SMARTLIBERTY

— MORE TIME FOR CARE —

Wi-Fi or Cell Service in Nursing Homes

Why the Right Answer Often Lies Somewhere in Between

Context

In our last post “GSM vs. WLAN telephony”, we highlighted why cellular networks (GSM) offer significant advantages in many areas of long-term care—particularly in terms of reliability, mobility, and ease of operation. In our view, this assessment remains unchanged and has been confirmed in numerous projects.

At the same time, practical experience is increasingly showing that the requirements for communication infrastructure are evolving. New technologies, changing usage patterns, and rising expectations mean that the original question must now be considered from a broader perspective. This post is therefore not intended as a counterposition, but rather as a deliberate complement and further development of our previous perspective.

Why the discussion often falls short

The question “Wi-Fi or cellular?” is posed in a very fundamental way in many projects. At first glance, this seems reasonable, as both technologies offer different strengths. Upon closer examination, however, it becomes clear that this comparison falls short.

A technology decision is rarely neutral today. Choosing one system clearly often means simultaneously ruling out other possibilities. This not only defines the current solution but also limits future flexibility.

This aspect is particularly crucial in the long-term care sector, where investments must be planned for the long term. An excessive focus on a single technology can result in future developments being implemented only with additional effort—or not at all.

The Constant: Communication Must Work

Regardless of technological trends, one requirement remains constant: communication must not fail in everyday care. It is the foundation for safety, coordination, and efficient processes.

In this context, mobile communications has proven to be particularly robust. Independence from local infrastructure, stable voice quality even while on the move, and continuous reachability beyond the building are characteristics that play a decisive role in daily life. The value of this reliability is particularly evident in situations where time is of the essence.

These strengths remain and continue to be a central component of a resilient communication solution.

What has changed in the environment

In addition to these constant requirements, several developments have emerged in recent years that broaden the perspective.

First, the use of so-called M2M (machine-to-machine) SIM cards is increasing significantly. More and more systems—from emergency call solutions and sensor technology to technical installations—communicate directly with cloud platforms via the mobile network. These devices no longer rely on a local Wi-Fi infrastructure but function independently of it. As a result, part of the infrastructure is increasingly shifting away from the building toward external networks.

On the other hand, user behavior has changed. Residents, relatives, and staff members bring their own smartphones and mobile phone plans with them. As a result, mobile coverage is already widespread today—regardless of a facility's internal infrastructure. At the same time, expectations for continuous connectivity are rising, both inside and outside the building.

In parallel, the demands on digital processes are growing. Mobile care documentation, applications on tablets or smartphones, and other digital services require a high-performance data infrastructure. Here, Wi-Fi continues to play a central role, provided it is professionally planned, implemented, and operated.

The key insight

These developments lead to a clear conclusion: The future does not belong to a single technology. It emerges where different technologies are meaningfully combined.

The reality in modern care facilities is already characterized by a coexistence of different communication channels. Communication, data, and devices have different requirements—and consequently require different solutions.

Why extremes become a risk

In practice, we often encounter two opposing approaches. On one hand is the idea of meeting all requirements through a high-performance Wi-Fi network. On the other hand is the focus on cellular networks as the primary solution.

Both approaches have their merits and are based on sound reasoning. At the same time, experience from projects shows that they reach their limits when used as a standalone strategy.

A pure Wi-Fi approach entails a high degree of complexity. In particular, the requirements for stable voice communication while on the move place high demands on planning, operations, and end devices. Even small deviations can significantly impair quality.

A purely mobile-based approach, on the other hand, can reach its limits with data-intensive applications and integration into existing systems. Processes that rely on local networks cannot always be fully replicated via mobile networks.

An often underestimated factor: the lifecycle and security of Wi-Fi infrastructure

An additional aspect that is often overlooked in the discussion is the lifecycle of Wi-Fi infrastructure—particularly access points.

Access points are security-critical network components and follow a clear lifecycle.
To ensure compliance with current security standards and minimize cyber risks, they must be replaced regularly or at least technologically upgraded.

In practice, a similar picture emerges across industries:
- Aruba (HPE): approx. 5–7-year lifecycle (End of Support / Security Updates)
- Huawei: approx. 5–6 years
- Hikvision (network components): often approx. 4–6 years, depending on the model and security requirements

After these periods expire:
- Security updates expire
- New standards are no longer supported
- Cybersecurity risks increase significantly
-

In concrete terms, this means:
Wi-Fi infrastructure is not a one-time investment, but an ongoing renewal process
This aspect often puts the supposed cost-efficiency of a pure Wi-Fi approach into perspective while simultaneously increasing the demands on planning and operation.

The SmartLiberty Perspective

Our experience shows that a clear separation by function leads to the best results. The focus is not on the technology, but on the specific use case.

Mobile communications is particularly well-suited for areas where reliability and availability are top priorities. These include voice communication, emergency call systems, general reachability, and, increasingly, M2M and IoT applications.

Wi-Fi, on the other hand, plays to its strengths in data-driven processes. Applications, documentation, and internal systems can be efficiently operated via a properly designed Wi-Fi infrastructure.

This division creates an architecture that is both robust and flexible. At the same time, it avoids the need for a single technology to meet all requirements.

A Look into the Future

Current developments suggest that this trend will continue to gain momentum. The number of connected devices is increasing, applications are becoming more cloud-based, and mobility in everyday work continues to grow.

This also changes the role of the infrastructure. It will become more flexible, more distributed, and less tied to individual locations. Systems that are designed to be open and combinable today offer clear advantages here.

Conclusion

Our original position remains unchanged: Mobile communications provide a robust and reliable foundation for communication in long-term care.

Today, we would add: A future-proof infrastructure emerges where technologies are combined in a meaningful way.

The crucial question, therefore, is not which technology is better. Rather, it is about which solution offers the greatest security and flexibility in each specific application.

Or to put it another way:
It is not the decision to choose a technology that matters—but the ability to refrain from ruling one out.
That is precisely the key to sustainable and future-proof solutions in care.