European Liver Transplant Registry (ELTR) privacy statement, data and information security policy

The ELTR was created in 1986 with the following objectives:

- Registry of all liver transplantation (LT) procedures in Europe.
- Link between European liver transplant centers.
- Scientific use and publications.

The ELTR is a service of the European Liver and Intestine Transplant Association (ELITA). It therefore, includes the ELITA members who provide data to the ELTR. The ELTR collects data on adult and pediatric LT performed in all of Europe to evaluate the results and outcomes of LT in Europe.

ELTR believes that the greatest attention should be given to handling personal data. Therefore, we process, manage, and protect personal information with the utmost care in compliance with the requirements imposed by the General Data Protection Regulation (GDPR) or in France the “Commission Nationale de l’Informatique et des Libertés” (CNIL). As the supervisory authority for the protection of personal data in France, the CNIL is responsible for ensuring the proper application of the GDPR in France. It is also responsible for assisting public and private entities engaged in their efforts to comply with the regulation.

At all times ELTR respects the privacy aspects defined by the GDPR which came into effect on May 25, 2018. ELTR never provides information allowing the patient or center identification or other data that might lead to the identification of a specific donor or patient, except in a specific case with a commitment to respect the GDPR by the obligation of signing the ELTR DPA with the third party (see paragraph 5). For any questions related to the processing of data by ELTR in the framework of the GDPR, you can send an e-mail to the ELTR DPO (registration N° DPO-95083) Dr. Vincent Karam Vincent.karam-ext@aphp.fr. For detailed information on the General Data Protection Regulation (GDPR) please visit https://gdpr-info.eu or https://www.cnil.fr

1. Purpose of the processing of data:

ELTR processes data exclusively for scientific studies in line with RGPD Article 9.2 (i) and (j) - Article 89 and Recitals 157 and 159, consent being the legal basis of data processing. The basic requirements for the effectiveness of a valid legal consent are defined in Article 7 and specified further in recital 32 of the GDPR. Consent must be freely given, specific, informed, and unambiguous. To obtain freely given consent, it must be given on a voluntary basis. The element “free” implies a real choice by the data subject. An ELTR Patient Information Security Policy and an ELTR Patient Consent Form were created to this purpose.

Data from the centers and Organ Sharing Organizations (OSOs) are aggregated to create a Datawarehouse.

What is an OSO?

The purpose of the OSO is:

- to serve as a common organ exchange organisation and allocation resource for its member hospitals including kidney, liver, heart, lung, pancreas, pancreatic islet, liver cell, composite graft, intestinal and multi-visceral transplantation. This is done transparently, using ethical principles and in full compliance with the national legislation of the members' countries,

- to maintain and operate a common waiting list for transplantation,
- to ensure complete traceability from organ donors to patients,
- to maintain and operate follow-up registries of transplanted patients,
- to maintain and operate follow-up registries of living donors,
- to serve as a collaborative platform through specialized working groups and advisory groups to facilitate best practice recommendations and policies optimizing retrieval, allocation, and transplantation of organs, and
- to form a collaborative network for the member hospitals to promote research and development related to organ donation, allocation, and transplantation.

All patients waiting for an organ transplantation in the country (or group of countries) are listed on one common list for each organ. The OSO ensures that all necessary data are available for the transplant professionals to allocate the organs according to rules and monitors compliance with these rules. The OSO is also used as the link between the transplantation community in a country (or group of countries) and the rest of the world.

How are data used?

Data are analyzed to produce 5 semi-annual reports containing more than 750 statistical figures and tables:

- Overall data analysis booklet
- Last 15 years data analysis booklet
- Adult data analysis booklet
- Pediatric data analysis booklet
- Living donor data analysis booklet

The entire 5 booklets are made available to the contributing centers in a space of the ELTR Server that is password protected. Centers' identification is necessary for ELTR to allow centers the editing and referral to clinical records when necessary, to resolve any inconsistencies that are detected during data entry or the statistical analyses. It is also necessary for the communication and exchange of information between the ELTR and its community members. In addition to the 5 booklets, each center receives confidentially the analysis of its data allowing an audit of its experience when compared to the rest of Europe.

Data privacy needs to point out the fact that centers' benchmark is not performed in ELTR studies. ELTR scientific committee considers this task as reserved to national health authorities via their OSOs. Nevertheless, the center's effect is evaluated in ELTR studies by assessing cutoffs of centers' volume of a given condition that significantly impacts the outcomes. Outcome data are considered as major data since most routine ELTR figures and thematic studies require the calculation of graft and patient survival rates. These are determined by actuarial methods and the statistical significance is determined by the log-rank test to compare survival curves. Regression methods are also used to identify risk factors associated with LT.

These studies minimize the potential biases, by assessing interactions between confounding factors and identification of independent predictors among all the ELTR variables that can have an impact on the liver graft and/or patient outcome. With its dynamic model of European collaboration, ELTR has helped develop risk models for graft loss and mortality following LT. Owing to the large cohort of patients, the exhaustiveness, the quality and security of the data, and the long-term follow-up provided by the ELTR, the results are representative of LT in Europe and provide valuable information to the clinicians, the health stakeholders, and the patients. There is of course heterogeneity in the policies in the 32 contributing countries. The ELTR data summarizes the results as a whole and represents a kind of freeze-frame rather than a generalized statement for Europe. At the same time, the ELTR remains the unique entity capable of providing such statistics, capable of giving a global snapshot of the European experience and helping to identify important trends that may guide further practice. The updated list of ELTR publications is available at the link.

2. Data collection

In 2021, 174 centers from 32 countries contribute to ELTR. This encompasses all their patients receiving LT for the treatment of end-stage liver disease (ESLD). The registered data is estimated to more than 97% of the overall European LT experience and are regularly updated. There are two sources of ELTR data provision:

- 76% of data (68% of centers) are shared by the main Organ Sharing Organizations (OSOs) (i) national OSOs: the French ABM, the Spanish ONT/RETH, the United Kingdom-Ireland NHSBT and the Dutch NTS) and (ii) international OSOs: Eurotransplant and Scandiatransplant. Beforehand, a harmonization of OSOs' metadata was conducted and put in place with each of the OSOs to allow a transfer of data compatible with ELTR. At each biannual ELTR update, OSOs data are overwritten and ELTR retains a maximum of two previous versions of the data batch in its archives, i.e., with every new transfer of data the data transferred one year before being deleted. The backup of the two previous versions is kept in case we need them for quality control purposes.

- 24 % of data are directly entered into the ELTR platform by the concerned 37 centers.

ELTR does not store data for any longer than is necessary for the purpose for which they are being processed or to fulfill legal requirements or the registry's scientific needs.

Whether for OSOs or centers entering data directly into the ELTR platform, ELTR has no contact with patients. Patients are intended to have been asked by their physician/center to express their consent for the use of their data for scientific research or exchange of their data for the same purpose with official partners of whom ELTR is a part.

The ELTR questionnaire includes data on indications for LT, donors and recipients characteristics, technical aspects of LT and type of graft (reduced, split, domino, alive or deceased donors), perioperative data, initial and maintenance regimen of immunosuppression, graft and patient outcomes (morbidity and mortality), and cause of death or graft failure. ELTR also collects data on living liver donors. A full list of ELTR data forms is available in electronic format. The ELTR data dictionary and ELTR dataset specifications describe the structure of the database. This is updated whenever a revised data collection form is produced and whenever coding changes or database modifications are made.

The ELTR has developed an online application (Electronic Data Capture – EDC) for collecting data https://eltr.fmdata.fr/eltr-form. A Web-based module was developed with FileMaker Server 19.1.2 technology (https://www.claris.com) to allow for real-time data entry and analysis. Registered users are requested authentication before access is granted to the system by providing a confidential login and password. Software, questionnaires, validation routines, and statistics are located on a central server, which can be accessed by the participating centers with a standard internet browser. No center has access to data from other centers.

3. How do we process personal data?

ELTR processes the personal data in compliance with the GDPR and its derogations applied to scientific registries (Article 9.2 (i) and (j) - Article 89 and Recitals 157 and 159). Personal data is defined as any details that could disclose information about an identified or identifiable natural person. The information we collect is exclusively used for scientific research. We receive personal data of patients and donors from transplant centers and OSOs involved in the process of organ donation and transplantation.

ELTR's protected data includes health information about individual transplant patients, considered as sensible data. We use personal information under these terms and conditions. As part of the

ELTR data quality control procedures, ELTR has made available in the platform to each center, with protected access, a dynamic list of patients with missing data to allow their identification for completion. No center has access to data from other centers.

4. Security compliance policy:

The purpose is the description of steps taken to ensure physical, operational, and technological security of the data collected by ELTR.

ELTR ensures that appropriate technical and organizational measures are in place to prevent the misuse, loss, or unlawful processing of personal data. This means that personal data is encrypted and sent via a secure connection. The 2 ELTR employees (Data Manager & Biostatistician) and the server hosting company who have access to ELTR data are bound by a confidentiality clause. All of them only have access to data if it is necessary for the performance of their duties.

Security measures: Measures put in place to ensure the security of all collected information include the following:

Physical Security

- restricted access to the Paul Brousse Hospital, ELTR office requiring access code.
- paper forms are in locked storage cupboards when archived.
- network data is stored on physically secure and separate servers with protective firewalls.
- access keys, codes, cards, and passwords are controlled by defined and enforced security procedures.

Operational Security

- users as part of their employment contract agree to the privacy and confidentially standards.
- procedures are in place for employees leaving the ELTR for logins, password, and pass cards, etc. to be canceled.
- passwords are changed regularly and must maintain a level of strength to reduce hacks or reproduction.

Technical Security

- validation of data is performed to ensure integrity and accuracy.
- business continuity is regularly audited and updated.
- system software and licenses are maintained, ensuring certification, authenticity, security, anti-theft, and anti-virus needs are functioning and up to date.

Data Transfer Security

- email guidelines are in place for the transfer of information; lists maintained; encryption and enforced security engaged for transmitting information.

Disposal and destruction

- Physical records are destroyed using the Paul Brousse hospital's secure destructive service.
- Computer records are kept indefinitely, and hardware physically wiped and destroyed when decommissioned.

Data Security Breaches

- An audit trail tool exists to track all user activities in accessing the database and entering data. All user activities can be reviewed in the event of a data security breach.
- An error log is produced that records all potential attempts at fraudulent access to the database and other access errors. This error log is reviewed regularly by the ELTR to detect potential security risks.
- All security breaches and near misses must be reported to the ELTR and dealt with in line with GDPR (see paragraph 8).

5. Who do we share raw data with?

ELTR does not share raw data with third parties without the agreement of the ELTR/ELITA scientific board members. There are two situations where raw data are shared with third parties:

- Registry's studies that use only available data: in that case centers are anonymized.

- Registry's studies that need to request to centers supplementary data necessary to conduct the study: in this case, the centers' ID is provided to the study leader who takes care of the survey by contacting centers and collecting the required supplementary data.

In any situation, third parties must be from an ELTR contributing center. In case third parties submit a proposal to perform a registry study, the ELTR/ELITA board examines the project according to the regulations for the ELITA /ELTR studies and carefully select eligible parties. Thus, ELTR/ELITA and the study leader conclude a Data Processing Agreement (DPA) in which the party is obliged to keep ELTR data confidential and to only process data on behalf of ELTR/ELITA, for the authorized purpose and in compliance with GDPR.

6. Privacy Policies

The purpose is to describe the consent process for data collection and how the privacy of patient information collected by ELTR is ensured.

- Patients are intended to have been entitled by their center and/or OSO to view the information the ELTR holds about them, and request alterations if the data is thought to be inaccurate.
- Only the patient first 3 letters of the names are required in ELTR (a few of the 24% of centers who enter data directly into the ELTR platform enter this information) are not included in the locked analysis data set that is used for reporting and data extraction.
- All ELTR staff are required to sign a confidentiality agreement, confirming that data will only be accessed for purposes related to their work within the ELTR and that identifiable data will only be accessed when essential.
- All ELTR staff are required to be familiar with and act under GDPR.
- All ELTR published reports present summary data only in tabular or graphic format.
- ELTR does not release data identifiable by patient name.
- All data linkage projects with raw data must adhere to GDPR standards that protect patient privacy.
- At the time of data collection, each center is asked to certify that they have complied with measures under the relevant privacy measures.

7. Platform technical specifications

ELTR has developed the platform with FileMaker Server 19.1.2 deployed with WebDirect. The location includes a dedicated server located in a professional hosting company OVHcloud in a data center, with complete duplication of another server and site, from the Registrar of the domain name to the database. The server is protected vis-a-vis external intrusion by a firewall. Monitoring, maintenance, and security updates to this server are carried out by the hosting company. The accommodation center meets the standards of "Carrier Class" in terms of secure power, air conditioning, security anti-fire, access security.
OVHcloud holds the ISO27001 certification in Information Security Management Standards (ISMS) and many other certifications of the very highest security standards including HDS.

ELTR ensures the administration of the server by remote management via a tool type "Terminal server". The transfer of files is done by An FTP protocol. ELTR has available also a reboot remote type APC via the internet.

The technical characteristics of the server:

- Linux Ubuntu 18.04
- 2 vCores
- 7 Go RAM
- 50 Go
- 250 Mb/s
- Backup FTP 100 Go

Finally, an external backup system is carried out on another server in the hosting company:

- 4HS - 1 backup every 4 hours between 08:00 and 20:00 (backups kept: 4)
- HBD - 1 weekly backup every Monday at 04:00 (backups kept: 4)
- FMS - 1 backup per day at 00:00 (backups kept: 7)
- Automatic 7-day rolling server snapshots at 06:00

The weekly backups are transferred via FTP according to the same frequency on a workstation dedicated to ELTR and on an external independent hard disk.

The Web browser or user workstation is any computer with access to the internet that connects to the ELTR platform.

The server is the heart of the application: it contains all the programs, databases, and tools needed for the operation of the application. Each action of the user workstation leads to a query and a response from this server through the FileMaker platform.

The login and password required for the study are transmitted by email. This procedure allows users to be protected by the internal password of their electronic mail. Logs of user activities, logs of FileMaker platform (internal FileMaker servers), web server, and logs of FileMaker program are frequently monitored by the ELTR team.

External audit of ELTR security

At the ELTR request, an audit of the ELTR database security was carried out by Atos Digital Security on July 2021. The following no-exhaustive list of examinations has been performed on the application:

□ Information gathering related to the application’s infrastructure;
□ Analysis of the application’s platform;
□ Account takeover attempts;
□ Cross-Site-Scripting (XSS) injections;
□ SQL injections;
□ Sensitive and technical information leakage;
□ Application crawling;
□ Authentication mechanism analysis and session management control;
□…

The security audit on the targeted perimeter showed a **satisfying security level.**
The application showed qualities in its state-of-the-art cryptography, ensuring the integrity of the communications. Additionally, an anti-brute force mechanism is preventing attackers to send multiple login requests targeting one specific account by locking it after a few failed attempts. Also, it has been noted that generic error messages were displayed on the login forms on failed authentication attempts. This behavior prevents an attacker from testing if an account exists.

8. Data breach

GDPR defines a “personal data breach” in Article 4(12) as: “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.”.

The ELTR uses the EU Guidelines on Personal data breach notification under Regulation 2016/679 (wp250rev.01) as a reference document. The importance of being able to identify a breach, to assess the risk to individuals, and then notify if required, is emphasized in Recital 87 of the GDPR. The ELTR always considered it vital to implement appropriate technical and organizational measures to prevent such incidents. Thus, ELTR data security governance (equipment, design, and operating procedures) was set up to enable timely detection of eventual cybersecurity events that can threaten data since the ELTR platform is regularly monitored by:

- the ELTR team (2 full-time employees) visits the platform almost daily to verify the data and checks the users' connection log from time to time. The periodically standard ELTR statistical reports and the very frequently realization of ELTR/ELITA studies also allows verifying if any data anomalies would be related to misuse, or a system failure or violation.
- the centers regularly connect to their space and can alert the ELTR if they notice an anomaly in the system or their data.

ELTR's protected data includes information about individual transplant patients, considered as personal health information. But this information is difficult to identify because, in addition to strong preventive access security measures including data encryption, the records are pseudo-anonymized. However, if that occurs, and it is likely that the breach poses a risk to an individual’s rights and freedoms, in accordance with Article 33(1), Article 34 and Recitals (85) to (88) of the GDPR, the ELTR will notify the supervisory authority (CNIL) and all concerned data providers, without undue delay, and at the latest within 72 hours after having become aware of the breach.

The ELTR team is prepared to respond when a data breach is detected. We Mapped out a Data Breach Protocol (BDP) we are aware of what to do in the event of a data breach, per see, do a thorough investigation to fully understand what happened, how it happened, what data is affected, and what needs to be done to prevent similar incidents from happening in the future.

We can recover data since at each biannual ELTR update, OSOs datasets are overwritten and ELTR retains a maximum of two previous versions of the data batch in its secured archives. We can also recover systems and services that were stolen or destroyed in a data breach. We have therefore a recovery plan and test and improve it regularly.