“We trust FileSender’s built in zero-knowledge encryption for sending files via the internet”

In order to keep all internal and external processes of Amsterdam University Medical Center (UMC) running smoothly, employees of the care, education and research departments regularly send files to internal and external users. It is essential that the exchange process takes place in a safe and responsible manner. After testing out several options, Amsterdam UMC chose FileSender as their preferred service for sending files via the Internet.

“Like many institutions, we started using FTP to send and receive files,” says IT Security Officer Ewald Beekman of Amsterdam UMC. “But this method is cumbersome and confusing to users. In addition to having to create accounts manually, we had to share FTP information with other institutions. We then switched to Accellion, a cloud service whose user experience is superficially similar to FileSender. But this service did not meet our expectations either, so around 2011 we switched to FileSender, the cloud service for sending files, which we still use today.”

Necessary end-to-end encryption

Because FileSender uses an identity federation to handle logins, users within Amsterdam UMC can use their institutional account to access the service. The federation does this by referring login attempts to the employee directory systems kept at the Human Resources department instead of issuing separate accounts for every connected service. As an additional benefit, this means that unprovisioning is automatic too: as soon as someone leaves the company, that person can no longer log on to FileSender. Amsterdam UMC uses the FileSender instance of SURF, a cooperative association of Dutch educational and research institutions in the field of information and communication technology that considers information security of paramount importance.

"For sending information classified at low confidentiality levels, online services such as WeTransfer and Dropbox are permitted within Amsterdam UMC. But if a transfer involves confidential data, such as patient medical data, employees must use FileSender because of the necessary end-to-end encryption."

- Ewald Beekman

FileSender is a native web application and that includes the encryption functionality. The end user only needs a web browser to securely transfer files. Using a (strong) password of their own choosing, the encryption of the files takes place in the browser. At the time of sending, the files are already encrypted. The recipient receives an email with the link to the download. To actually open the received file, a password is required, which employees are not allowed to share via email for security reasons. To send the required password, they can use secure instant messaging apps such as Threema, Signal or iMessage.

Receiving confidential files doesn't require a login. But in those cases where external parties need to send confidential files to Amsterdam UMC and don't have login access to the FileSender service, a voucher mechanism comes to the rescue. An Amsterdam UMC employee needing to receive confidential files then sends a voucher to the sending party. The voucher, which is valid for two months, allows the sending organization to send files at the same security level on a one-time basis. A voucher is further restricted in that someone uploading on a voucher may only send their file transfer to a recipient inside the Amsterdam UMC organisation.

SURF commissions an audit of their FileSender instance each year by an independent party. Every year, the auditor looks at one of three aspects: quality of the program code, robustness against hacks, and security of the design and architecture. SURF shares the results of each audit with organizations that use FileSender. "This annual audit indicates that FileSender is a solid service. We are able to use it with confidence," concludes Ewald Beekman.