GOBIERNO
DE ARAGON
Instituto Aragonés de Ciencias
de la Salud

ARiHSP Information Security Policy

Policy Introduction and Scope

This information Security Policy has been developed by the Health Services and Policy Research (ARiHSP) team led by Enrique Bernal-Delgado to ensure that research based on health data conducted at the Instituto Aragones de Ciencias de la Salud (IACS) ARiHSP group follows appropriate technical and organizational measures to protect individual sensible data against accidental or unlawful destruction or accidental loss, alteration, unauthorized access and/or disclosure.

The security and management procedures in place for data collection, data handling, data storage, data analysis and data destruction are detailed in a System Level Security Policy (SLSP). The SLSP details the lines of accountability within the Instituto Aragones de Ciencias de la Salud (IACS) and, where relevant, the following bodies: regions/countries providing pseudo-anonymised raw data; Aragonesa de Servicios Telematicos (AST) a public law entity that provides IT services to the Government of Aragon; and other stakeholders (ex. IT Companies working in tasks related with data Extraction, Transformation and Loading (ETL).

The ARiHSP collects stores and process information in accordance with applicable laws. This document, together with related SLSP and implementation documents, defines the framework within which information security is managed across the ARiHSP.

Atlas Repository System Details

The repository Atlas of Variations in Medical Practice in the National Health Service (Atlas Repository) lead by IACS has been registered by the Spanish Health Ministry by Resolution of 7th June 2012. Further Information is available at http://www.msssi.gob.es/estadEstudios/estadisticas/sisInfSanSNS/registros/docs/Atlas_VPM.pdf
The Atlas Repository includes the following datasets: Spanish Autonomous Communities Hospital Episode Statistics (HES); Contextual variables (public source, available at the Spanish Health Ministry); Socio-economic variables (public source, available at the Spanish Health Ministry).

Spanish Autonomous Communities Hospital Episode Statistics (HES) Data are collected and made available by a range of external public organisations. Prior to regional/national datasets being transferred, a process of pseudo-anonymization of the raw individual record level data takes place at origin. This process entails erasing any personal information (such as name or other identifiers), censoring or recoding variables (quasi-identifiers) like age from birthdate or postal code from address, finally assigning a fictitious number[1] as independent key (ID) using consistent algorithms across the years of the study, thus preventing the reverse identification of individuals.
Clear data transfer and use protocols (including data encryption prior to transfer) and responsibilities are set up bilaterally with each regional/national partner, making it clear who is responsible before, during transportation, on reception and use of the individual data. To this

[1] Regional/National authorities are the only parties able to link this pseudonymous data to the patient through this key.

end, a number of data transfer & data use agreements establishing specific data protection obligations have been signed.
Datasets are received on encrypted electronic media such as CDs, DVDs or Portable Memory devices. Data is read and transferred to the data server. The electronic medium is kept afterwards in a locked safe at IACS premises and physically destroyed at the end of the project.

According to the data transfer and use agreements signed, when needed, data existing within the VPM Information System is removed by IACS personnel using electronic shredder through a 7-round input random data process (low-level drive formatting) to securely delete the data from the VPM Information System data servers. The physical CD or DVD is disposed through mechanical means (smashing). A certificate of data destruction is delivered.

International projects

IACS ARiHSP research group uses specific data security policy guidance for protecting anonymised research information in the international projects in which it takes part.

Authorised users

Access to aggregated data reports through web application

There is 1 web application (Atlas VPM) deployed on production environment through a public URL available at http://www.atlasvpm.org/login accessible online.
Access permission has been granted to 66 Spanish stakeholders which have all signed a terms of use agreement prior to accessing data through the Atlas VPM web application.
To guarantee statistical confidentiality in small areas, the Atlas Tool detects when the outcome of a query would deliver cells with less than k cases (k ~30). Although used in the analysis, those cells are excluded from the report delivered to the user.

As part of its policy, ARiHSP applies a minimum cell-size requirement for reports to ensure statistical confidentiality and prevent against accidental identification of individuals. When the outcome of a query would deliver cells with less than k cases (k ~30), although used in the analysis (e.g. for risk-adjustment purposes), those cells are truncated to a fixed value (<k) in the report delivered.

Access to truncated aggregated datasets/excerpts underlying manuscript findings

Datasets/excerpts of data underlying the findings reported in a published manuscript can be either publicly available or available upon request. Due to the sensitivity of the Atlas repository, access and view of the data underlying the findings cannot be made publicly available for legal reasons (in particular, the Law 37/2007 on the Public Sector Information Reuse, the Law 14/2007 on Biomedical Research and the Law 15/1999 on Personal Data Protection) as public availability might compromise patient privacy (re-identification risk) and/or third parties restrictions eg. hospital confidentiality. As a consequence, when needed, truncated aggregated data may be accessed upon request throughout a data sharing agreement.