WEJ Cell & Gene Therapy
Consulting Services, LLC
2640 Ivy Road, Eads, TN 38028
we.janssen@wejcellgenetherapy.com

MANAGEMENT OF CLIENT DATA POLICY

PRECIS

In the course of providing consulting services, it is frequently necessary for WEJ Cell and Gene Therapy Consulting Services, LLC (**WEJCGTCS**) to have access to, and even to temporarily hold in our possession, data that belongs to client organizations. Client data must be treated with respect and attention to its security, including risks of data theft or corruption through hacking, data loss from digital systems failures, disclosure of patient related protected health information residing within the data, or any other form of data breach. Accordingly, WEJCGTCS is promulgating this policy regarding Management of Client Data.

DEFINITION OF TERMS

- *Client data*: Any record that reflects a narrative regarding a client's methods, results, business planning, testing and results, and/or organizational structure, or quantitative data, generally in the form of a spreadsheet or database
- *Data security*: prevention of compromise of data through loss, theft, or damage
- *Data storage location*: the identity of a device or virtual device, such as a cloud location, on which the digital representation of data is physically present
- *RAID*: Redundant Array of Independent Devices – a system whereby data is redundantly stored in exact copies on multiple devices to protect against data loss from the failure of a single device
- *Firewall*: a security device — computer hardware or software — that can help protect a network by filtering traffic and blocking outsiders from gaining unauthorized access to the private data on the network or individual computers
- *Cloud data storage*: a model of computer data storage in which the digital data is stored in logical pools, said to be on "**the cloud**". The physical storage spans multiple servers (sometimes in multiple locations), and the physical environment is typically owned and managed by a hosting company. These cloud storage providers are responsible for keeping the data available and accessible, and the physical environment secured, protected, and running. People and organizations buy or lease storage capacity from the providers to store user, organization, or application data.
- *Possession of Data*: presence of data on a device or cloud location that is in the primary control of a specific individual or organization
- *Digital data* or *electronic data*: data that is maintained on an electronic device, requiring that device or another computational device to become readable by a human
- *Hard copy data*: data that is written or typed on paper or other writing surface in a way that humans can immediately recognize it

POLICY DETAIL

Access to Client Data

Client data that is required in the course of consultations may have different forms, ranging from documents that must simply be read, to un-analyzed raw data obtained from laboratory testing and/or

instrumentation. It is desirable that clients make this data available for consultant access through a secure data storage "room". Examples of Data Rooms may include Sharepoint™, Teams™ or Dropbox™ sites. Provision of access to such storage locations will be considered to be implied by any consulting agreement to which WEJCGTCS is a party, unless such consulting agreement specifically identifies data access arrangements that may or may not be consistent with this paragraph.

Temporary Possession of Client Data

Although it is preferable insofar as practical for WEJCGTCS to access such data directly from the client site, it is frequently desirable or even necessary to make a copy of client data and hold it in a secure storage location that is in the control of WEJCGTCS. Examples of such situations include documents that may need to be marked up as part of a review effort and raw data, such as may exist in a spreadsheet or listmode file, that requires analysis by WEJCGTCS. Unless otherwise stated in a consulting agreement to which WEJCGTCS is a party, permission to make such copies is considered to be implied. All such copies will be wiped from their storage location upon conclusion of any associated consulting agreement.

Storage Locations, Data Transfer, Security Conditions and Indications for Particular Storage Locations

When temporary possession of copies of client data is taken by WEJCGTCS, the specific storage location will be dictated by the specifics of the data involved, giving consideration to the sensitivity of the data, intellectual property content, and the presence of data that has specific legal protections such as private health information (PHI) as defined by the U.S. Health Insurance Portability and Accountability Act (HIPAA) (see also below section on 'Special Circumstances').

The transfer of data between client organizations and WEJCGTCS may be by email attachment, although that is insecure and not preferred. Direct host to host transfer is preferred, and encrypted host to host transfer is most preferred. Transfer on a physical device is also possible, however flash drives, when not encrypted, are insecure and have been known to be vehicles for malware.

Data when held temporarily by WEJCGTCS may reside either on a cloud based host, specifically OneDrive™, or it may be housed on a secure server that is physically located at the office of WEJCGTCS.

Cloud Storage

Most client data that is copied to WEJCGTCS controlled storage will be maintained on the WEJCGTCS cloud storage that employs Microsoft OneDrive™. On client request, clients will be provided access to the Cloud "folder" wherein their data has been copied to, along with any secondary files that may be created through the review and analysis process. Because consultant analysis, including markups of original client documents, are intermediate work products of WEJCGTCS which are critical to final work products, client access for these will be limited to read-only.

On Premise Storage at WEJ Cell and Gene Therapy Consulting Services Offices

WEJCGTS maintains a firewall protected server on company premises. If a client is not comfortable with the cloud storage that is employed for most client data in WEJCGTCS possession, and in particular if client data is particularly sensitive, such as if intellectual property or protected health information is contained therein, this storage may be employed instead of the OneDrive™ location.

The WEJCGTCS server employs “redundant array of independent disks” (RAID) storage technology, wherein all data is maintained in exact duplicate on two physical drives. This provides protection against physical failure of one of the drives. In addition, backup copies of client data are made on portable hard drives that are kept in an independent safe location. The server employs encryption to protect from hacking.

Special Circumstances

Data that is covered by Health Insurance Portability and Accountability Act (HIPAA)

Protected health information (PHI) may be transmitted to WEJCGTCS only if a “business agreement” between the originating entity and WEJCGTCS has been executed. PHI that is transmitted to WEJCGTCS in the absence of a business agreement will be immediately destroyed when it is found to be in WEJCGTCS possession.

When data containing PHI must come into WEJCGTCS possession, it will be kept on the firewall protected on-site server described above.

PHI containing data will be securely destroyed (secure deletion from disk storage, secure paper shredding) within 24 hours of completion of analysis for which it is required.

Financial Responsibility

WEJCGTCS is insured against data loss or compromise, whether due to negligence or outside hostile activity (hacking).

REFERENCES

Data Security Best Practices. White paper available from Netwrix Corporation at https://www.netwrix.com/data_security_best_practices.html

POLICY LIFECYCLE

This policy is effective on the date specified below. The policy may be reviewed and revised at any time, but minimally must be reviewed bi-annually on or before the anniversary of it’s original effective date.

Date	**Event**	**Responsible Party**
01/25/2022	Policy Initiation	William Janssen