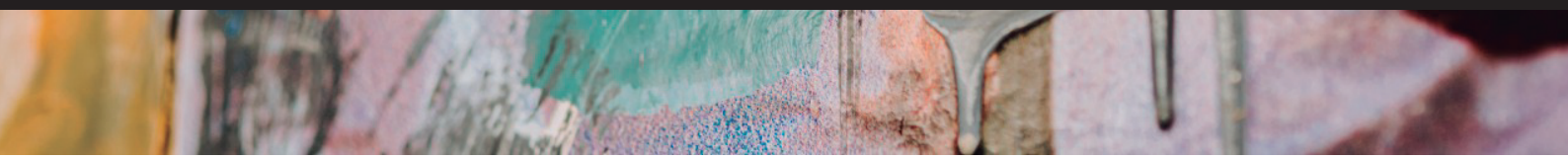


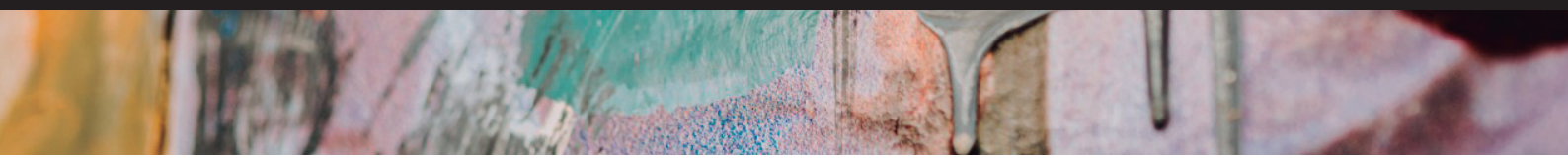
Guide for Healthcare Establishments regarding COVID-19

The Personal Data Protection Directorate has published a "**Guide for Healthcare Establishments**", which details the measures required in order to guarantee the confidentiality of health data of patients diagnosed with COVID-19. This entity ensures the protection of personal data, defined as any information that identifies or enables identifying a **natural person** through reasonably available means.

"Sensitive data" is a subcategory of personal data, which, according to the Law on Protection of Personal Data - Law No. 29733 and its Regulations (the "Law"), is biometric data, on its own, is capable of identifying the holder; data referring to racial and ethnic origin; economic income; information related to physical or mental health, among others. The treatment of sensitive data requires special protection and the holder's prior **express written consent.**

Furthermore, the Law establishes that any person, whether natural or legal entity, who processes personal data must implement certain measures to protect any personal and/or sensitive date to which they have access. Also, the recently published Guide specifically states that every health care facility must establish the following technical and organizational measures in order to ensure the confidentiality, integrity and availability of patients' personal data, as well as to prevent its loss, leakage or unauthorized dissemination:

- **The computer systems used for the processing of personal data must be implement:**
  - Authentication and authorization procedures, including the use of secure login credentials, which must not be shared.
  - Documented procedures: access management, privilege management and periodic verification of assigned privileges, which must be in motion.
  - User interaction logs, such as login, logout and relevant user actions that may include recording, updating and modifying personal data records.
  - Security controls: appropriate for the environments where personal data is processed, stored and handled, such as isolated environments, authorized accesses, fire extinguishers, electrical risks, among others.



- Data backup protocols.

- Data transfer: will proceed with the owner of the personal data's prior authorization, taking security measures to prevent loss of or unauthorized access.

- **Safeguarding of physical documents with personal data:**

  - Lockers, filing cabinets or other facilities where documents containing personal data is stored must be located in restricted areas restricted, where access is protected by a key or other similar item assigned to the entity's personnel.

  - Copies or reproductions of documents containing personal data may only be made by authorized personnel, for example, by assigning a username and password to the printer.

  - Access to documents containing personal data must be limited to authorized personnel, for example, by implementing mechanisms that allow for the identification of the people who have accessed a certain documents, where documents may have been accessed by multiple users.

  - The physical transfer of documents containing personal data should be carried out with measures aimed at preventing access to or manipulation of the information thereby being transferred.

Health facilities that fail to comply with the Law may be charged with the unauthorized processing of personal data, which qualifies as a minor infraction and may incur in a fine of up to S/ 21,500.00; or, processing personal data in contravention of the principles established in the Law or in breach of its other provisions, which qualifies as a serious infraction and may be subject to a fine up to S/ 215,000.00.