

10 PRIVACY AND DATA SECURITY

PEDSnet believes that the protection of privacy, confidentiality, and data security is essential to the existence and success of research. Equally essential is fostering an environment of trust among patients who are contributing to the data resource, and the entities who are stewards and users of the data. PEDSnet maintains a policy for the protection of patient privacy, data security, confidentiality of health data, and appropriate use of data.

Transparency and Communication

PEDSnet will make its policies and practices on health information open and available for patients and other stakeholders. PEDSnet will clearly communicate with patients, their families, and all other stakeholders about how patient data are used in clinical research, the safeguards undertaken by the network to protect patient privacy and maintain data security, and will seek input from patients and other key stakeholders on how best to engage the PEDSnet community on these issues.

Legal Requirements

Each PEDSnet healthcare organization adheres to all local policies regarding the use of healthcare data. All research practices in PEDSnet comply with current local and national, legal and regulatory requirements. PEDSnet institutions that collect and maintain personal information are subject to the federal Privacy Rule under the Health Insurance Portability and Accountability Act (HIPAA), which requires a description of institutional privacy practices on how the entity collects and maintains personal information, and patients' rights regarding their data.

Use Specification and Minimization

The purposes for which health information are used should be specified at the time of study design (including reference to future use), and only the minimum necessary information for those purposes should be released. Common categories of data that will be made available to data requestors (who have undergone appropriate review and approval mechanisms) include: deidentified, aggregate data; deidentified, individual level results or small populations; non-readily identifiable patient level data ("limited data sets"); and, identifiable patient level data.

Response to Breach

Data provided by PEDSnet must be used only for the purposes specified. If there is a breach of data that risks identification of individual patients, mechanisms for notification as outlined in PEDSnet policies will be activated. The level of action will be low if the risk of invasion of privacy and breach of confidentiality is minimal, and high if the risk of invasion of privacy and breach of confidentiality is significant.

Voluntariness and Local Control

Decisions to participate in specific PEDSnet research projects that involve individual patient-level data will always be made voluntarily by each participating PEDSnet institution. Research using readily identifiable personal information will be done only with the consent of the individual families participating, or in rare cases when an Institutional Review Board decides

that the information is limited and there are safeguards in the study to insure that identifiable information will not be released.

Data Security

PEDSnet adopts best practices for protection of patient data. The Data Coordinating Center implements a broad set of security and reliability controls targeting the Statements on Standards for Attestation Engagements No. 16 (SSAE16), which are widely recognized audit standards that verify the state of internal controls for a data center. Individual PEDSnet institutions implement their own information security policies to safeguard the data that is held locally. The PEDSnet Data Coordinating Center coordinates a significant number of administrative safeguards to minimize the risk of a breach involving protected health information.

