Ordered and Secured

To start with, personal medical data is private and strictly protected. However, progress cannot be made in medicine without human data. The solution is a data management software program that provides security and only grants access to authorised material.

“REMS is an access management tool that, where necessary, prevents the illegal use of data.”

CSC, the Finnish ELIXIR node, develops and maintains the open source REMS tool that can be used to manage access to datasets containing confidential material. REMS (Resource Entitlement Management System) is an access management tool that, where necessary, prevents the illegal use of data. With the REMS tool, it is possible to order a specific file from a large amount of data and have it delivered to the ordering party locked in a secure manner.

“There may be various tools within an organisation handling similar things. Although there are many ready-made tools and services available for identity and role management, I have not heard of any other general resource entitlement software like REMS”, says the REMS tool’s product owner Tommi Jalkanen from CSC.

ELIXIR AAI: a federation of 200 organisations

REMS is part of a federated system formed by the ELIXIR community comprising nearly 200 organisations. Becoming a federation has required agreements between the different organisations regarding information security, personal data law, rights and

Data on the human genome should be treated with the utmost care and complying with information security protocols. In order to ensure information security, ELIXIR provides a service in which researchers log into a system that identifies their electronic identity while also distributing access rights to the biomedical data stored in the cloud. In this way, the researcher creates a secure analysis environment for the data to be analysed. This is made possible by the REMS tool.

ELIXIR strictly adheres to the EU law on information security. When researchers utilise data, the REMS tool can be used to ensure that the shared data is subject to authorisation.
ELIXIR AAI (Authentication and Authorisation Infrastructure) is a federation of user identities and access rights. First, get an ELIXIR identity. Second, apply for software, storage and compute, and data access authorisation if the data resource is protected. Your service and data access authorisation is stored and travels with your electronic identity relying on REMS service. With this attribute attached to your electronic identity, you can open a database or start a virtual machine. Permission is granted by the service provider.

The ELIXIR compute platform provides a seamless workflow for users: the researchers may use their electronic identity to securely create a scientific software analysis environment, and gain access to large sensitive biological data resources stored on a cloud. The platform also helps research groups to create scalable services.
obligations. This has resulted in ELIXIR’s own trust network, ELIXIR AAI, the rules of which each member organisation has committed themselves to follow.

In practice, ELIXIR AAI is a community that uses federated authentication and identity management. This federation has been developed based on the trust network of Finnish universities and research institutes (HAKA). The ELIXIR federation enables Single Sign-On (SSO) to joint services.

ELIXIR’s member organisations maintain basic user information that shows the role of the user in addition to the name and contact details. Determining the role is important because the REMS tool distributes access rights based on it. That is to say, REMS decides what kind of a view opens for the user in the service on the basis of personal details. This is so-called entitlement-based REMS.

Despite the high level of information security, REMS is still easy to use. No separate sign-on is required to use the tool. Logging in to the service is done with the user name and password of the ELIXIR home organisation. No service-specific user name/password pair is required. It is this federated management that ensures the use of data resources can be monitored. At the same time, it is possible to ensure that the materials are not used for wrongful purposes. The use of the service can be monitored and reported.

The way the service works is that a researcher applies for permission to use the data with the REMS tool. The researcher logs in to REMS with their federated identity and then fills in an application for data use and agrees to comply with the terms of use. ELIXIR’s Data Access Committee (DAC) receives the application through REMS and approves or prohibits the use of the data. The applicant is notified of this by e-mail. If approval is granted, the applicant is provided with instructions on what happens next. REMS directs the data request to CSC’s Data Access Service. It provides the researcher with a view of the entitled data in the ePouta cloud service.

A federated user ID can be easily closed by the responsible organisation if the user switches workplaces, for example. The use of strong identification facilitates traceability and reporting. Fumbling with user name/password pairs is also reduced, as are password resets. Single sign-on reduces the need for separate user IDs and saves time, effort and money. Overlapping data management is reduced and data quality is improved. The service owner can focus on the service as the data administration of the ELIXIR organisation manages the IDs. These new practices support, for example, the use of ELIXIR’s many software services.

Interface support for utilities

A new feature of the REMS software is a programming interface support for utility programs. A modern and widely-used web technology that enables the joint use of services, such as databases, is now available for researchers. This makes it possible to easily and safely build ecosystems and grant third-party access to the service. REST (Representational State Transfer) is a well-known and frequently used application architecture for decentralised systems. The REST interface allows different software programs from different platforms to use the same resource.

“Creating an all-encompassing interface is currently in the works, providing extensive opportunities for the building of third-party utilities”, says Tommi Jalkanen.

“A modern and widely-used web technology that enables the joint use of services, such as databases, is now available for researchers “
Why monitoring access rights is important

Using statistical methods, it is possible to identify a person with sufficient probability from anonymised material if genomic information is available on the subject. Therefore, this issue must be approached through information security, the usage agreements of the service providing genomic data as well as national and international legislation.

If the anonymised material is linked with additional information, such as year of birth or the name of the disease, the researcher must be reliably authenticated in the service and accept the service’s terms of use, which prohibit the identification of the persons included in the materials. It is also possible to profile users, in which case each profile can be provided with an appropriate view of the material. The access rights and legislation define how the materials should be, for example, stored and analysed.

Ari Turunen