
CASE STUDY

Microsoft was the default answer. For IPW, it was the wrong one.

How a 1000-employee psychiatric institution in Zurich navigated US Cloud Act restrictions and Swiss federal data protection requirements to find a sovereign, end-to-end encrypted communication platform that put encryption key control back in the hands of IT.



At a Glance

Sector

Psychiatric Healthcare,
Switzerland

Organisation

IPW (Integrierte Psychiatrie
Winterthur-Zürcher
Unterland)

Employees

1,000

IT team

15

Challenges

Microsoft Teams ruled out: US Cloud Act exposure and Swiss federal data protection requirements made US-hosted platforms untenable for sensitive patient communications

Solutions

Wire, deployed initially as a departmental pilot, now expanding organization-wide

Key result

Full alignment with Swiss federal data protection requirements; encryption key control retained in-house; compliant Microsoft licensing path avoided



The challenge: when the path of least resistance isn't an option

For most organizations, Microsoft Teams is where the unified communications conversation starts. IPW was no different. With roughly 1,000 employees across a complex psychiatric care environment, Teams was the natural starting point and, for most staff, the preferred one.

It did not survive the compliance review.

IPW operates under the Swiss Federal Act on Data Protection (FADP), which classifies health data as sensitive personal data requiring heightened protection. Where data lives and who can access it under foreign law is not a preference for a psychiatric institution. It is a baseline condition. The specific conflict is the US CLOUD Act of 2018. In November 2025, Privatim, the Conference of Swiss Cantonal Data Protection Officers, concluded that the Cloud Act can compel US providers to hand over customer data to US authorities without following international mutual legal assistance procedures, even for data stored in Swiss data centers, and that Microsoft 365 does not meet the required standard in its default configuration.

"For the majority of people, Teams would probably have been the preferred choice," said Dario Chiga, Application Manager at IPW. "But because of the Cloud Act and US data centers, it doesn't really meet requirements in Switzerland."

The cost compounded the issue: according to Chiga, reaching the required licensing tier would have cost approximately CHF 500,000 per year.

1,000

Employees across a complex psychiatric care environment



Reaching the required licensing tier would have cost approximately CHF 500,000 per year.



The specific conflict is the US CLOUD Act of 2018

The search:

Two years, three alternatives, Sovereignty non negotiable

Finding the right platform took approximately two years. That timeline reflects both the stakes involved and how narrow the field becomes once genuine data sovereignty requirements are applied as a hard filter rather than a procurement checkbox.

IPW's search surfaced three candidates: Threema, Signal, and Wire. Each was evaluated against two non-negotiable criteria: data residency and encryption key control. Sovereignty risk, the exposure created by dependence on infrastructure subject to foreign jurisdictions, and compliance risk, specifically ISMS obligations and lawful handling of patient communications under the FADP, together defined the decision.

Sovereignty non negotiable



Threema and Signal offered strong encryption credentials but fell short on organizational scale and administrative control. Wire cleared the threshold: hosted or on-premise deployment, customer-controlled encryption keys, and European foundations. The interface mattered too. Chiga described Wire's design as familiar, comparable to apps staff already use in their personal lives. In a healthcare environment where clinical staff have limited time and tolerance for new tools, that familiarity is a deployment advantage that compounds over time.

The rollout: a deliberate start, learning fast

IPW began with a departmental pilot, a deliberate choice that gave the IT team room to observe adoption patterns and surface friction before committing to full organizational deployment.

The signals from that pilot were mostly quiet, which Chiga read as positive. In a clinical environment where communication tools are operationally critical, minimal complaints from end users is meaningful data. Staff were using it. The most actively used feature was video calls with patients, a use case that sits at the intersection of operational need and patient care delivery, and one that has become increasingly central to how modern psychiatric services are provided.

Where things stand: expanding to the wider organization

IPW is now moving from departmental pilot to organization-wide rollout, with the CEO and department heads involved in the decision. That shift in stakeholder level signals something important: Wire has crossed the threshold from IT evaluation tool to organizational infrastructure.

Staff took to it quickly. The familiar, WhatsApp-like interface reduced the onboarding burden across a workforce ranging from clinical staff to administrative teams, which in a healthcare environment is often the difference between a tool that gets adopted and one that gets abandoned. The platform has proven reliable in day-to-day operations, and Wire is actively developing the reporting and analytics capabilities that growing deployments naturally demand.

On integration, Wire operates independently of the Microsoft ecosystem by design. That independence is precisely what makes it sovereign and compliant, and for IPW it was a tradeoff made deliberately and without regret.

The rollout

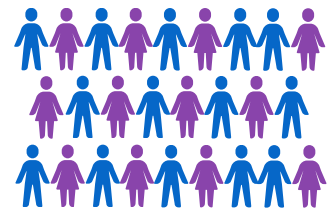
Department Pilot



Observation



Full organisational
deployment



What this means for organizations like IPW

IPW's experience surfaces a decision pattern that is increasingly common among regulated European institutions, particularly in healthcare, public services, and critical infrastructure, where the assumption that major US-hosted platforms are "good enough" is colliding with stricter regulatory guidance on data sovereignty.

Four dynamics are worth understanding for any IT or security leader navigating the same landscape:

1 Sovereignty requirements narrow the field dramatically

Once Cloud Act exposure and data residency requirements are applied as hard filters, the market of genuinely compliant options shrinks significantly. Organizations that have not yet run this filter often discover it mid-procurement, which creates pressure to either accept compliance risk or restart the evaluation entirely.

2 Compliance and sovereignty are not the same constraint, but they travel together

IPW's ISMS obligations and its requirements under the Swiss FADP are distinct constraints that both point to the same answer. Organizations in similar positions should evaluate communication platforms against both simultaneously rather than sequentially.

3 Encryption key control is the operational line in the sand

For ISMS-driven organizations, this is not a differentiating feature to be weighed against others. The *Privatim* resolution makes clear that organizations must control their own keys and that the provider must have no access to them. Platforms that cannot offer this remove a fundamental compliance decision from the organization's hands entirely.

4 A familiar interface is a clinical deployment accelerator

In environments where adoption failure means staff revert to ungoverned consumer tools, the usability gap between a compliant platform and an intuitive one carries real governance risk. Choosing a platform that staff recognize reduces that risk before rollout begins.

About IPW

IPW (Integrierte Psychiatrie Winterthur-Zürcher Unterland) is a psychiatric institution based in the Canton of Zurich, Switzerland, serving patients across a range of inpatient, outpatient, and community-based mental health services. With approximately 1,000 employees and a 15-person IT team, IPW operates at the intersection of complex clinical care and strict cantonal data security requirements.

Wire is a sovereign, end-to-end encrypted communication platform built for organizations where security, compliance, and data control are non-negotiable. Deployed by governments, healthcare institutions, and enterprises across Europe, Wire gives organizations full control over their communications infrastructure without compromising usability.

"Specifically, regarding patient care, it has streamlined our day-to-day workflow by providing a simple, intuitive platform for secure messaging. Because we no longer have to worry about data privacy or complex communication barriers, our team can share updates, coordinate treatment plans, and make decisions much faster. This seamless communication directly improves our efficiency, allowing us to focus more time and energy where it matters most: delivering attentive, high-quality care to our patients."

Dario Chiga, Application Manager at IPW



For more information visit wire.com

© 2026 Wire Swiss GmbH. All rights reserved.

Wire | ipw