WFH
WORLD FEDERATION OF HEMOPHILIA
FÉDÉRATION MONDIALE DE L'HÉMOPHILIE
FEDERACIÓN MUNDIAL DE HEMOFILIA

WBDR
WFH World Bleeding
Disorders Registry

World Bleeding Disorders Registry

Data Privacy & Security

What is the World Bleeding Disorders Registry (WBDR)?

The WBDR is an online, web-based patient registry. Patients are enrolled through a network of hemophilia treatment centers (HTCs) around the world. The WBDR system includes numerous privacy and security safeguards and minimizes its use and retention of identifying information. Each HTC's data remains separate and the WBDR does not hold any direct identifiers. Data linkage between HTCs is impossible without prior approval by the WBDR and a Data-Sharing Agreement to ensure that appropriate data security and privacy safeguards are in place.

Data Ownership

Patients are enrolled in the WBDR through their HTC. Data about consenting patients is entered prospectively into the WBDR following each clinic visit. The patient data from each HTC is held separately. Each HTC has access to the patient data it collected itself, but by default has no access to data collected by any other HTC. Combined data sets across HTCs can only be generated with the approval of the WFH WBDR Steering Committee.

Data Security

The WBDR uses privacy-preserving record linkage to determine when records from participating hemophilia treatment centers (HTCs) refer to the same person, with a high degree of accuracy.

Cryptographic hashing is the underlying technology that enables the WBDR to minimize patient identifiability while enabling robust linkage. The specific hashing algorithm used is SHA-256, which is applied to a set of immutable properties related to each patient, as described below.

This algorithm provides a one-way function that reliably produces the same output whenever it is given the same input, while also guaranteeing that it is computationally infeasible for anyone to draw inferences about the input data (i.e. each patient's identifying data) based on the output of the hash alone.

In addition, a random string of characters known as a "salt" is added to the patient's immutable properties before hashing. In the unlikely event that the safeguards that the WBDR has put in place to prevent unauthorized access are circumvented, this "salting" technique protects the data further, by preventing the use of a large dictionary of precomputed hash values to attempt to infer the immutable properties of some of the patients with particularly common values. In other words, the WBDR remains secure against even this type of effort to compromise its data.

To explain the process in further detail, for each patient that a given HTC registers in the system, the following steps are taken:

- The HTC seeks the patient's specific consent to be included in the international registry, according to standard procedures throughout the system that have been established in accordance with all relevant laws.

- The HTC collects the patient's date of birth, first name at birth, last name at birth and country of birth.
    - These data are entered in the WBDR, but the WBDR does not store them in its database.
    - The WBDR instead applies a cryptographic hash function to this patient data, which produces one or more cryptographic hash values.
    - The WBDR immediately and securely discards the patient information that was used to generate the hash values.
    - The WBDR then checks whether the hash values match those in any existing patient record, which would indicate that this person has previously been registered in the WBDR, and if so, the system retrieves the relevant record. If no match is found, the WBDR creates a new record for the patient and stores the hash values in it.
    - In either case, the WBDR assigns a new, random identifier to the patient that is specific to the submitting HTC and returns that identifier to the HTC.
    - The HTC assigns the identifier it receives from the WBDR to the data for that patient.

How does the WBDR protect privacy and security?

Although no system can eliminate the risk of misuse, the WBDR was conceived and implemented to minimize the risk of unintended use of patient data. It has also been designed to minimize the potential harm that could result if any breach of its safeguards were ever to occur.

The protections built in to the system include the following:

- The WBDR system is designed and hosted by the Swedish healthcare IT provider Health Solutions AB, whose health data processing services adhere to stringent security and privacy standards:
    - Its RealQ product, which supports the WBDR, is certified as having been registered as compliant with Swedish medical device regulations that implement the European Union's CE marking regulation on medical devices, Directive 93/42/EEC.
    - Its personal information processing practices have also been certified as complying with the United Kingdom's Information Governance Toolkit standard.
    - Its health information processing services are used by Swedish hospitals to hold and process patient data.
- All communication between the WBDR and an HTC occurs over a secure connection which is end-to-end encrypted, using HTTP over SSL (HTTPS), which prevents third parties from intercepting any communication between the two.
- There is no way for any participating HTC to use the WBDR identifiers to link patient data between projects without the cooperation and approval of the WBDR itself. This is a result of the fact that each identifier is HTC-specific, and so they have no inherent relation to one another.
- Because of this, there is also no way for anyone who gains unauthorized access to a participating HTC data to perform an authorized linkage without access to the data in the WBDR repository, which is held and managed separately.
- Because the personal health data used to generate the hash values is not stored, even if a person were

to gain unauthorized access to the WBDR data repository, the system minimizes the risk this person can determine the identity of the patients held in the system. The WBDR incorporates additional safeguards against this risk by using a salted hash algorithm and by applying the hash algorithm to concatenated versions of the input values, rather than on each individual input alone. These measures greatly reduce the risk of re-identification attacks based on large dictionaries of precomputed hash values.

- Access to the WBDR database is restricted to users with either physical access to the premises where the servers are hosted, or with access to a VPN connection that has been set up for Health Solutions.