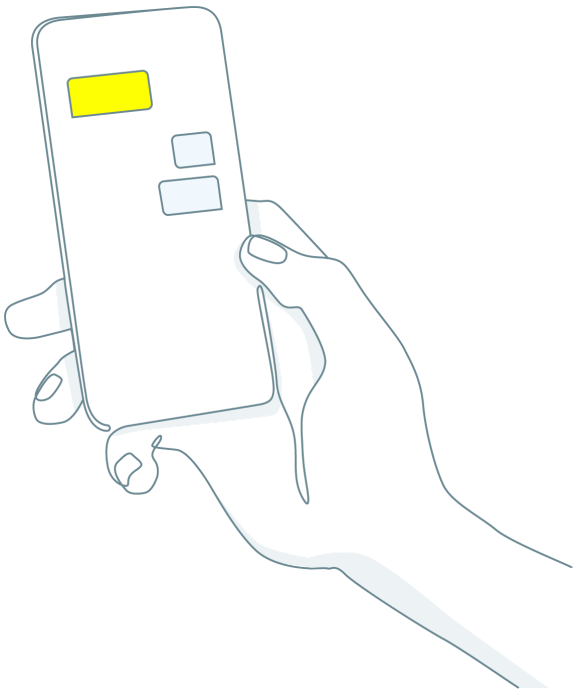
Data Protection Impact Assessment

Version 2.1



Author: Joost Bruggeman, Arvind Rao, Paul Willems, Jordi van Duyne
Audience: Patients and their families, healthcare professionals, IT professionals, data protection professionals and authorities, Siilo users, Siilo customers
Keywords: GDPR, General Data Protection Regulation, DPIA, Data Protection Impact Assessment, sensitive information, security, privacy, transparency
Purpose: This document explains how Siilo protects the data of users and messages which are sent by our users. This document can be used as input for Data Protection Impact Assessments (DPIA's) of our customers and users.
Abstract: The most important determinant to safeguard privacy and security in software platforms such as Siilo messenger, is company culture. For instance, how well does a company adopt to feedback from user-, privacy- and security communities, how is that feedback is invited and how transparent a company is about that feedback. This document is aimed to demonstrate this, and describes what (personal) data is shared and gathered on/ by Siilo, what privacy- and security risks are involved, and what can be done to safeguard that data.
Our request to you, our reader: we would like to invite you to share your opinion on what we collect, how we collect it, and how we process and protect the information from these sources. We also hope that the language and explanations offered in this document are accessible for everybody with interest in our DPIA document. If this is not the case, or you have other questions or feedback for us, please send us an email at privacy@siilo.com and kindly include "DPIA" in the subject header.
Important note: this is a 'living' document. It is continually edited and updated, just like Wikipedia articles.
Revision History:

Revision	Date	Initiator	Nature of Change
1.0	10-12-2018	-	Initial version
1.1	13-03-2020	Paul Willems & Jordi van Duyne	Actualisation of chapter 3: Siilo Sub-processors
2.0	22-04-2020	Jasper Aarts & Jordi van Duyne	Added detailed overview of sub-processors
2.1	06-07-2020	Jordi van Duyne	Added Siilo Connect specifications

Contents

1.0 Introduction

This Data Protection Impact Assessment (DPIA) is part of Siilo's commitment to our users and their patients, as well as Siilo's (future) customers, to help them understand how Siilo is handling personal data in relation to the General Data Protection (GDPR).

The GDPR considers healthcare-related data particularly private. Under the GDPR, healthcare professionals must give their patient information sharing habits serious consideration. This includes not only the kind of programs to use on their smartphones, but also their behaviour with regards to the sharing of patient information.

There is a mounting pressure on the clinical workforce today and the quality of their decision-making depends on the quality and efficiency of information that flows between healthcare teams. Today, healthcare professionals all over the world aggregate patient information on their mobile devices in order to provide patients with the best care possible. In fact, multiple physician-led studies have demonstrated that clinical decision making can be faster, more efficient and of a higher quality when messenger apps on smartphones are used in clinical communication. The concept of privacy is indeed a strong consideration in the minds of medical professionals, but it can sometimes become overshadowed by the pursuit for optimal patient care.

In this document, we undertake a detailed analysis of how Siilo processes personal data, the associated risk involved and how we ensure these risks are avoided, minimized and properly managed. For the technical details regarding our cryptography and other security measures, please read our security white papers. For the medicolegal details on how messenger apps should be used in healthcare, please read our legal white papers which are available to you in the resources section of our website www.siilo.com.

1.1 Responsibility and medical legislation

Before sharing any content with colleagues via their smartphone, the steps usually taken by healthcare professionals is to completely anonymize patient information. Although this might appear as a logical and standardized approach, it can, in fact, conflict with certain medical laws that are aimed primarily to protect patients. For example, if incomplete patient information leads to care team confusion and improper treatment, patient care and safety could be jeopardized. Therefore, in the interest of patient safety, information sharing and professional diagnoses should never be given anonymously within care teams. Depending on the patient's condition and their treatment relationship with their medical professional, a signed document of informed consent to share information should be considered; the sharing professional must use this relationship as a guide when it comes to patient consent issues. Siilo has published several legal white papers on the website to aid professionals in this decision-making process. The content of these papers addresses how professionals should approach the concept of GDPR, taking into consideration their country-specific medical legislation, when using clinical communication messenger applications. However, it will always remain the responsibility of individual healthcare professionals to adhere to their own personal code of practice, as well as their organization's internal policies on this.

As the provider of an app that contains sensitive patient data, Siilo understands the importance of safeguarding and processing information on behalf of its users. In order to ensure secure data protection, the handling of sensitive data should be clearly defined in a processor agreement that is signed by every user of the app. In this agreement, the provider of the app should be defined as the "Processor," and the user as the "Controller" of patient information. In Siilo's case, Siilo Holding B.V. is the Processor of the message data that our users are sending to each other.

1.3 Message data vs. user data

Siilo distinguishes between two types of data:

- **Message data:** this refers to data which is sent by our users to each other. As healthcare professionals are the main users of the Siilo app, it is largely anticipated that our users will be transferring sensitive information and personal data regarding the health of patients (data subjects). Put simply, Siilo is a Processor for message data; our users are the Controller of message data.
- **User data:** this refers to the personal data of users that Siilo must collect in order to have a secure and compliant functioning of the Siilo app. Siilo is a Controller for user data; our users are the data subjects.

As with every organization, Siilo also processes information about its customers, employees, suppliers and partners. However, these sources of information fall outside the scope of this document, but can be accessed via email at privacy@siilo.com

1.4 Siilo's network features

Healthcare has become far too complex for siloed medical networks to exist; an ageing and multi-morbid patient is likely to receive treatments from multiple specialists from multiple organizations across multiple lines of care. Further developments include, high volume-low complex care beingly increasingly moved out of hospitals and delivered closer to the home of patients. Developments like these illustrate the fact that siloed professional structures can be potentially counter-productive. Siilo recognizes that the 21st century is the new era of 'network medicine' where eventually patients will be able to define and control their own medical network. This new era sees a development of consumer networking tools that allow users to make connections, whilst simultaneously maintaining privacy and professional distance. To help this transition in delivering efficient cross-disciplinary, transmural care, Siilo facilitates GDPR-compliant medical professional networking (i.e. "making connections") for the benefit of patient care. On Siilo you can have:

- **1st-degree connections;**
- **2nd-degree connections;**
- **Siilo Network connections, and;**
- **organisation directory connections.**

1st-degree connections are connections based on phone number matching, connections based on a common group chat, and connections from accepted chat- and connection requests. Users can find their 1st-degree contacts listed on the Chats tab. All users on Siilo will be able to access their 1st-degree contacts unless they have failed verification.

2nd-degree connections are the colleagues who are connected to a user's 1st-degree connections. Only verified users can find 2nd-degree connections listed in the "People You May Know" feature on the Spaces tab under "My Networks" [Symbol] "Siilo Network." The list of 2nd degree connections is limited to 8 professionals and these were selected on how often a connection was connected to a 1st-degree connection.

Siilo Network connections are all colleagues on Siilo who were verified as a medical professional and did not opt-out to be in the Siilo directory. Users can find the "Siilo Network" on the Spaces tab under "My Networks." The search functionality on that tab can be used to connect with other verified medical professionals. Only verified medical professionals will be able to search the Siilo Network unless they request to opt-out via the Siilo Service Desk chat. When they opt-out, they cannot search the network of verified professionals on Siilo, nor can they be found by other verified colleagues on Siilo.

Organisation directory connections are all part of the same organisation as defined by a Siilo Connect customer. Regardless of verification status, users can search and contact their organization directory connections. The organisation directory can be found on the Spaces tab under "My Networks" [Symbol] "Organisation name." It is the organization that curates the organisation directory connections via a manual process or an automated process (e.g. connection via an integration with their local directory access protocol).

1.5 Reading

In the following chapters, we provide a comprehensive explanation of our data processing procedures, then we describe the risks that are involved with processing this information and our methods to finding solutions to such issues, in the context of a constantly changing world filled with security risks.

2.0 Collected (personal) data

2.1 Message data

It is of the utmost importance and cannot be emphasised strongly enough: message data which is shared in healthcare teams should never become available to anyone who isn't directly involved in delivering optimal care for the relevant patient.

Due to the nature of Siilo's encryption protocols, employees -or anybody else- are never able to understand what information is shared, nor why it is shared. Therefore, Siilo only focuses on the process of how it is shared and develops the app in such a way that this sharing is done as securely as possible without imposing friction to the user.

Message data enters Siilo on smartphones of healthcare professionals via:

- the phone's camera app,
- another communication app on the phone (messenger apps, email apps);
- Siilo's web application on a tablet, laptop or desktop;
- a message from another Siilo user, or;
- Siilo's dedicated camera app (Android) or long-press functionality (iOS).

Once the information is in the Siilo app, the most important default settings are:

- information will never be automatically shared with other apps (e.g. photos will never end up on a camera roll) and servers (e.g. iCloud, Google Cloud or Dropbox);
- all information is specifically excluded from iCloud/Android automated backed-ups
- messages are deleted automatically after 30 days.

Any deviation from these default settings can only be achieved deliberately by the user.
For example, a user may choose to download messages from the web app onto a computer or may select messages/conversations to be kept longer than 30 days. Another example could be if a healthcare organisation purchased an integration of Siilo messenger with their electronic patient files; a professional can then select messages to be exported into the patient file for record keeping. Information can get out of the app via the following routes:

- via the download functionality in Siilo's web app;
- via the export functionality in Siilo's mobile app;
- via a secure custom-built integration with on premise servers of healthcare institutions; or
- via taking screenshots or snapping pictures of phones that have the app open.

2.2 User data

The legitimate interest of collecting and processing personal data is necessary for the performance and compliance of contract. Before a user installs the Siilo app on their smartphone, the License Agreement, which includes the Data Protection Agreement, is agreed by the user through clicking the link that is sent to their email address during registration for the app.

One crucial element to safeguard the exchange of patient information in a professional setting, is to ensure that the intended receiver of the information is indeed the party with whom you intended to share the information with. After all, if a healthcare professional signs up on a messenger platform to discuss actual patients, and names herself as "ZDoggMD", how can one be certain that the person behind that name is indeed Dr. Zoe Domani?

Siilo believes that its users' identities should undergo thorough checks and verification procedures. This ensures that other users on the platform can have peace of mind when sharing information with one another. In order to give professionals this peace of mind, they can clearly see the verification status of their contacts on their avatar. The 4 statuses are:

1. unverified;
2. verified identity;
3. verified registered medical professional, and;
4. verification failed.

The users will be able to quickly see the verification status of their colleagues on Siilo with the following badges:

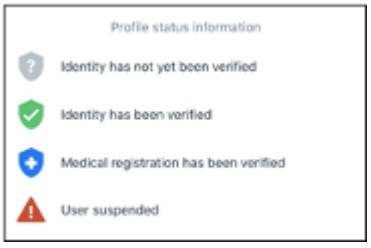


Figure 1 *Verification badges that are visible on users' avatars and profiles.*

In order to become verified, Siilo users are asked to provide personal data during the registration process, as well as by the Service Desk chat in the app. This personal data is then sent to Siilo's servers securely via the mobile app. Please see the table below for all the personal data a Siilo user is asked for:

Information	Reason for processing	Retention
Names (first, last)	Relevant for verification, establish peer trust	Immediate deletion after ending license agreement.
Phone number	Relevant to establish connections on the Siilo platform and relevant to contact users for further product improvement	Immediate deletion after ending license agreement.
Email address(es)	Relevant to send link with end user and processor agreements, relevant for part of the verification process, relevant to identify users as part of a customer's organization, relevant to contact users for further product improvement	Immediate deletion after ending license agreement.
Medical registration number	Relevant for verification, establish peer trust (optional)	Immediate deletion after ending license agreement.
Avatar picture	Relevant for peer to peer trust (optional)	Immediate deletion after ending license agreement.

Medical profession	Relevant for verification, establish peer trust (mandatory)	Immediate deletion after ending license agreement.
Title(s)	Relevant for peer to peer trust (optional)	Immediate deletion after ending license agreement.
Specialization(s)	Relevant for peer to peer trust (optional)	Immediate deletion after ending license agreement.
Interest(s)	Relevant for peer to peer trust (optional)	Immediate deletion after ending license agreement.
Organisation/ association	Relevant for peer to peer trust (optional)	Immediate deletion after ending license agreement.
Phone contacts telephone numbers	Relevant to immediately establish connections on the Siilo platform (optional)	Immediate deletion after ending license agreement.
Findable group name, group description	Relevant to establish connections on the Siilo platform (optional)	Immediate deletion after ending license agreement.
Copy of medical ID, driver's license or passport	Relevant for verification, establish peer trust (optional)	Immediate deletion after verification.
Organisation specific profile fields	Relevant to the members of a specific organisation on Siilo	Immediate deletion after ending license agreement.

Table 1 *Personal data that Siilo users consciously fill out as part of the registration flow, filling out their professional profile or setting up a public, findable group on Siilo.*

Due to the nature of messaging software, Siilo collects, or needs to collect the following personal data, listed in the table below. This data is essential for proper functioning of the Siilo app:

Information	Reason for processing	Retention
Number of connections on Siilo	Relevant to receive information on how to get started with Siilo	Immediate deletion after ending license agreement.
Device information: user IP address mobile device type operating system version of the app language of the device push destination Touch-ID enabled Face-ID enabled	Relevant to development process, and understand bugs in the software and how to fix them	Immediate deletion after ending license agreement.

WhatsApp installed **Adobe Acrobat installed**	Relevant for certain functionalities in Siilo such as invites via WhatsApp and viewing PDF files on the mobile device	Immediate deletion after ending license agreement.
Number of groups	Relevant to understand level of engagement on Siilo for Siilo customers	Immediate deletion after ending license agreement.
Organisational role	Relevant for privileges in the Siilo.Connect environment	Immediate deletion after ending license agreement.
How many messages sent/ received	Relevant to understand level of engagement on Siilo for Siilo customers	Immediate deletion after ending license agreement.
How many and which days online (past 30 d)	Relevant to understand level of engagement on Siilo for Siilo customers	Immediate deletion after ending license agreement.
Web app activation and current sessions	Relevant to understand level of engagement on Siilo for Siilo customers	Immediate deletion after ending license agreement.

Table 2 *Personal data about Siilo users that is obtained from users by using the app.*

In order to improve and understand the Siilo product, as well as providing a greater Siilo user experience, Siilo employees may need to access and process automated meta-data which is also referred to as user 'profiling.' Siilo ensures that user profiling is solely carried out as a necessary requirement to improve operations, and this is reflected through the way meta-data is accessed; currently, Siilo developers must either write code in order to gain access to this information, or members of the Siilo verification and management team must go through a "break the glass procedure" (See Chapter 5 for an explanation of this procedure) in order to access meta-data that is listed below:

Information	Reason for processing	Retention
Which user chats with user, at what time exactly	This information is the by-product of a messenger platform	Immediate deletion after ending license agreement.
Time and duration of VoIP/ video calls	This information is created on any asynchronous messenger platform	Immediate deletion after ending license agreement.
Message size	This information is created on any asynchronous messenger platform	Immediate deletion after ending license agreement.
Which groups are active	This information is created on any asynchronous messenger platform that allows for group conversations	Immediate deletion after ending license agreement.

Group names of private groups	This information is created on any asynchronous messenger platform where group chats can be given a name	Immediate deletion after ending license agreement.
Members of groups	This information is created on any asynchronous messenger platform that allows for group conversations between multiple users	Immediate deletion after ending license agreement.

Table 3 *Personal data that Siilo processes to be able to send a message from one user to another.*

3.0 Siilo sub-processors

Due to the design of the Siilo messenger software, Siilo utilises certain pieces of software which are licensed to Siilo by other providers. These providers are referred to as sub-processors because parts of Siilo users' information interacts with their software. For example: when a Siilo user signs up for the app, an SMS is sent to the phone number of that user to verify that phone number. Siilo has not developed its own SMS verification service but uses software from another provider to do this. Thus, that provider processes a Siilo user's phone number on behalf of Siilo. Siilo has contractual Data Protection Agreements with all sub-processors. Monitoring of the security and the performance of sub-processors is part of the information security management system (ISMS) policies of our ISO-27001 certification.

Sub processor	Amazon Web Services
General	Siilo's server infrastructure is hosted by Amazon.
Where is the data hosted?	All messaging related activities are in Amazon's Frankfurt data centers. For services such as the email verification (Amazon Simple Email Service), and website content security policy logging (Amazon Lambda), those services are only offered in the Ireland datacenter. In summary, all data is hosted within the EU and the vast majority of it is located in Frankfurt. However, the emails exchanged with Siilo users go through the Ireland data center.
Which data is processed?	Processed by Amazon AWS: - email addresses and email content - user profile data - encrypted message data - message meta data (pseudomised) - request meta data
More info	https://aws.amazon.com/compliance/gdpr-center/ https://aws.amazon.com/privacy/

Sub processor	Twilio
General	Twilio is used in some cases to send SMS messages. Also, Twilio is used to provide Siilo's in-app VOIP (calling via internet) and video call functionality. The contents of your calls are end-to-end encrypted (DTLS/SRTP). If necessary due to firewalls, Twilio works by first determining which of their servers is best positioned between the caller and recipient to act as a blind relay via a mechanism known as TURN.
Where is the data hosted?	https://www.twilio.com/docs/video/ip-address-whitelisting
Which data is processed?	- phone numbers - sms content - in-app voice/video call meta data
More info	https://www.twilio.com/legal/privacy

Sub processor	CM.com
General	As part of the Siilo registration flow, users are asked to provide their phone number. This phone number is integral to contact discovery for new users. As part of Siilo's policy on verifying information, we use CM as an SMS provider to send an SMS to the user with a code which they input to confirm that they indeed have access to the device connected to that number. The service providers engaged by CM are:, Unbounce, LinkedIn Insights and Google Analytics.
Where is the data hosted?	The datacenter is located in the Netherlands.
Which data is processed?	- phone numbers - sms content
More info	https://www.cm.com/about-cm/security-compliance/ https://legal.cmtelecom.com/en/cm-online-bv/privacy-policy

Sub processor	Firebase
General	Firebase is used by Siilo for Analytics and Crash reporting in the iOS and Android Mobile applications, Push notifications for the Android application and Dynamic links for non-users. User data is sent fully anonymized and does not include personal identifiable data such as phone numbers, emails, names. Users can opt out of the analytics service during the registration of the app.
Where is the data hosted?	Google datacenters: https://www.google.com/about/datacenters/locations/index.html
Which data is processed?	No personal identifiable data Firebase Crash Reporting: - Instance IDs - Crash traces Crashlytics: - Installation UUID - IP Addresses Firebase Cloud Messaging - Instance IDs Firebase Dynamic Links: - Device specs (iOS)
More info	https://firebase.google.com/support/privacy

Sub processor	ZenDesk
General	Siilo is a largely user-focused organisation that improves its software primarily in response to user input. Siilo users have several ways to provide user feedback, such as via the Siilo messenger app, but also of course through either Siilo's contact form on www.siilo.com or the following email address: info@siilo.com. Due to the high volume of these interactions, Siilo has a ticketing system, using a software called ZenDesk, to keep track of employee-user communication exchanges.
Where is the data hosted?	Zendesk has datacenters in three main regions — United States, Asia Pacific, and the European Union. Service Data may be stored in any region.
Which data is processed?	Names, email addresses, phone numbers
More info	https://www.zendesk.nl/company/customers-partners/privacy-policy/

Sub processor	Adjust.com
General	Adjust is the industry leader in mobile measurement and fraud prevention. Siilo uses Adjust for making it possible to know which link users used to download the app.
Where is the data hosted?	Adjust is located in Germany. In some cases they transfer data outside the European Union. This is done on the basis of statutory contractual provisions that are intended to ensure an adequate protection level of your data. And, they comply with the EU-U.S. Privacy Shield Framework.
Which data is processed?	Hashed IP addresses, mobile identifiers
More info	https://www.adjust.com/terms/privacy-policy/

Sub processor	Salesforce
General	Information that is entered in the contact form on the website is processed in Salesforce. We use Salesforce to correctly and efficiently respond to requests from (potential) customers.
Where is the data hosted?	Frankfurt, GER / Paris, FRA
Which data is processed?	Names, email addresses, organization name, characteristics and needs
More info	https://www.salesforce.com/company/privacy/

Sub processor	Zapier
General	Information that is entered in the contact form on the website is processed and routed by Zapier to different end-points.
Where is the data hosted?	United States
Which data is processed?	Names, email addresses, organization name, characteristics and needs
More info	https://zapier.com/privacy

Sub processor	Mailchimp
General	The time and privacy of Siilo users is important to us and as such we minimize the emails that we send to our users. However, there are times when critical information needs to be shared. Examples of this include: privacy law changes (GDPR), informing users of a potential security incident (should one be suspected), or an important change in Siilo policies. Occasionally we will ask for information of (some of) our users in order to make further product improvements. In these cases, Siilo uses an email provider called Mailchimp to handle the logistics of sending out emails.
Where is the data hosted?	Mailchimp is US based and part of the Privacy Shield framework.
Which data is processed?	Names, email addresses
More info	https://mailchimp.com/legal/privacy/

Sub processor	Google Analytics
General	Google Analytics is used by Siilo in order to acquire a greater understanding of visitors and users of https://www.siilo.com and https://web.siilo.com/. Further still, the use of analytics is essential to continually improve visitor and user experience. The data sent to Google only reflects user behavior and does not include personally identifiable data. Google Analytics uses opt-out by installing a browser add-on. On www.siilo.com users can use opt in through the Cookie consent dialog.
Where is the data hosted?	Google datacenters: https://www.google.com/about/datacenters/locations/index.html
Which data is processed?	No personal identifiable data
More info	https://www.google.com/analytics/terms/us.html

Sub processor	Google Optimize
General	Google Optimize is used by Siilo in order to execute A/B tests on the website. With this information Siilo can learn what works best for our visitors. The data sent to Google only reflects user behavior and does not include personally identifiable data. Google Optimize is built on Google Analytics, so the same data is processed.
Where is the data hosted?	Google datacenters: https://www.google.com/about/datacenters/locations/index.html
Which data is processed?	Data from Google Analytics
More info	https://optimize.google.com/optimize/home/#/accounts

Sub processor	Links in the app: Itunes.apple.com (iOS only) Play.google.com (Android only) Youtube.com Map.google.com
General	Within the app helpful links are provided. They are hosted by third parties; however, their use within Siilo is 100% at the discretion of the user. No application features depend on/nor send data to these websites.
Where is the data hosted?	Not applicable
Which data is processed?	No application features depend on/nor send data to these websites.
More info	

4.0 Identification of security and privacy risks

This chapter summarizes our security and privacy risks. In the next chapter we have described how we manage these risks.

4.1 Message data

The lifecycle of message data shared between healthcare professionals via a communication or messenger app on smartphones is separated into two main phases. The shared (patient) information can be:

- in transit, i.e. when the information travels from one device to another, and;
- at rest, i.e. when the information is not in transit.

In contrast to what the term "at rest" suggests, often information that was received or created on a phone, is rarely ever "at rest." The default behaviour of today's apps is to synchronize with other apps and cloud services. An image shared via WhatsApp, for instance, automatically syncs to a user's camera app on that device, which is then usually synchronized with cloud services. The same is true for text messages on WhatsApp: all this sensitive content is automatically backed-up on the iCloud or Google cloud services. Because most consumer apps follow this pattern, it means that when using these types of messengers, personal (patient) data leaks beyond the control of professionals or the organisations they work for. In addition, the exchanged information is not deleted by default and therefore will accumulate in endless amounts across several locations and devices. This lack of control makes the use of BYOD smartphones and consumer social media applications not compliant with law and regulations (e.g. GDPR) because personal data, containing sensitive medical information, will certainly leak to third parties that are not involved in the care of patients.
This chapter aims to describe the potential security risks involved in these two phases, as well as the privacy risks involved if security is compromised. They are summarised in the table below:

Information	Security risks	Privacy risks
Data in transit	• man-in-the-middle attack • compromised company servers • rogue employee • accidental bug in software • socially engineered attack • replay attack	• access to unstructured, encrypted data on patients treated by all professionals on Siilo that have not yet been deleted from the server • access to (un)encrypted information of patients on 1 single professional's device (mobile, tablet, desktop) • metadata of Siilo messages: sender, receiver, time, size of message • information identified as profile information pertaining to Siilo users • access to a network of professionals who can be lured into sharing information about patients
Data at rest	• physical access to professional's phone • compromised company servers • rogue employee • compromised user phone • socially engineered attack • ignorant usage of export functionalities of Siilo by a user	

Table 4 *Security and privacy risks of message data*

If an individual's phone is accessed without authorization, an attacker may be able to read messages associated with this single user. Due to the default deletion process, such an attack would yield limited, unstructured and small amounts of information. However, if an account is completely hijacked by an attacker, specific information may be retrieved which is exacerbated by the fact colleagues are unaware this account has been compromised. This is known as a socially-engineered attack, or more specifically, phishing. If the Siilo servers were to be accessed without authorization, where information and meta-data for many Siilo users are stored, this information is protected due to encryption.

4.2 User data

User information is valuable to an attacker for various reasons: the information could be sold for marketing or soliciting purposes or could even be used to launch socially engineered attacks to other systems, including Siilo. The table below summarizes the security risks involved with regards to Siilo user information and the associated privacy risks:

Information	Security risks	Privacy risks
User data	• compromised company servers • rogue employee / Siilo.Connect admin • accidental bug in software • socially engineered attack	• personal information of healthcare professionals is obtained for soliciting, marketing, etc. • that personal information is used for a socially engineered attack to obtain patient information

Table 5 *Security and privacy risks of user data*

5.0 Description of solutions

In this chapter, we detail the technical and organizational control measures Siilo has implemented to minimize the potential risks that were identified in the previous chapter.

5.1 Organisational and administrative policies and controls

Siilo has implemented an information security management system (ISMS) and Siilo is certified against ISO27001 and NEN7510 (Dutch standard for managing information security in healthcare). As part of the ISMS, Siilo has implemented several organisational and administrative policies and controls such as periodic and standard risk assessments, internal audits, an information security policy, a least privilege policy, training of staff, a (security) incident management procedure and a data breach notification procedure. The objective of Siilo's ISMS is to enable further improvement of the organization, staff and its products.

Every solution that Siilo implements goes through a risk assessment and data protection impact assessment. It follows a strict process safeguarded by our ISMS policies demonstrated by our ISO-27001 and NEN7510 certificates. Siilo has appointed an independent Security Officer and Data Protection Officer who is registered with the Dutch Data Protection Authority.

Development process

Siilo's development process employs several strategies to ensure both the quality as well as the security of data:
(1) Unit tests: for every feature we develop a set of basic tests which exercise that feature in isolation;
(2) Peer code review: changes to the app are reviewed by at least two developers before acceptance into a beta release. For features which impact security or privacy-related tasks, those new lines of software code are reviewed by a senior developer from outside of the team and the senior developer interacts with the security officer and privacy officer before releasing the new feature(s) to the messenger.
(3) Manual testing and limited public beta: prior to release, features are released internally for manual testing and are often also released to a select pool of "friendly beta testers." This approach is used to screen device-specific features, as well as any features which may only emerge after being exposed to a diverse set of work flows.

Least privilege

Privileges are provided to Siilo staff on a strict need-to-have basis. This is monitored and checked annually by a security officer. Any Siilo employee who needs access to information outside of their allocated role, must first log the request with our standard template.
These requests are logged and authorized by the Data Protection Officer if a request is deemed compliant with the General Data Protection Regulation prior to its fulfilment. These requests are also reviewed once per quarter by the Siilo ISO-27001 committee comprised of the Data Protection Officer, and Siilo's Chief Executive Officer and/or the Chief Financial Officer.

5.2 Technical policies and controls

Message data – data in transit

To understand the solutions to mitigate the risks for data in transit, please read our security white paper (https://www.siilo.com/resources/security-white-paper) as it describes in detail our security-by-design approach, the threat model and cryptographic protocols.
In short, Siilo uses end-to-end encryption implemented with the NaCl crypto library https://nacl.cr.yp.to/ This means that each message between sender and receiver (Alice and Bob in Figure 2) is protected via a public/private keypair. Only

Alice and Bob are able to decrypt and read the messages they exchange, and the authenticity of any message can be empirically verified. Third parties, including Siilo company and its employees are never able to read them.

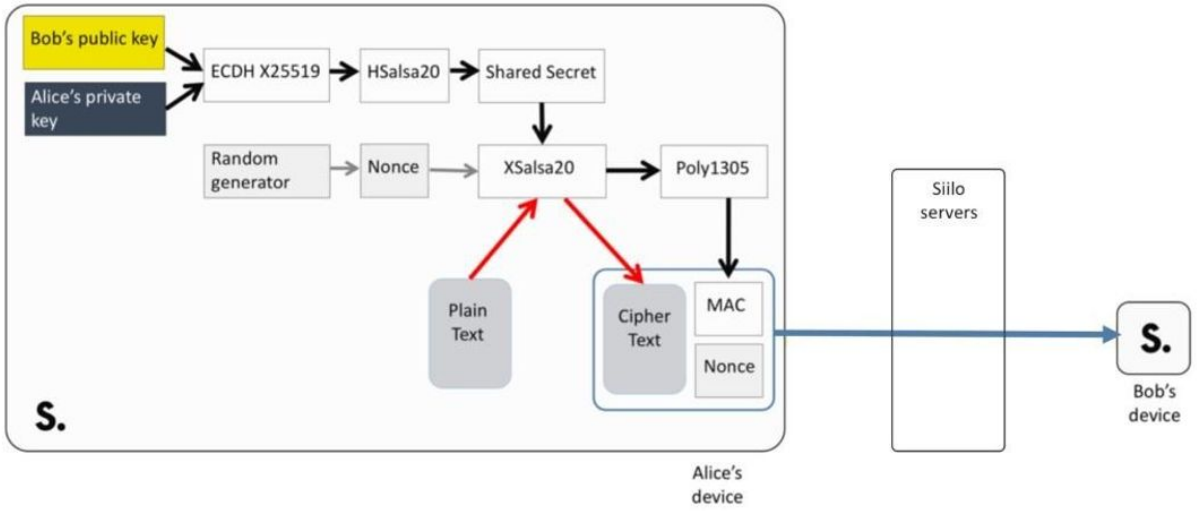


Figure 2 *Schematic of the encryption protocol between Alice's Siilo app and Bob's Siilo app.*

Siilo uses certificate pinning to prevent so-called "man-in-the-middle" attacks, a process whereby attackers access the traffic between the phones and try to break in and tap the communication lines to read the messages. Standard TLS v1.2 communications require a valid SSL certificate that was issued from a trusted certificate authority, recognized by the device. Certificate pinning goes further and mandates that those certificates must be only issued from a chain of trust rooted to a specified issuer. This closes a litany of vulnerabilities arising from the key distribution problems associated with the internet's certificate authority infrastructure.

Siilo's encryption enforces the notion of "public-key authenticators," a term coined by researchers. This property allows the application to mathematically prove that the message came from one of the two parties (sender/receiver). However, this process is not secure enough due to the nature of social engineering attacks in which people use similar names or profile photos to phish sensitive information from a prospective target. A mechanism which can prevent this type of attack is known as the out of band verification. Siilo supports this process by allowing users to go to their profile and to see their unique ID called a "Key fingerprint." Two users can exchange these IDs; ideally in person, and thus ensure that they are indeed who they claim to be.

Message data – data at rest on user device

For data at rest on the device (iPhone, iPad, Android) the following safeguards are in place:

- All "key material" also known as the codes used by the cryptograph are stored in the iOS KeyChain or the Android KeyStore as appropriate;
- All "key material" is encrypted by a "master key" that is derived from the pin code chosen by the user;
- The entire database is encrypted using SQLiteCipher. All messages, message metadata, and contact information are stored in this manner;
- All received media is stored encrypted by the single use, symmetric encryption key. This key is accessed via the database mentioned above;
- An application level pin code mechanism prevents access by humans that have physical access to the device. This addresses most forms of in-person social engineering such as asking to borrow the phone for a quick call, etc.
- All exchanged information in the Siilo app is automatically deleted after 30 days. Users can decide for themselves to delete individual messages on an ad hoc basis if they deem 30 days too long. We have consciously not included

count-down timers and message lifespans such as seconds/ hours as we believe it will create a sense of urgency resulting in screenshots and other unwanted behavior at the receiving end;
- When a user knows his/her device is lost, stolen or otherwise compromised, he/she can alert its organization (this is a Siilo Connect feature) and a Siilo Connect Admin can remotely wipe the Siilo data off the device.

Message data – data at rest on Siilo servers

For data at rest on Siilo servers the following safeguards are in place:

- All Siilo servers are located within the European Union with the highest security- and compliance norms;
- Firewall rules prevent network access to the databases (MySQL and ElasticSearch) and is restricted to a subnet containing Siilo's servers and a VPN, which a limited subset of Siilo employees are able to access;
- The MySQL database is password protected and encrypted industry standard AES-256 and stores messaging data, messaging metadata, Siilo Connect configuration data, and user profile data;
- ElasticSearch encrypts specific fields such as email and phone numbers to enable matching. Other profile fields which are shown in the app as "public" to Siilo members are stored in plain text;
- All media (sent via the application and thus considered sensitive) is stored and encrypted by the single use, symmetric encryption key. That key is not stored on any Siilo server except as part of the encrypted message data stored in MySQL. The keys to decrypt that data are only available on the devices of the sender and recipient.

Storage of personal data on Siilo servers

Message data is stored at servers in Frankfurt (Germany) and for backup purposes, daily automated 'snapshots' are taken that are stored for no more than 7 days. These snapshots are encrypted at rest.

Siilo's server infrastructure is hosted by Amazon, Inc. Siilo has purposefully chosen Amazon Web Services (AWS) as they employ the highest security and encryption standards and ensure (GDPR) compliance with their SOC level I-II-III, ISO9001, ISO27001, ISO27017, and ISO27018 certifications.

User data

User data is stored at servers in Dublin (Ireland) and is backed up daily and stored for no longer than 30 days in a preconfigured bucket that is encrypted at rest. Siilo user data is treated with the following security measures with regards to the personal information we gather from our users:

Information	Security measures
Names (first, last)	Not encrypted in Siilo database, safeguarded by ISMS policies
Phone number	Encrypted in the Siilo database and safeguarded by ISMS policies
Email address(es)	Encrypted in the Siilo database and safeguarded by ISMS policies
Medical registration number	Encrypted in the Siilo database and safeguarded by ISMS policies

Avatar picture	Not encrypted in Siilo database, safeguarded by ISMS policies
Medical profession	Not encrypted in Siilo database, safeguarded by ISMS policies
Title(s)	Not encrypted in Siilo database, safeguarded by ISMS policies
Specialization(s)	Not encrypted in Siilo database, safeguarded by ISMS policies
Interest(s)	Not encrypted in Siilo database, safeguarded by ISMS policies
Organisation/ association	Not encrypted in Siilo database, safeguarded by ISMS policies
Phone contacts telephone numbers	Encrypted in the Siilo database and safeguarded by ISMS policies
Findable group name, group description	Not encrypted in Siilo database, safeguarded by internal company policies
Photograph of medical ID, driver's license or passport	Encrypted in the Siilo database and safeguarded by ISMS policies. Also, after a Siilo Service Desk employee has seen the photograph, it is manually deleted from the database. Currently Siilo is implementing an automated process for this

Table 6 *Security measures of user data provided by user*

Information	Security measures
Number of contacts	Not encrypted in Siilo database, safeguarded by ISMS policies
Device information: user IP address mobile device type operating system version of the app language of the device push destination WhatsApp installed Adobe Acrobat installed Touch-ID enabled Face-ID enabled	Not encrypted in Siilo database, safeguarded by ISMS policies
Number of groups	Not encrypted in Siilo database, safeguarded by ISMS policies

Organisational role	Not encrypted in Siilo database, safeguarded by ISMS policies
How many messages sent/ received	Not encrypted in Siilo database, safeguarded by ISMS policies
How many and which days online (past 30 d)	Not encrypted in Siilo database, safeguarded by ISMS policies
Web app activation and current sessions	Not encrypted in Siilo database, safeguarded by ISMS policies

Table 7 *Security measures of user data collected by Siilo*

Information	Security measures
Who chats with whom, at what time exactly	Not encrypted in Siilo database, safeguarded by ISMS policies
Time and duration of VoIP/ video calls	Not encrypted in Siilo database, safeguarded by ISMS policies
Message size	Not encrypted in Siilo database, safeguarded by ISMS policies
Which groups are active	Not encrypted in Siilo database, safeguarded by ISMS policies
Group names of private groups	Not encrypted in Siilo database, safeguarded by ISMS policies
Composition of groups	Not encrypted in Siilo database, safeguarded by ISMS policies

Table 8 *Security measures of user data collected by Siilo to enable transfer of message data*

Phone number matching on Siilo

Siilo optionally lets the user discover other Siilo contacts by cross-referencing with the phone's address book. If the user chooses to do so, the following information is uploaded through an encrypted TLS connection to the server:
(1) First 64bits of the SHA1 hash of the E.164 normalized form of each phone number found in the phone's address book
(2) Key: EEDAAC207FC6BA08727C
(3) Only the phone numbers are hashed and cross-referenced. Siilo does not touch associated names, email address(es) and other information the phone's address book holds. The Siilo server then compares the list of hashes from the user with the known phone hashes of current Siilo users. The server will only match against current Siilo users, and after returning the matches to the mobile client, the server immediately discards the submitted hashes.

6.0 Siilo Connect

Healthcare organisations can organise their members onto Siilo in single, and sometimes multiple networks. To enable organisations to do so, Siilo has developed a member management tool. Siilo Connect is the name of the web-tool for our customers. The customer decides on who operates that web-tool (the Siilo Connect Admin).

With this product, organisations can securely on-board their members via any of the supported matching criteria that is known to them, and with which the Siilo user has registered on the platform, such as;

- entire email address, e.g. "t.smith@examplehospital.com"
- email domain, e.g. "@examplehospital.com"
- telephone number
- well-established medical registration IDs

Organisations that are unaware of this kind of information can also on-board their members via QR code scanning or via the Siilo Service desk chat. The latter option requires users to provide a unique phrase they have received from their organisation. When sending this phrase to the Siilo Service desk, they are automatically added to that organisation on Siilo.

Siilo Connect customers will first have to know an email address or phone number with which a Siilo user is registered on the platform or will do so in the future. This will match those Siilo users with their organisation members. The only Siilo user information they will obtain, are:

- the names of the Siilo user that belongs to their organisation on Siilo;
- the email address or phone number a Siilo user has used to sign up for the app (which they know already).

Siilo will never share the personal information of Siilo users with other Siilo customers. However, Siilo Connect can allow customers to add profile fields to their organisation-specific profile on Siilo. If they choose to do so, they can introduce profile fields such as “phone number,” “email address” or “medical license number.” It is the Siilo user’s own decision to fill this out as it is not mandatory to fill anything out on the profile page (opt-in).

When in an organisation, users will be able to see each other’s organisation-specific profile. Outsiders will not see this profile information unless the organisation wishes to. An organisation can also include profile information that is hidden for all users, organisation members themselves included (e.g. membership identifiers).

At the organisational level, Siilo Connect customers will have access to usage information, specifically:

- number of members online per day;
- number of groups online per day;
- number of messages sent per day;
- number of total (un)registrations per day.

These statistics are not traceable to individual users. To prevent reverse engineering of these numbers, by adding/removing single or groups of users in an attempt to understand more about them, they are fixed historically. Also, when users are added/ removed from their organisation, they will receive a push notification from the Siilo Service Desk that this has happened.

Within Siilo Connect, the user has the possibility to adjust data by themselves. Siilo Connect Admins can change the following information:

Information	Changeable for Siilo Connect Admin[1]
Organization name	Yes
Organization logo	Yes
Name and description of an organisation Service Desk chat	Yes
Name and descriptions of organisation groups	Yes
User's internal name for internal identification	Yes
Organization specific profile fields	Yes
User's personal information (Table 1)	No
Log activities	No

Table 9 *Changeable data by Siilo Connect Admin*

Siilo Connect Admins cannot change name, job title or any other personal information. See Table 2 for an overview of all personal data that Siilo users consciously fill out as part of the registration flow. Siilo Connect Admins don't have access to any logged events.

[1] Changeable: The organisation and Siilo are joint-controllers of this personal data. Not changeable: For this personal data the organisation is the Controller.

7.0 The continuous process of security

Security is often perceived as a desired end state, achieved ultimately through encryption. But security is not just about encryption protocols. It is a continuous process, a culture, a mindset. The risk of an outsider attacking Siilo software is entirely different, yet equally important, to internal risks that may arise, and cannot be solved simply by encryption but instead by the values instilled in company culture.

A company culture is the set of customs, traditions and values of the people within that organisation. A company's culture can be observed from certain parameters such as adoption of feedback from user and security communities, the process of how critical feedback is received and processed and how transparent a company is regarding its feedback. Siilo believes it demonstrates a part of its culture by:

- communication such as this data protection impact assessment document;
- its ISO27001 and NEN7510 certification, about its information security management;
- its (bi)annual audits and penetration tests by esteemed external security experts;
- its training of staff on a regular base
- making Siilo's source code available to professionals with an interest in investigating the code.

What would we like from you?

In this document Siilo has implemented many organizational, administrative and technical controls to reduce potential risks and to offer you a secure product and messaging service.
We expect from you, as a user, that you handle personal data with the same care as we do. We would like to emphasise the importance of keeping your Siilo pin code confidential and to never share it with others.

Do you want more information about Siilo, its security or privacy policies? Do you have suggestions to improve this document or our app? Please contact us at privacy@siilo.com.