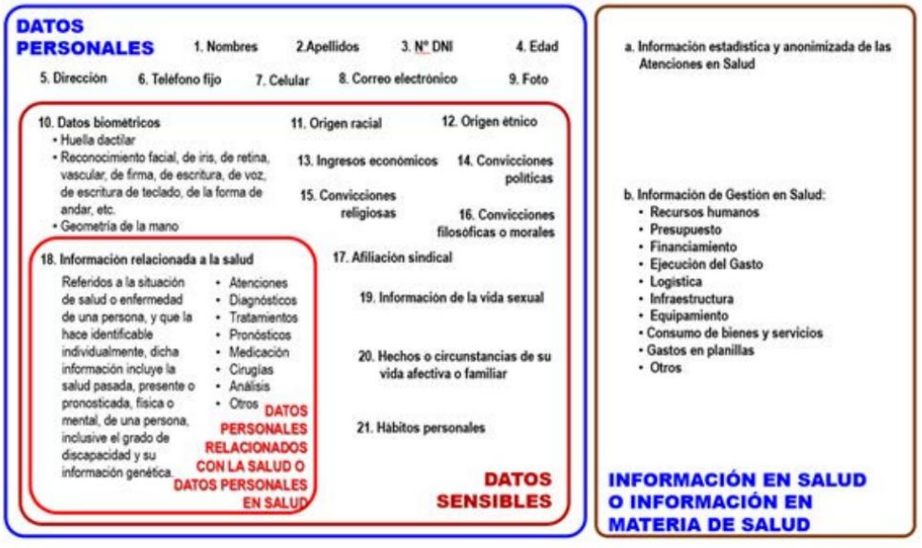
Annex 01.- Data Classification Chart in the Health Sector

Annex 02.- Regulatory references that recognize and guarantee the right to the protection of personal health data

Annex 03.- Confidentiality commitment of personnel with an employment relationship
Annex 04.- Confidentiality commitment of personnel with a contractual relationship
Annex 05.- Characteristics of consent for the Treatment of DPS in accordance with the provisions of article 12 of the Regulation of Law No. 29733, Personal Data Protection Law.

ANNEX No. 01

Data Classification Chart in the Health Sector



Disposiciones Específicas

ANNEX No. 02

REGULATORY REFERENCES THAT RECOGNIZE AND GUARANTEE THE FUNDAMENTAL RIGHT TO THE PROTECTION OF PERSONAL DATA IN HEALTH

Political Constitution of Peru

The Political Constitution of Peru in its article 2 regarding rights fundamentals of the person states that: Every person has the right:

6) That **computer services, computerized or not, public or private, do not provide information that affects personal and family privacy.**

7) To honor and good reputation, **to personal and family intimacy,** as well as as well as one's own voice and image. (…)

10) To the secrecy and inviolability of your communications and **private documents.** Communications, telecommunications or Their instruments can only be opened, seized, intercepted or intervened by reasoned order of the judge, with the guarantees provided for in the law. Secrecy is kept from matters unrelated to the fact that motivates your examination. Private documents obtained with Violation of this precept has no legal effect. (…)

Law No. 29733, Personal Data Protection Law

Law No. 29733, Personal Data Protection Law, in its article 2 Definitions, established as:
(…)

4. Personal data. Any information about a natural person who identifies or makes it identifiable through means that may be reasonably used.

5. Sensitive data . Personal data consisting of biometric data that by themselves can identify the owner; data referring to racial and ethnic origin; economic income; political, religious, philosophical or moral opinions or convictions; union membership; and information related to health or sexual life.

Article 13. Scope of the processing of personal data (…)

13.5 Personal data can only be processed with the consent of the owner, except by authoritative law in this regard. Consent must be prior, informed, express and unequivocal.

13.6 In the case of sensitive data, consent for the purposes of its processing must also be given in writing. Even without the consent of the owner, the processing of sensitive data can be carried out when the law authorizes it, as long as it meets important reasons of public interest. (…)

Article 14. Limitations on consent for the processing of personal data

The consent of the owner of personal data is not required to
the effects of your treatment in the following cases:
(…)

6. When it involves personal data related to health and is necessary, **in a risk circumstance,** for the prevention, diagnosis and medical or surgical treatment of the owner, provided that said treatment is carried out in health establishments or by health sciences professionals. health, observing professional secrecy; **or when there are reasons of public interest provided for by law or when they must be treated for reasons of public health, both reasons must be qualified as such by the Ministry of Health;** or for carrying out epidemiological or similar studies, as long as appropriate dissociation procedures are applied. (…)

Article 17. Confidentiality of personal data

The owner of the personal data bank, the person in charge and those who intervene in any part of its processing are obliged to maintain confidentiality regarding them and their background. This obligation subsists even after the relationship with the owner of the personal data bank has ended.

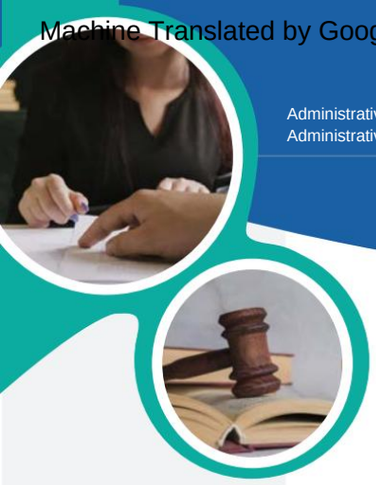
The obligated party may be relieved of the obligation of confidentiality when there is prior, informed, express and unequivocal consent of the owner of the personal data, a consented or enforceable judicial resolution, or when there are well-founded reasons related to national defense, public security or public health. , without prejudice to the right to maintain professional secrecy.

» Supreme Decree No. 003-2013-JUS, which approves the Regulation of Law No. 29733, Personal Data Protection Law, provides:

4. Personal data: It is that numerical, alphabetical, graphic, photographic, acoustic information, about personal habits, or any other type concerning natural persons that identifies them or makes them identifiable through means that can be reasonably used.

5. Personal data related to health: This is information concerning the past, present or predicted health, physical or mental, of a person, including the degree of disability and their genetic information.

6. Sensitive data: This is information related to personal data referring to the physical, moral or emotional characteristics, facts or circumstances of your life.



emotional or family, personal habits that correspond to the most intimate sphere, information related to physical or mental health or other similar information that affects your privacy.

» Single Ordered Text of Law No. 27806, Law of Transparency and Access to Public Information approved by Decree Supremo N° 021-2019-JUS

According to Supreme Decree No. 021-2019-JUS, which approves the Single Ordered Text of Law No. 27806, Law on Transparency and Access to Public Information, article 17 states that they are exceptions to the exercise of the right of access to public information: Confidential information: The right of access to public information may not be exercised with respect to the following: (…)

5) Information referring to personal data whose publicity constitutes an invasion of personal and family privacy. **Information referring to personal health is considered to be included within personal privacy.** In this case, only the judge can order the publication without prejudice to the provisions of paragraph 5 of article 2 of the Political Constitution of the State. (*)

(*) In accordance with the Eighth Final Complementary Provision of Law No. 29733, published on July 3, 2011, it is specified that the confidential information referred to in this section constitutes sensitive data in accordance with the scope of the aforementioned Law, the which comes into effect within a period of thirty business days, counted from the publication of the regulations of the aforementioned Law.

» Law No. 26842, General Health Law

Section XIV of the preliminary title: Health information is of public interest. Every person is obliged to provide the Health Authority with the information required by law. What the State has in its possession is in the public domain, **with the exceptions established by law.**

Article 15. Every person has the right to the following:

15.3 Health care and recovery
a) To be attended to with full respect for their dignity and privacy without discrimination due to action or omission of any kind.

Article 25. All information related to the medical act that is performed, It has a reserved nature.

The health professional, technician or assistant who provides or discloses, by any means, information related to the medical act in which he participates or of which he has knowledge, incurs civil or criminal liability, as the case may be, without prejudice to the sanctions that correspond in application of the respective Codes of Professional Ethics.

Anexos

They are exempt from the reservation of information related to the medical act in the following cases:

a) When there is written consent from the patient;

b) When required by the competent judicial authority;

c) When it is used for academic or scientific research purposes, provided that the information obtained from the clinical history is recorded anonymously;

d) When it is provided to family members or close friends of the patient with the purpose of benefiting them, as long as the patient does not expressly prohibit it;

e) When it concerns diseases and damages that must be declared and notified, as long as it is provided to the Health Authority;

f) When it is provided to the insurance entity or financing administrator linked to the care provided to the patient, provided it is for the purposes of reimbursement, payment of benefits, supervision or audit;

g) When necessary to maintain continuity of medical care to the patient. patient;

h) When strictly necessary for the exercise of the functions of supervision and protection of health rights of the National Health Superintendency. For the application of this exception, this Superintendency must prove that it has previously requested the consent of the patients or their representatives to access the content of their medical history and that it has not obtained a response within the period that will be determined by supreme decree. Additionally, it must support the seriousness of the facts involved with respect to the impact on the rights to health or life of the patients, whose requirements and conditions will be defined by regulatory standard.

Article 120. All health information that Public Sector entities have in their possession is in the public domain. **Exceptions are information that may affect personal and family privacy or self-image,** national security and foreign relations, as well as information that refers to aspects protected by industrial property regulations in accordance with the law.

Of the mattery.

» Regulation of health establishments or medical support services approved by Supreme Decree No. 013-2006-SA

Article 116.- Confidentiality of patient information

The health establishment and medical support service must guarantee respect for the dignity, integrity, privacy, intimacy of the patient or user, as well as the confidentiality of information about the illness of the patient who participates in teaching activities.

Anexos

» Law No. 30024, Law that creates the National Registry of Clinical Records Electronics and its amendment DL No. 1306

Article 7. Confidentiality of the National Registry of Electronic Medical Records.

Those involved in the management of the information contained in the National Registry of Electronic Medical Records are obliged to maintain confidentiality with respect to it, in accordance with numeral 6) of article 2 of the Political Constitution of Peru; Law 29733, Personal Data Protection Law, and other regulations, under administrative, civil or criminal responsibility, as the case may be.

THIRD FINAL COMPLEMENTARY PROVISIONS. Ownership, reservation and security of clinical information

The clinical information contained in electronic medical records is the property of each patient; Their confidentiality, privacy and confidentiality are guaranteed by the State, health establishments and medical support services.

The patient has the right to reserve their clinical information, with the exceptions established by Law 26842, General Health Law, and especially sensitive clinical information related to their physical or mental health, physical, moral or emotional characteristics, facts. or circumstances of their emotional or family life, personal habits and others that correspond to their intimate sphere.

» Legislative Decree No. 1353, Legislative Decree that creates the Authority National Transparency and access to public information, strengthens the personal data protection regime and the regulation of interest management

Article 10.- Confidentiality of information (...)

10.2 When dealing with secret, reserved or **confidential information, they have the obligation to take diligent care if they become aware of it in the exercise of their function. Likewise, they cannot make it public knowledge.** These obligations extend for five (5) years after leaving the position or as long as the information remains secret, reserved or confidential.

Failure to comply with this duty is considered a serious offense, without prejudice to the civil or criminal liability that it entails.

Anexos

» Supreme Decree No. 019-2017-JUS, which approves the Regulation of Legislative Decree No. 1353, Legislative Decree that creates the National Authority for Transparency and Access to Public Information, strengthens the Personal Data Protection Regime and the regulation of interest management.

Article 36.- Sanctions against civil servants

In case of violation of the rules of the Law or of this Regulation, the entity applies the following sanctions to civil servants, in accordance with article 29 on the graduation of the sanction:

1. Minor infractions are punished with a written reprimand or an unpaid suspension of between ten (10) and thirty (30) days.

2. Serious infractions are punished with an unpaid suspension of between thirty-one (31) days and one hundred twenty (120) days.

3. Very serious infractions are punished with suspension without pay of between one hundred twenty-one (121) days and one hundred eighty (180) days, or dismissal and disqualification for up to 2 years.

In the event of a repeat offense in the commission of two (02) minor infractions, in the same year, the third minor infraction is punished as a serious infraction.

In the event of a repeat offense in the commission of two (02) serious infractions, in the same year, the third serious infraction is punished as a very serious infraction.

» Legislative Decree No. 1246, Legislative Decree that approves various simplification measures administrative

Article 2.- Interoperability between Public Administration entities

Provide that Public Administration entities, free of charge, through interoperability, interconnect, make available, allow access or provide the information or updated databases that they manage, collect, systematize, create or possess regarding users. or administered, that other entities necessarily require and in accordance with law, for the processing of their administrative procedures and for their internal administration acts.

Anexos

In cases in which the information or data is protected under Law No. 29733, Personal Data Protection Law, Public Administration entities must obtain the express and indubitable authorization of the user or administrator to access said information or data.

» **Legislative Decree No. 1412, Legislative Decree that approves the Digital Government Law.**

Article 5.- Guiding principles
(...)

5.9 Default Open Data. - The data is open and available immediately, without compromising the right to protection of citizens' personal data.

When in doubt, it is up to the Transparency Authority to define it.

5.10 Adequate level of protection for personal data.- The processing of personal data must be carried out in accordance with the provisions of the Personal Data Protection Law and its Regulations.

Anexos

ANNEX No. 03
Commitment to Confidentiality of Personnel with an Employment Relationship

COMPROMISO DE CONFIDENCIALIDAD

Lima,.....de..... de .....

El (LA) SUSCRITO (A):

CARGO:

DEPENDENCIA:

RELACIÓN CON EL MINSA:

En virtud de la Ley N° 29733 - Ley de Protección de Datos Personales y de la Resolución Ministerial N° 004-2016-PCM que aprueba el uso obligatorio de la Norma Técnica Peruana NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2DA Edición, en todas las entidades integrantes del Sistema Nacional de Informática, implementado en la Institución, acepto y reconozco que por motivo de mi condición laboral y contractual con el MINSA y por el trabajo y las funciones que realizo para esta Institución tengo acceso a tecnología, documentos, datos, especificaciones, métodos, procesos y en general información CONFIDENCIAL, en tal virtud, por este medio me obligo a no divulgar, revelar, comunicar, transmitir, grabar, duplicar, copiar o de cualquier otra forma reproducir, sin la autorización expresa y por escrito del Ministerio de Salud, la información y documentación a la que tengo acceso. En caso del tratamiento de datos personales, me obligo solo a almacenarlos y gestionarlos en los soportes y modalidades autorizadas por el Ministerio de Salud.

Por lo que declaro, haber leído y tener conocimiento de los documentos de gestión que involucran mi función y desenvolvimiento en el Ministerio de Salud, el Reglamento de Organización y Funciones del Ministerio de Salud - ROF, La Ley 27815 – Ley de Ética de la Función Púbica y demás normativa pertinente.

En caso de incumplimiento, me someto a las responsabilidades de índole administrativa, civil y/o penal conforme a Ley.

Las obligaciones y derechos inmersos en el presente acuerdo de confidencialidad estarán vigentes a partir de la fecha de firma del vínculo con la Institución, durante el tiempo que dure esta relación y dos años después de la fecha en que se haya dado por terminada la relación laboral, sin importar la razón de la misma.

A los efectos previstos en este Compromiso, se define como "Información confidencial" a toda aquella información, ya sea técnica, financiera, comercial, datos personales, personal o de cualquier otro carácter, que sea suministrada y/o comunicada por el Ministerio de Salud o por un tercero por encargo del Ministerio de Salud, mediante palabra, por escrito o por cualquier otro medio o soporte, tangible o intangible, actualmente conocido o que posibilite el estado de la técnica en el futuro.

En el supuesto de que, previamente a la firma del presente compromiso, el suscrito hubiera tenido acceso a la información de la institución u otra que se le haya encargado para el cumplimiento de las obligaciones establecidas con el Ministerio de Salud, aquella será considerada también, a todos los efectos previstos en el presente documento, como información confidencial, salvo aquella que expresamente sea calificada por el Ministerio como información de libre uso o divulgación.

Firma: _____

DNI:

Anexos

ANNEX No. 04
Confidentiality Commitment of Personnel with a Contractual Relationship

COMPROMISO DE CONFIDENCIALIDAD

Lima,.....de..... de.....

El (LA) SUSCRITO (A):

DEPENDENCIA:

ORDEN DE SERVICIOS Nº:

En virtud del cumplimiento de la Resolución Ministerial N° 074-2017/MINSA, que aprueba la Directiva Administrativa N° 227-MINSA/2017/OGTI correspondiente a la "Organización del Sistema de Gestión de Seguridad de la Información del Ministerio de Salud", de la Ley N° 29733 - Ley de Protección de Datos Personales y del Sistema de Gestión de Seguridad de la Información, implementado en la Institución, acepto y reconozco que por motivo de mi condición contractual con el MINSA y por las prestaciones y las funciones que realizo para esta Institución tengo acceso a tecnología, documentos, datos, especificaciones, métodos, procesos y en general información CONFIDENCIAL, en tal virtud, por este medio me obligo a no divulgar, revelar, comunicar, transmitir, grabar, duplicar, copiar o de cualquier otra forma reproducir, sin la autorización expresa y por escrito del Ministerio de Salud, la información y documentación a que tengo acceso. En caso del tratamiento de datos personales, me obligo solo a almacenarlos y gestionarlos en los soportes y modalidades autorizadas por el Ministerio de Salud.

En caso de incumplimiento, me someto a las responsabilidades de índole administrativa, civil y/o penal conforme a Ley.

Las obligaciones y derechos inmersos en el presente acuerdo de confidencialidad estarán vigentes a partir de la fecha de firma del vínculo con la Institución, durante el tiempo que dure esta relación y después de la fecha en que se haya dado por terminada la relación contractual o profesional presente o las que se establezcan en el futuro, sin importar la razón de la misma.

A los efectos previstos en este Compromiso, se define como "Información confidencial" a toda aquella información, ya sea técnica, financiera, comercial, datos personales, personal o de cualquier otro carácter, que sea suministrada y/o comunicada por el Ministerio de Salud o por un tercero por un encargo del Ministerio de Salud, mediante palabra, por escrito o por cualquier otro medio o soporte, tangible o intangible, actualmente conocido o que posibilite el estado de la técnica en el futuro.

En el supuesto de que, previamente a la firma del presente compromiso, el suscrito hubiera tenido acceso a la información de la institución u otra que se le haya encargado para el cumplimiento de las obligaciones establecidas con el Ministerio de Salud, aquella será considerada también, a todos los efectos previstos en el presente documento, como información confidencial, salvo aquella que expresamente sea calificada por el Ministerio como información de libre uso o divulgación.

Firma: _____

DNI:

ANNEX No. 05

Characteristics of consent for the treatment of DPS in accordance with the provisions of the Article 12 of the Regulations of Law No. 29733, Personal Data Protection Law

Obtaining the consent of the DPS owner must be:

1. **Free:** Without error, bad faith, violence or fraud that could affect the demonstration of the owner of the personal data.

   The delivery of gifts or the granting of benefits to the owner of personal data on the occasion of his consent does not affect the condition of freedom he has to grant it, except in the case of minors, in cases in which his consent is admitted, in which consent given through gifts or benefits will not be considered free.

   The conditioning of the provision of a service, or the warning or threat to deny access to benefits or services that normally have unrestricted access, does affect the freedom of the person who grants consent for the processing of their personal data, if the data requested They are not essential for the provision of benefits or services.

2. **Prior:** Prior to the collection of the data or, where applicable, prior to processing other than that for which it was already collected.

3. **Express and Unequivocal:** When the consent has been expressed in conditions that do not admit doubts of its granting. It is considered that express consent was given verbally when the owner expresses it orally in person or through the use of any technology that allows oral dialogue.

   Written consent is considered to be that which is granted by the owner through a document with his or her handwritten signature, fingerprint or any other mechanism authorized by the legal system that remains or can be printed on a paper or similar surface.

   The express condition is not limited to verbal or written manifestation. In a restrictive sense and always in accordance with the provisions of article 7 of this regulation, express consent will be considered to be that which is manifested through the conduct of the owner that shows that he has unequivocally consented, given that otherwise his conduct would necessarily have been another.

   In the case of the digital environment, the consistent manifestation is also considered express in “click”, “click” or “pinch”, “tap”, “touch” or “pad” or other similar.

   In this context, written consent may be granted by electronic signature, by writing that is recorded, in such a way that it can be read and printed, or that by any other established mechanism or procedure allows the owner to be identified and consent obtained, through text. written.

It may also be granted through pre-established text, easily visible, legible and in simple language, which the owner can make his own, or not, through a written, graphic response or by clicking or clicking. The mere conduct of expressing will in any of the ways regulated in this section does not eliminate, nor does it fulfill, the other requirements of consent referring to freedom, opportunity and information.

4. **Informed:** When the owner of the personal data is clearly, expressly and undoubtedly communicated, in simple language, at least of the following:

a) The identity and address or address of the owner of the personal data bank or of the person responsible for the treatment to whom you can contact to revoke consent or exercise your rights.

b) The purpose or purposes of the processing to which your data will be subjected.

c) The identity of those who are or may be its recipients, if applicable.

d) The existence of the personal data bank in which they will be stored, when correspond.

e) The mandatory or optional nature of your responses to the questionnaire that was given to you. propose, when applicable.

f) The consequences of providing your personal data and your refusal to do it.

g) Where applicable, the national and international transfer of data that is carried out.

Anexos

Av. Salaverry 801 - Jesús María, Lima, Peru

Telephone center (01) 315 6600