xund

Medical API Privacy

This white paper provides a brief overview of our privacy by design architecture and the security and privacy measures we apply to patient data.

Introduction

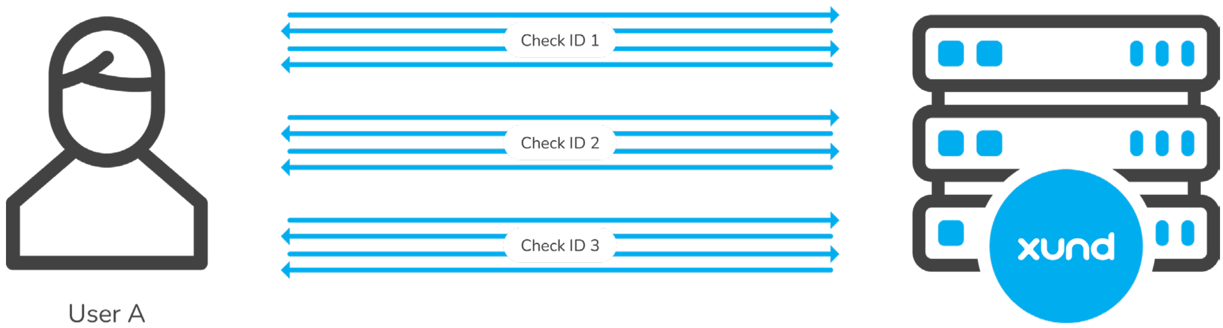
Awareness and regulation around the handling of personal data have significantly increased over the past decade. Multiple breaches and leaks have highlighted practices where companies have harvested vast quantities of personal data to analyze for their own profit. While there are innovations that rely on the use of personal data, too often, there is a lack of measures to minimize the use of personal data and practices incorporating privacy by design. At XUND, we aim to foster innovation and maximize the support our software can provide while limiting the collection of personal data and minimizing the possible privacy risk. We put emphasis on ensuring that we comply with privacy regulations at the highest level and incorporate privacy by design into our development processes.

This white paper provides a brief overview of our privacy by design architecture and the security and privacy measures we apply to end user data. For further information, please refer to our Data Processing Addendum, the Privacy Policy, and our Technical and Organizational Measures (TOMs) document.

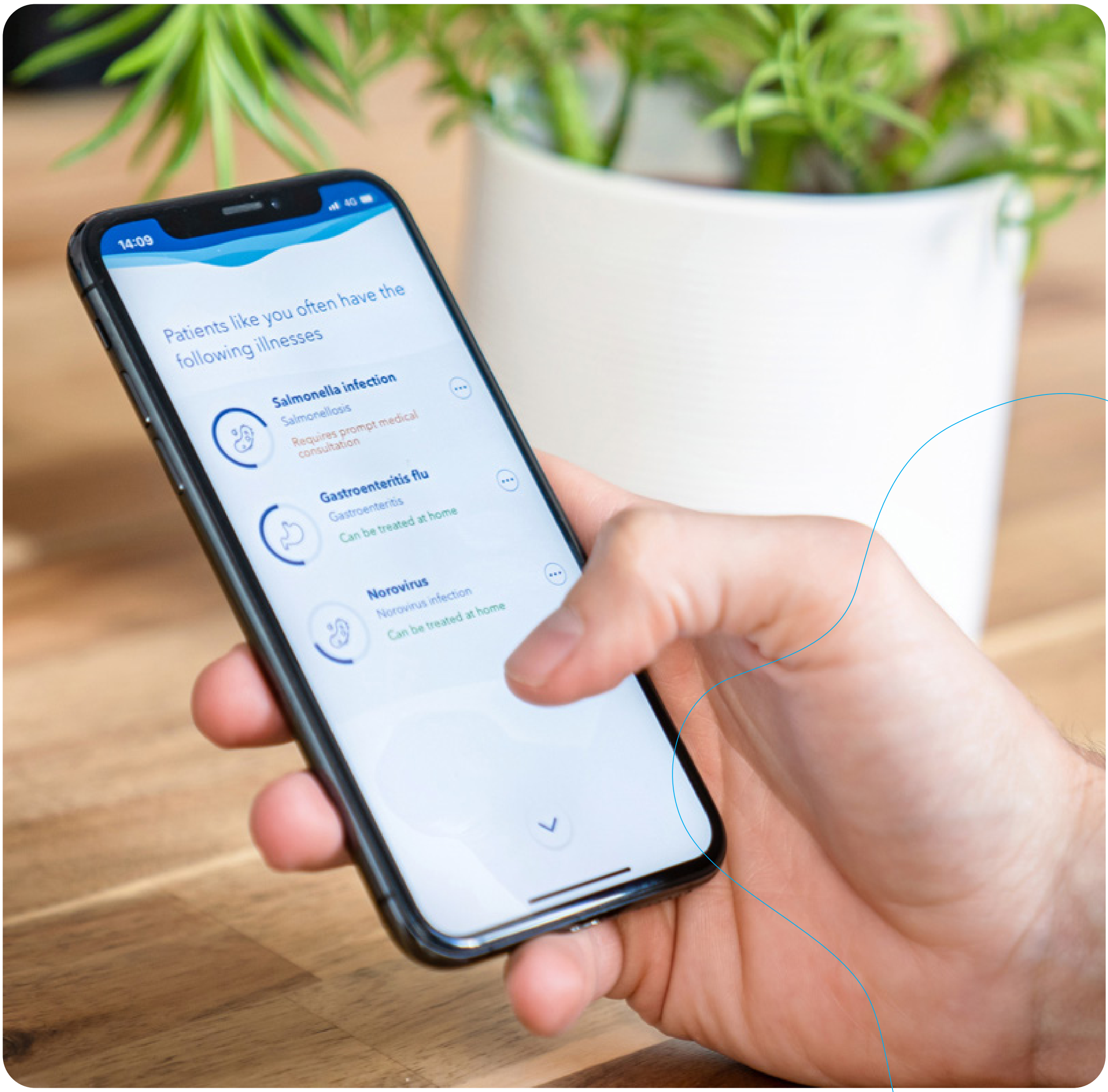
How we ensure data minimization of health data

The most critical personal data that could be available in XUND's systems are the answers to the various symptom and lifestyle questions asked of users. As this data concerns health, it is considered a special category of personal data according to GDPR and requires a significantly higher level of protection. For this reason, XUND has implemented an architecture where the answers to symptom and lifestyle questions are never linked to a user profile, and no direct or indirect identifiers of an individual are stored on our servers.

Our term for sessions consisting of questions and answers about lifestyle, illnesses, and symptoms is "checks". When a check is started on the client's website or app, they request a new access token for our API on behalf of the end user. This access token, which does not contain any user specifics, is used to authorize the end user to our services and assign them a random check ID.



On our servers, we store the questions and answers associated with the check ID. Additionally, the check ID is associated with the client who initiated the check for their end user. We do not have any other end user data linked to the check IDs. There are no direct or indirect identifiers linking multiple checks, nor is the specific age stored – only an age interval.



Legal overview of participating entities

The XUND Medical API is offered as a B2B solution that supports various use cases depending on the customer's implementation. There is a significant difference between the legal status of the data collected as part of the illness-, symptom check and the health check. For the former two – due to the data minimization that is applied and the temporary nature of the conditions - the check data can be considered de-identified. For health data collected as part of the health check, we consider it personal data according to the definition of the General Data Protection Regulation (GDPR).

Illness Check and Symptom Check

As the Medical API of XUND was designed with data minimization in mind, the data XUND receives as part of an Illness or Symptom Check is considered de-identified from XUND's perspective. That means that XUND contractually will not and technically cannot re-identify data subjects who answer the questions. If intended in the client's implementation of the XUND Medical API, it is possible to bind the information of a check to an individual in their system, but that happens outside of XUND's Patient Interaction Suite.

As XUND has to have a direct legal relation to end users, due to the medical device status of our Medical API, we simplify the relation by also acting as data controller for the data exchanged as part of Illness Checks and Symptom Checks. We provide data subjects our Privacy Policy and have an appointed Data Protection Officer to ensure the highest level of compliance with GDPR.

Health Check

As part of a Health Check, XUND collects characteristics of an individual like family health history, previous medical conditions, and long-term lifestyle information. While XUND does not collect direct or indirect personal identifiers, the answers to the Health Check might be specific enough to be regarded as personal data. As such, processing health related personal data requires a legal basis from GDPR Article 9 that can be for example fulfilling a legal obligation in the field of employment law, for the purpose of preventive or occupational medicine, or explicit consent.

As we are not in the position to choose the legal basis appropriate for the client's application and also to simplify the user journey, XUND acts as a data processor in case of the Health Check and only does processing on the instructions of its customers, the data controllers, which are documented in the service contract and extended via configurations on the ClientHub. It is up to the data controller to ensure transparency requirements and legal basis, including consent where needed, before making the XUND Medical API available to users.

Company privacy controls

While XUND's architecture ensures data minimization, that is not all we do to protect the privacy of our system's users. We have implemented comprehensive security practices and certified our Information Security Management System according to ISO27001. All our internal processes consider the data in our production system to be highly confidential and personal: Only selected employees have access to the production servers, and it is prohibited to copy any data from these databases.

XUND has dedicated internal staff focusing on data protection and additionally contracts an external Data Protection Officer to ensure independent supervision of our practices. We maintain complete GDPR accountability documentation and have documented processes for the handling of any personal data. We have additionally conducted a Data Protection Impact Assessment for the XUND Medical API product to ensure that the rights and freedoms of end users are adequately respected.

We sign Data Protection Addendums with all of our customers. Accordingly, as data controllers, our customers can request our support in fulfilling any data subject requests they receive related to XUND. We will delete personal data – unless it conflicts with our legitimate interests or legal obligations – on request within 30 days and automatically delete personal data from expired subscriptions after 90 days.

In the course of providing our services, we rely on vendors and service providers (collectively sub-processors). When selecting sub-processors, we take great care ensuring that their services hold up to the privacy standards XUND is committed to. Sub-processors are chosen based on the privacy regulations applicable at the company's headquarters, the hosting locations leveraged, and additional technical and organizational privacy controls offered. Providers from countries not recognized by the European Commission to provide adequate protection of personal data are only chosen if appropriate further safeguards have been put in place.

Author Info

Dr. Mark Vinkovits
Head of Data Protection
XUND

As Head of Data Protection, Dr. Mark Vinkovits is responsible for data security and privacy at XUND. His role also entails working on internal data protection projects, reviewing internal policies, and designing security-related customer-facing material about our security structures. In this white paper, he informs about the security and privacy standards at XUND.

About XUND

XUND enables healthcare companies to digitize the patient journey and translate unstructured data into actionable insights. We are the first digital point of contact for healthcare providers, helping patients to understand their symptoms better, get reliable assessments, and take the right next steps. Our technology offers an automated solution that is certified as a Class IIa medical device under the European Medical Device Regulation (MDR) and is the only one on the European market to meet all quality and safety requirements. The underlying database is powered by proprietary NLP models analyzing millions of medical publications and utilized by market-leading insurance, pharma, and big tech companies.