Deutsche Gesellschaft
für Internationale
Zusammenarbeit (GIZ) GmbH

This guideline serves as a practical compass for project managers, helping them design and implement digital health projects that are sustainable and scalable.

How to Digital Health

Standards and guidelines for digital health interventions in international cooperation

GIZ's Task Force Digital Health Blueprint – Sector Network Health and Social Protection

Contents

About this guide 1
Introduction 1
Why digital approaches fit the current challenges of the health sector 2
Partner needs and demand 3
The guiding framework for digital health projects – digital public infrastructure for health 3
A whole-of-system approach attuned to health system reform priorities 4
Key objectives for digital health projects: building interoperable systems at scale 7
Transformative opportunities and innovative enablers 10
Practical consideration for implementation – managing political economy and agility 10
Conclusion 14

About this guide

This guide was developed through a collaborative effort of GIZ practitioners working across the health portfolio, bringing together experiences and lessons learned from digital health projects implemented in different country contexts. It reflects the collective expertise of a community of practice dedicated to strengthening the quality, sustainability, and scalability of digital health interventions in international cooperation.

The guide builds on practical implementation experience, partner country demand, lessons learned from ongoing projects, and international best practices and frameworks. It was developed through exchanges within GIZ's Digital Health Community of Practice and aims to provide project managers with a shared orientation for designing and implementing digital health interventions.

The lead authors of this guide are **Julius Murke** and **Pauline Krolinski**, with valuable contributions and feedback from members of GIZ's health portfolio and the Digital Health Community of Practice.

Introduction

This guideline has been developed to provide project managers with high-level orientation on how to plan, design, and implement digital health projects. Its purpose is not to prescribe detailed technical solutions, but rather to serve as a practical compass that helps projects align with international best practices, respond effectively to partner needs, and contribute meaningfully to the digital transformation of health systems.
At the core of this document are quality criteria for digital health projects. These criteria are derived from four key sources:

1. Partner needs and priorities, ensuring that digital health contributes directly to country ownership and sector strategies.
2. Lessons learned from existing GIZ projects, with particular attention to addressing recurring shortcomings and implementation challenges.
3. International guidance from expert communities and organizations, drawing on widely recognized frameworks and recommendations.

Based on these foundations, the guideline introduces a framework for quality digital health projects:

1. Primary Quality Criteria – Projects are assessed against two essential questions:
   a) Does the project contribute to standards-based, interoperable digital public infrastructure?
   b) Does the project support the implementation of digital systems at scale rather than through fragmented, small-scale pilots?
2. Innovative Enablers – Projects are encouraged to explore three areas of transformative potential:
   a) Artificial Intelligence (AI) applications for health,
   b) Collaboration with the private sector, and
   c) Data spaces as emerging instruments for data governance and value creation.
3. Good implementation practices – projects are encouraged to apply identified implementation practices:
   a) Political Economy Management
   b) Agile Management and in project IT-expertise
   c) Ensuring Information security

By providing this structured orientation, the guideline empowers project managers to integrate digital first approaches into health projects.

Why digital approaches fit the current challenges of the health sector

The health sector represents both, an economic opportunity for new businesses, and a challenge to governments' budgets and societal risks. An opportunity because especially the digital health care market is forecasted to grow "at a Compound Annual Growth Rate (CAGR) of 23.4% from 2024 to 2030" in Africa"[1] and "16% from 2023 to 2030"[2] in Europe. A challenge, because the sector is characterized by 1) unsustainable spending, 2) a double burden of diseases with the persistence of infectious diseases and an increase of non-communicable diseases, 3) the emergence of new threats such as anti-microbial resistance and pandemics and 4) demand for personalized care and an increasingly blurred boundary between health and wellbeing, which puts individuals in the center but also in charge of their health.

The challenges that the health sector must grapple with require structural transformations that will only be possible to realize with digital solutions. Unsustainable spending demands a shift from focusing on treating patients to preventing diseases. Care of non-communicable diseases requires more coordination of care and continuous follow-up of patients outside of health facilities. Emerging threats must be safeguarded against by multi-sectoral management approaches by governments. Personalized care needs individual information from people over their live course.
Digital can help in all of these:

1. Preventive/Predictive medicine: analysis of social media behaviour signals to me that I should screen for diabetes, informs me about environmental risks and my health insurance proposes to offer special benefits for lifestyle changes
2. Coordinated and assisted self-care: remote blood level monitoring and surveillance of treatment schedules
3. Safeguard against new threats: prevent the spread of emerging infectious disease with satellite data-based risk monitoring.

Notwithstanding the potential benefits of digital health, many digital health projects fail or are not able to scale due to their complexity. Given the example of Germany's electronic health record, it took 20 years to launch a concrete digital application. To improve the implementation quality of digital health projects the blueprint offers a summary of good practices and proposes standardized approaches.

Partner needs and demand

Based on a market analysis conducted by GIZ's, the following main partner country demands were identified:

Standards & Interoperability:
Countries need support with standards and interoperability solutions to connect specialized systems. Donors can help coordinate planning, maintain consistent health systems architectures, and manage system standards. Cross-sectoral interoperability needs are growing, including digital identity, payment systems, and One Health integrated systems.

Strategy & Investment:
There is a demand to support digital health strategy and investment planning. Embedded in Health System Strengthening, governments demand scalable approaches suited to country needs.

Workforce:
Country needs include both general and specialized IT staff. Demand exists to provide digital health training courses for country staff, addressing knowledge gaps and integrating training with interoperability and strategic planning.

Services & Applications:
While there's low demand for new standalone applications, there's high demand for publicly funded Digital Public Global Goods.

The guiding framework for digital health projects – digital public infrastructure for health

The magic of digitalisation really comes into play when multiple systems start to talk to each other. This allows for the automation of processes and the reuse of existing digital services. For example, when a supply chain management system and a hospital information system are interconnected, prescriptions made in the hospital information system can be automatically transformed into an order for a medication in the supply chain management system. If the data from the two systems is additionally used for Routine Health Information for monitoring purposes, real-time high-quality data can be provided without the need for manual data collection and transcription. This said, the gold-standard for digital health interventions need to be interventions that contribute into a larger framework of digital public infrastructure for health.

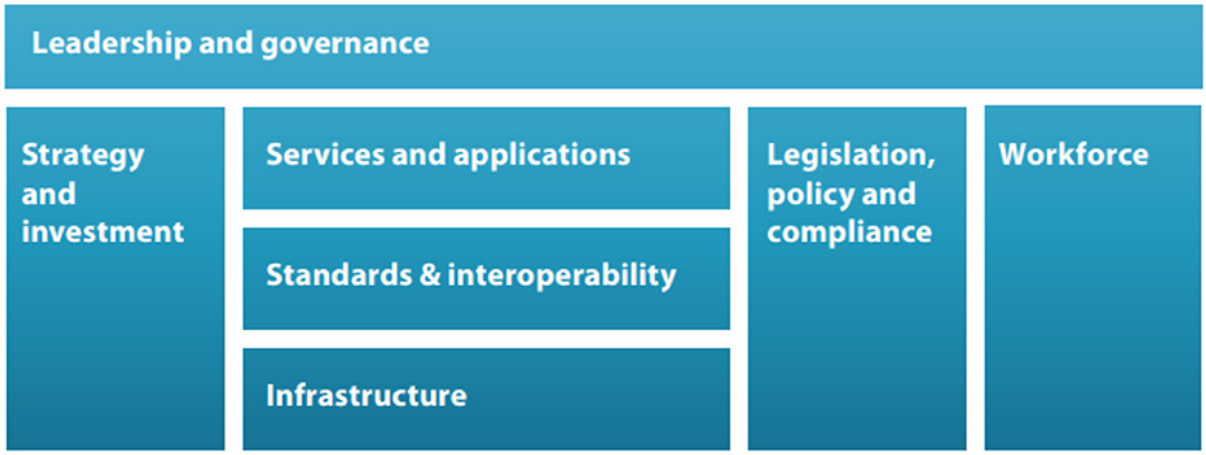
Digital Public Infrastructure is the collection of standards and foundational connectivity services that allow digital health applications to function as a system. Whereas the concept is rather abstract, implementing Digital Public Infrastructure in health is about supporting governments in developing the software systems and cloud services, that allow for different specialised systems to seamlessly exchange data. This would for example mean to develop a public software service that would manage unique patient identifiers, which would be usable by all software systems and would thereby allow to exchange patient data across different systems. In the health sector such unique identifiers need to be made available for all kinds of information, such as medication names, health provider codes or codes for diagnoses. Thus, a Digital Public Infrastructure for health would provide the platform for specialised systems to communicate seamlessly.

A whole-of-system approach attuned to health system reform priorities

Digital health projects cannot be designed as isolated interventions or stand-alone tools. To be sustainable and impactful, they need to strengthen the health system as a whole. For this reason, this guideline adopts a systems approach, using the WHO eHealth building block framework as a reference for mapping how interventions contribute to different system elements. This perspective helps project managers to ensure that digital health projects:

- Address real gaps in the health system, rather than creating parallel solutions.
- Complement other ongoing initiatives, avoiding duplication or fragmentation.
- Contribute to long-term digital transformation rather than short-term pilots.

The WHO framework identifies six key system elements that should be considered when planning or assessing digital health interventions. Projects can contribute to one or several of these elements, but every project should be positioned clearly within this overall system.



National eHealth Strategy Toolkit, WHO 2012

1. **Leadership and Governance**

Strong political commitment and effective governance mechanisms are prerequisites for sustainable digital health. Projects should support governments in developing policies, strategies, and governance structures for digital transformation. This includes aligning interventions with national eHealth strategies, strengthening institutional coordination, and promoting transparent decision-making.

2. **Strategy and Investment**

Digital health requires long-term financial and strategic planning. Projects can contribute by helping partners develop costed investment roadmaps, building capacities for budgeting and financing, and exploring blended finance or public-private partnerships. Ensuring financial sustainability is key to avoiding “pilot graveyards.”

3. **Services and Applications**

These are the actual digital solutions deployed in health systems, such as electronic medical records, telemedicine platforms, or disease surveillance systems. Projects should prioritize applications that meet pressing health system needs, are scalable, and can integrate with other services rather than functioning as stand-alone applications.

4. **Infrastructure**

Digital health relies on reliable connectivity, hardware, and power supply. While GIZ projects may not always directly invest in infrastructure, they should assess infrastructural readiness, identify potential bottlenecks, and where possible collaborate with broader infrastructure programmes to ensure feasibility and sustainability.

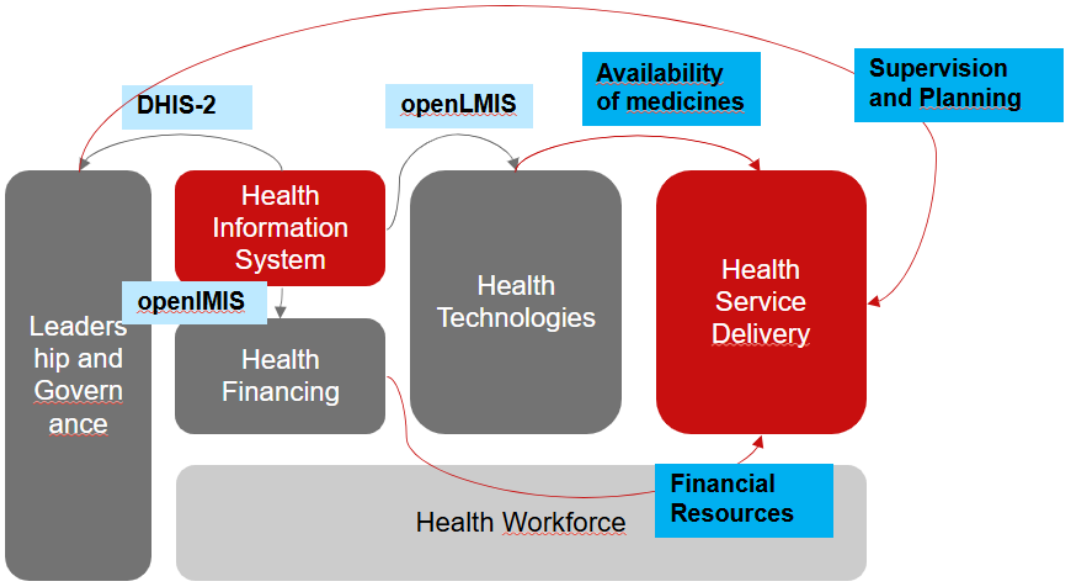
5. **Standards and Interoperability**

Without standards, digital systems cannot exchange or make use of data effectively. Projects must align with national and international standards, support open architecture, and promote interoperability. This ensures that solutions can grow over time, integrate with existing systems, and contribute to digital public infrastructure.

6. **Workforce**

Digital health depends on people as much as on technology. Projects should strengthen the digital health workforce by building digital literacy among health professionals, supporting capacity development for IT staff, and ensuring that end users are adequately trained. Gender and equity considerations are critical in workforce development.

In order for digital health interventions to create value and be sustainable they need to follow the current system reform priorities. A useful conceptualization of health systems is WHO's health system building blocks framework:



Source: GIZ, Julius Murke

Health system reform priorities, maturity and reference enterprise architecture pave the way

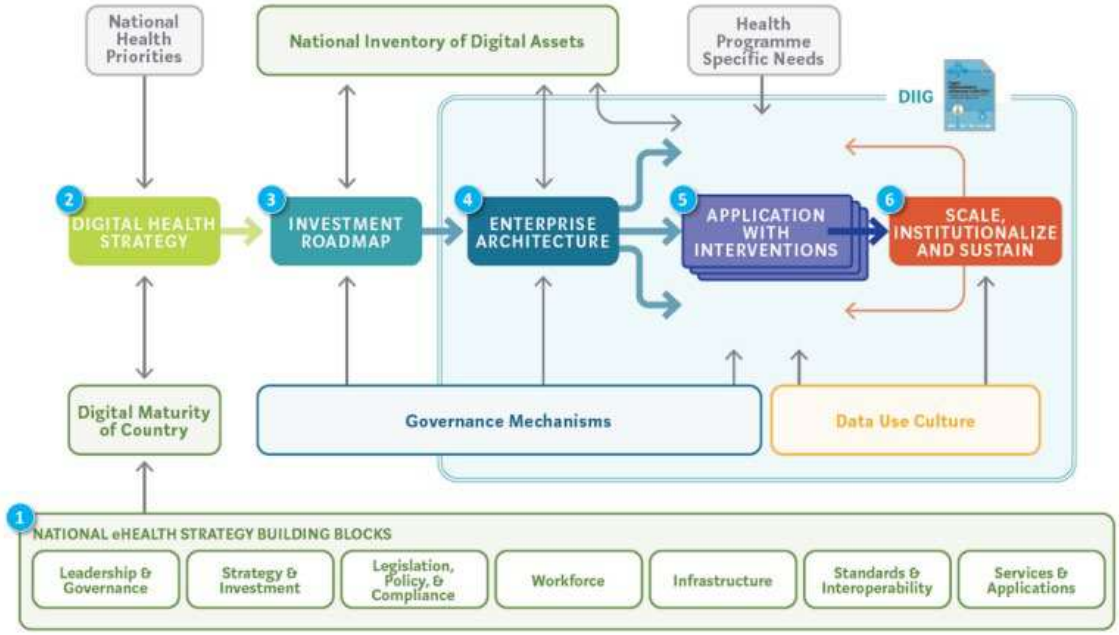
The logic of prioritizing interventions can usefully follow three principles:

- Digital health interventions should follow health system reform priorities. Thereby interventions can scale and deliver concrete value.
- Digital health interventions should contribute to or build a reference enterprise architecture. Thereby digital transformation will be built on systems, not stand-alone applications.
- Digital health interventions should follow the level of maturity of the health system and the digital system. Thereby, the first two principles will be combined, and the right priorities can be identified.

It must be noted that complex systems follow multiple underlying “logics”. The digital system perspective, applied via an enterprise architecture logic, goes beyond current health system reform priorities but is set out to ensure efficient digital approaches in the medium- to long-run because certain investment from the onset will dramatically reduce costs in the long-run even though the most pressing health system reform priority would not necessitate a certain infrastructure element from the onset (this especially relates to interoperability). Therefore, the different system logics must be combined according to the current context, and this is where maturity (both of the health system and the digital system) comes in.

The following graphic provides a high-level overview of a framework in which digital health interventions should be planned:

Figure 1 Essential processes of national digital health implementations.



Source: DICE - Stepwise Toolkit for Planning & Budgeting Interoperability of Digital Health Solutions

An illustration of how different maturity levels require different priorities

The objective to contribute to building digital public infrastructure for health should be the guiding principle in almost any intervention. Nevertheless, countries are at different stages of their digital health journey and therefore priorities will depend on context:

1. In low states of maturity, the government will mainly be concerned with developing and implementing the main specialised systems that are necessary to properly manage the health sector. This would be for example a digital supply chain management system, a public insurance management system or an electronic medical records system. As data sovereignty is an important element that our partners are concerned with, basic local cloud services need to be in place. Likewise, health facilities should be connected to the internet from the onset on.
2. In a next maturity phase, these foundational systems would then be interconnected via a public interoperability layer combined with standards-based meta-data services.
3. As a next step, foundational specialised systems would move from a “one public standard system”-approach to an open market approach in which multiple providers implement certified systems, such as supply chain management systems and electronic medical records systems. Likewise, a “data space” approach would be pursued that would enable the exchange of data especially among non-state actors. At

this stage, accreditation mechanisms, certifications, and collaborative standards-setting committees become the main tools of the government to ensure interoperability. Likewise, data protection and sharing regulations need to be implemented.

4. Once, a standards-based interoperable public infrastructure is in place, external applications and new innovations can be connected. Thereby, point-of-care diagnostic applications, such as AI-based radiology, or patient-based applications can share their data, and these products can easily be integrated into the care process. At this point, more elaborate governance of data sharing will be essential to establish a conducive ecosystem for AI-based innovations, since these depend on interconnected data as a key input. Data sharing needs to be regulated on multiple levels. On the one hand, this would be on the level of policies and regulations that clearly outline the requirements for private stakeholders on what data to share in what format. On the other hand, this would entail the promotion of data conveners or the setup of a public data repository. At this point, advanced local/regional cloud service capacities and connectivity infrastructure are important for an ecosystem conducive for new innovations.

It is important to note that the described states of maturity are not a description of how to phase interventions. Building specialized systems with standardized metadata and connected to an interoperability layer from the onset on is less expensive than introducing standards at a later stage. **Therefore, any digital health intervention should be compliant to a reference digital health enterprise architecture.**

Key objectives for digital health projects: building interoperable systems at scale

The two main shortcomings of common digital health interventions are: “fragmentation” and “no scale”. Therefore, project managers can strengthen its service offer by focusing on interoperability and the large-scale implementation of specialised systems. Additionally, even though strategies are an important ingredient, a lot of good plans are never implemented. Therefore, projects can apply agile instead of linear system implementation: “You should not work for 2 years on a 10-year strategy without starting implementation. Instead, implementation and strategy can be done in parallel.”

Implementation of interoperability

In digital health, interoperability refers to the ability of different digital systems, applications, and devices to exchange, understand, and use health data reliably and securely across organizational and national boundaries. Interoperability goes beyond technical connectivity: it ensures that data flows meaningfully, supports clinical decision-making, informs health system management, and empowers citizens.

There are three main levels of interoperability:

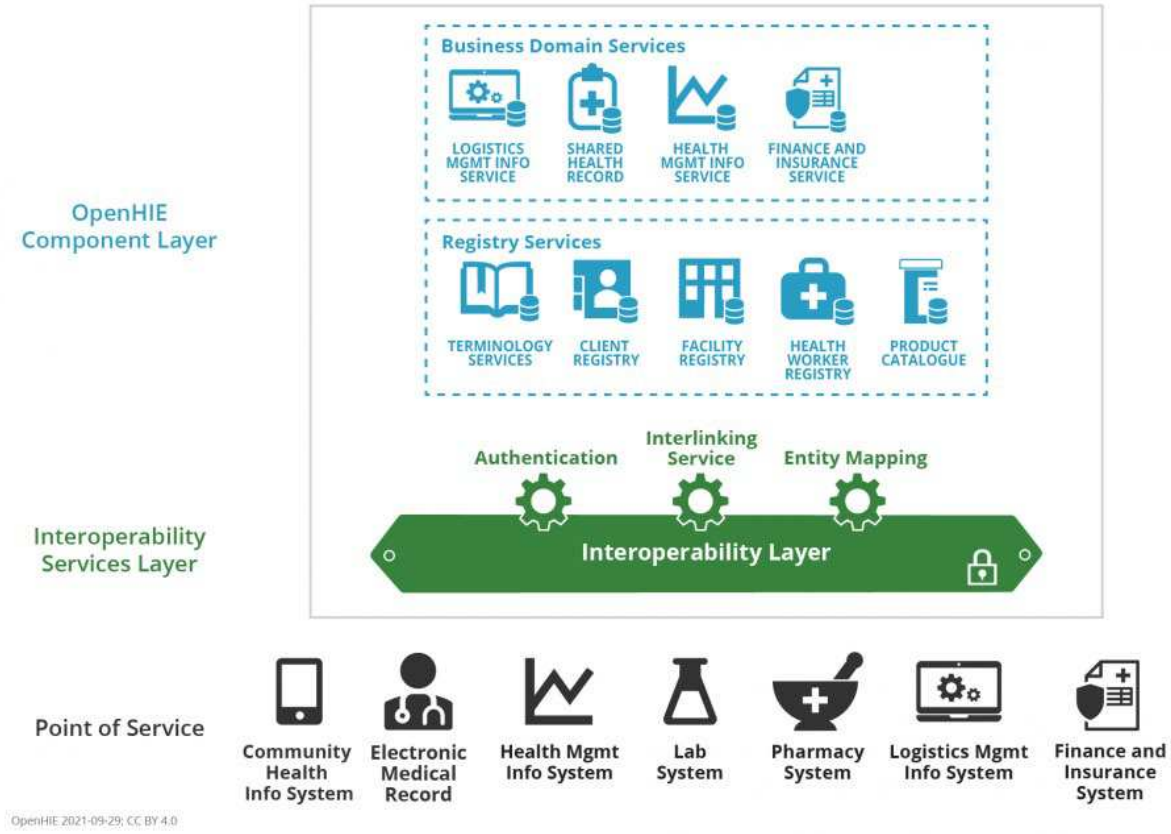
- Technical interoperability: the exchange of data between systems using common formats and protocols (e.g., HL7 FHIR).
- Semantic interoperability: ensuring that exchanged data has the same meaning across systems (e.g., using common terminologies such as ICD-10, SNOMED CT, LOINC).
- Organizational interoperability: aligning policies, workflows, and governance so that data exchange is trusted, legal, and usable in practice.

Interoperable systems bring significant benefits. They can improve the quality of care by making patient information accessible across facilities and levels of the health system. They can increase efficiency by reducing duplication of reporting and investments in parallel

systems. They can enable data-driven decision-making, as integrated data flows can inform disease surveillance, resource allocation, and policy-making.

While often described in abstract terms, interoperability must be understood as a **pragmatic implementation challenge** that requires simultaneous work on vision, infrastructure, and governance.

The first step can be the creation of a **clear vision through enterprise architecture**. Enterprise architecture describes how different components of a health information system are supposed to fit together and interact. It provides a structured map of the current state of digital health systems, the desired future state, and the transition path between the two. Without this system-wide vision, projects risk reinforcing fragmentation by developing applications in isolation. GIZ projects can therefore actively support partner governments in developing or updating enterprise architectures, ensuring that they are aligned with national health strategies and embedded in broader digital transformation agendas. WHO and ITU are currently working on a reference enterprise architecture and the openHIE framework also provides a solid framework.



Source: openHIE community

Once the vision is established, interoperability needs to be translated into **concrete software infrastructure**. This involves building or strengthening so-called “interoperability services” that function as a middle layer between health applications. Such services include health information exchanges, middleware platforms, and metadata registries for health workers, facilities, patients, and terminologies. They ensure that data can be securely routed, mapped, and reconciled across different systems. By focusing on this layer of digital public infrastructure, projects can provide unique added value. Many development organisations concentrate primarily on end-user applications, while fewer have the technical depth to invest in the architecture and middleware that make systems interoperable and sustainable.

At last, **governance through accreditation and standards-setting is also important.** Technical solutions alone do not guarantee interoperability unless they are backed by clear rules and incentives. Governments need mechanisms to accredit systems against defined standards before they can be integrated into national platforms. They also need institutional processes to define, adopt, and regularly update standards, ranging from technical protocols like HL7 FHIR to semantic frameworks such as ICD and SNOMED CT. Projects can support ministries of health in establishing these governance mechanisms, creating working groups with key stakeholders, and building capacities for standards compliance and certification.

In practice, implementing interoperability is rarely linear. Enterprise architecture may exist only in draft form, infrastructure may be fragmented, and governance may be weak. Project managers should therefore adopt a **stepwise and adaptive approach**: clarifying the vision where possible, making pragmatic investments in interoperability services, and gradually embedding governance and standards.

Implementation of specialized systems at scale

It must be noted that interventions that are not reform priorities are not likely to scale. Therefore, specialized systems would ideally be implemented according to the partners' priorities. In low- and middle-income country contexts the following large-scale system implementations are common government requests:

1. Insurance management/Health financing information system – a moderately complex intervention. These systems are critical for countries moving toward universal health coverage. At scale, these systems support enrolment, premium collection, claims processing, and fraud detection across millions of beneficiaries. To be especially effective, they can integrate with national identification systems, provider registries, and payment platforms, while ensuring compliance with data protection standards.
2. Supply chain management information system – moderately complex intervention. They form the backbone of reliable access to medicines, vaccines, and health commodities. Implemented at scale, they enable real-time stock visibility, demand forecasting, and automated resupply. These systems are most effective when integrated into national procurement and logistics processes and when linked to facility-level data on service delivery.
3. Electronic health records – a very complex intervention, especially at scale. They allow longitudinal patient histories to be maintained across facilities and levels of care, supporting continuity of treatment and reducing duplication. Implementing EHRs requires careful attention to clinical workflows, user acceptance, and training of health workers. They must also be interoperable with other national platforms, such as laboratory systems and health insurance databases.
4. Surveillance systems - a moderately complex intervention. These systems collect, analyze, and report data on disease trends and public health events. Ideally, surveillance systems integrate with routine health information systems, reporting tools, and with laboratory networks to provide timely and actionable information.
5. Laboratory information systems - a moderately to highly complex intervention. These systems manage test ordering, sample tracking, result reporting, and quality assurance across multiple laboratories. Ideally, laboratory information systems are interoperable with EHRs, surveillance systems, and supply chain platforms to ensure accurate and timely data flows.
6. Data integration platforms and repositories - an emerging and moderately complex intervention. These systems consolidate data from multiple digital health systems into a single, harmonized environment. These platforms enable cross-system analytics, advanced reporting, and research.

Across all interventions, scaling systems successfully requires attention to non-functional requirements, which are often overlooked in pilots. These include system performance under high loads, security and privacy protections, sovereign data storage, and organizational development to ensure sustainable operation.

Transformative opportunities and innovative enablers

In addition to core digital health systems, digital health projects can explore innovative enablers—interventions that extend the impact of digital health investments. The three main areas data spaces as instruments for data governance and value creation, artificial intelligence (AI) applications for health, and collaboration with the private sector. Scale is less of a concern for these areas as they are still emerging and governments are still learning how to implement in these intervention areas.

Data spaces are emerging instruments for managing data governance, interoperability, and data economy. They provide a structured framework in which multiple stakeholders can access, share, and use data under defined rules with specialized software infrastructure elements while retaining sovereignty over their datasets. This can be especially helpful in cross-border research or AI projects or collaboration with the private sector and academia because often times, projects fail due to missing authorizations for data sharing.

Artificial Intelligence (AI) applications for health can support predictive analytics for disease surveillance, optimize supply chain management, assist clinical decision-making through diagnostic support or triage tools or detect fraud in financial management systems. Working with systems at scale is a key enabler for AI projects because it makes large-volume data available and allows to implement AI models into real-world systems and to therefore create an added value.

Collaboration with the private sector can provide technical expertise, infrastructure, and business models that complement public sector initiatives. Projects can facilitate partnerships by identifying areas of mutual interest, negotiating shared responsibilities, and creating incentive structures that align with public health goals. Engaging with the private sector requires investments in networking and project proposals. Implementing systems at scale also helps in attracting private sector collaboration because thereby, projects offer a well-established contact to partners and deep-rooted context knowledge.

Adding these innovative enablers to projects focused on large-scale implementations can provide the right ecosystem to realize new business opportunities.

Practical consideration for implementation – managing political economy and agility

Successful implementation of digital health projects depends not only on technical design and infrastructure but also on how projects are managed. Hereby, three good implementation practices stand out: Political Economy Management, Agile Management combined with in-project IT expertise and Ensuring Information Security.

Managing political economy

Managing the political economy context is paramount if we want to implement interoperability and systems at scale, because both represent transformative changes to the systems we work in. Political economy refers to the interplay of political, institutional, economic, and social forces

that influence decision-making, resource allocation, stakeholder interests, and power dynamics.

A key ingredient to managing political economy is the dedication of specific resources to it. This means:

- staff that is available to participate in workshops and to engage in informal discussions with key stakeholders,
- financial support to key strategy processes linked to the project,
- travel allowances for participation of high-level decision makers in international conferences or study tours

Furthermore, managing political economy often requires the involvement of leadership staff – sometimes beyond project director level..

Whereas managing the political economy can differ depending on the context and does not have to be addressed as a stand-alone work stream, the following approaches can be applied:

Understand the landscape before designing or deploying solutions

The framework of a Political Economy Analysis provides the right questions. Nevertheless, you should not give this task to an external consultant, but should ensure that leadership and teams understand the context themselves:

- Know the key stakeholders: government agencies, donor partners, healthcare workers, private sector, civil society, and local communities.
- Know the power dynamics, incentives, and resistance points – identify winners and losers of the project.
- Know the formal rules (laws, policies) and informal norms (patronage, networks).

Alignment and ownership

Projects should be aligned to national strategies and set up in co-ownership with our partners from the outset. Otherwise, project failure for transformational interventions is very likely. Nevertheless, in most countries' strategies are not always coherent and whereas an intervention might be welcomed by one stakeholder it might be opposed by another. Therefore, alignment and ownership must be strengthened and constantly maintained. Thereby, projects can take the following actions:

- Ensure that new strategies, operational plans and projects are aligned to the intervention. Therefore, projects should be present in coordination meetings of development partners and establish a trustful working relationship with national partners. This might also require sometimes support strategy processes financially or with making technical expertise available that were originally not part of the project's objectives.
- Invest in local capacities: work with local software developers and train partners in system administration and configuration early on.
- Build alliances: facilitate consensus amongst stakeholders of partner organizations and align with other development partners.
- Create visibility for your partners: look for possibilities for your partners to share success stories in international fora and in front of the political leadership.

Agile (hybrid) management and IT-Expertise

Implementations of software and information system projects are prone to unforeseen costs, delays and even failure. As a response to the challenges in the management of software implementation projects, the agile management approach has become almost a gold standard in the private sector. The approach is especially well suited to adapt to previously unforeseen user needs. Nevertheless, agile management has not become a standard in the public sector.

Therefore, projects should proactively apply agile approaches in the implementation of digital health interventions.

Delays, never-ending business process analysis and underestimated budgets for software development

Linear project management approaches often face the following challenges:

- Business process analysis and system requirement specification take longer than commonly expected and do finally not fully fit user expectations and actual process requirements. This leads to both project delay and incomplete software design.
- Contracted software developers might not be available at 100% during the specific months foreseen for actual implementation of system requirement specifications leading to further project delay and shortcomings in quality of implemented code.
- Additional requirements that are identified after contracting with software developers are not accounted for in initial project planning and create frustration at the level of users and software developers alike.

Be agile but not negligent - challenges that can arise with agile project management

1. Focus on quickly developing a minimum viable product might lead to underinvestment in non-functional requirements such as software performance and information security.
2. Early project success can create overambitious timelines for scaling implementation to a number of users that the system cannot yet handle. This will eventually lead to low system performance and information security risks.
3. A highly dynamic and agile project management approach can lead to insufficient testing, resulting in deploying half-baked solutions in production – this might lead to high maintenance costs and user frustration.

Good practices in agile project management in digital health

Agile project management approaches are preferable to a linear setup. Agile especially helps in reducing delays and building software fit to processes. Nevertheless, agility requires considerable expertise and strong product ownership.

Enabling factors for agile and sound project management:

- Employ software developers and business process analysts in digital project management teams to ensure sufficient technical expertise. Sufficient expertise adds flexibility to the implementation. Unforeseen tasks that are not part of contracted service providers can be taken over by project staff and can reduce the need for additional contracts. Besides agility, technical expertise allows for more precise planning of required resources.
- Cooperate with other projects and build strategic alliances. This will add technical expertise and flexibility.
- Experiment with service level agreements: in a project that is constantly piloting new tools or continually updating already implemented software, service level agreements would provide more flexibility in implementation of activities that have not been specifically foreseen beforehand.
- Ensure sufficient funding for hosting and software development. Whereas unforeseen needs for training, user support and business analysis can usually be covered by the project implementation team to a certain extent, core software development and hosting will often be procured externally. Insufficient budgets in these areas are a considerable risk for project failure.

Practical approaches to ensure more agility in project implementation

- Plan for the deployment of multiple system upgrades during a typical implementation period of two years.

- If not already existing: start with developing a prototype/proof-of-concept and deploy an MVP as quickly as possible.

Manage product ownership in tandem between the digital project management team and the leadership of the public institution responsible for the implementation. This is especially important in setups where the public institution relies heavily on the technical expertise of an external digital project management team. A trustful working relationship in such a setup is a must for an agile approach.

Ensuring Information Security

While planning the implementation of a country's disease surveillance platform SORMAS, one question quickly became more important than any dashboard: Who can see what?

It was the right question to ask. The security of health information is not a technical detail to be resolved at the end of a project. It is one of the most fundamental steps in building trust. In digital health, trust is not a luxury. It is a requirement. If our systems cannot guarantee that data is protected, partners will hesitate to share it. If data does not flow freely and safely, there can be no effective health response.

What is at stake?
Health data is one of the most sensitive categories of personal information. Once leaked or misused, the damage cannot be undone.
In digital health projects, data routinely crosses borders, servers and organisations, often in contexts where harmonised legal frameworks or shared technical standards are still absent. This is precisely why information security must be embedded in the planning process from the outset. Retrofitting security into a live system is costly, disruptive, and rarely complete.

At its core, information security protects data along three dimensions, the same principles that underpin the internationally recognised ISO 27001 standard:

1. *Confidentiality: Only the right people see the right data*
   Software that we procure in this context handles highly sensitive health data such as case information, laboratory results, contact tracing details. Access must follow the need-to-know principle.
   Example: If user roles are not properly configured, a district officer might see patient data from other regions. Role-based access controls can prevent this. Laboratory users see test results, epidemiologists see aggregated case data, and national users see trends. Keeping these layers separate protects privacy and builds trust in the systems.

2. *Integrity: The data must remain correct and unchanged*
   Reliable public health action depends on trustworthy data. Errors, duplication, or tampering can delay or misdirect responses.
   Example: A health worker manually edits a confirmed positive test result to 'negative', whether by mistake or with intent, and the system records no trace of the change. Downstream analyses are based on corrupted data; the error goes undetected and a patient who needed follow-up falls through the cracks. Audit logs and write-protection mechanisms ensure that every change is recorded, attributable and reversible if needed.

3. *Availability: The data must be there when it is needed*
   During an outbreak, delays can cost lives. Systems must work under pressure, including in rural areas or during emergencies.
   Example: A district could not access the national dashboard for three days during a cholera outbreak because backups had not been tested. The result: delayed response and avoidable loss of life.

These three dimensions are inseparable. As system that is confidential, integer but unavailable when needed has failed. One that is available and intake but accessible to the wrong people has also failed. Health data is universally classified as high sensitivity and the standards applied must reflect that reality.

When Security is Outsourced. Responsibility is not.

Outsourcing is a standard feature of digital health implementation. Software development, hosting, maintenance, or technical support: these are routinely contracted to external providers, and there is nothing inherently problematic about that. What is problematic is the assumption that contracting out a function means contracting out the responsibility for it.

It does not. Regardless of who manages the technology, accountability for data protection and security remains with the organisation that commissioned the work. This has concrete implications for your work:

- Include security requirements in every tender where you specify what you expect.
- Put it in writing. Contracts must specify who stores the data, who has access, and who must be informed in case of an incident. Have a critical eye on e.g. Service Level Agreements.
- Ask for transparency and verify. Suppliers should disclose where servers are located, how backups are managed, which subcontractors are involved, and which certificates they hold to ensure information security. Verification matters as much as documentation.

Security is not an optional service tier. Addressing it at the procurement stage is not bureaucratic caution. It is the most effective form of crisis prevention available.

Secure data exchange builds on conditions for collaboration: between hospitals and ministries, national programmes and international partners, health systems and the communities they serve. It ensures that systems remain functional precisely when they are needed most.

Conclusion

Digital health projects bear immense potential for transformative change but are often confronted with a common challenge: many interventions remain fragmented or fail to scale. This guideline proposes a practical orientation to address these shortcomings and improve the quality of digital health investments.

The first guiding principle is that digital health projects should contribute to the development of Digital Public Infrastructure for Health. Digitalization creates the greatest value when systems can exchange data and work together. Therefore, projects should prioritize standards, interoperability, and the development of foundational services that allow specialized applications to function as part of a larger ecosystem whenever possible.

The second guiding principle is that digital health interventions should follow health system reform priorities. Projects should focus on strengthening the core information systems that governments need to manage their health sectors, such as health financing systems, supply chain management systems, electronic health records, surveillance systems, laboratory systems, and data integration platforms. In other words, digital health systems must focus on health system value.

The third guiding principle is that digital health interventions should be adapted to the maturity of the health system and the digital ecosystem. Countries are at different stages of their digital transformation journey and therefore require different priorities. Nevertheless, interventions

should align whenever possible with a reference enterprise architecture and apply standards in order to avoid costly fragmentation later.

The fourth guiding principle is that implementation matters as much as technical design. Strong political economy management, country ownership, stakeholder alignment, agile implementation approaches, and sufficient technical expertise within project teams are critical success factors. Digital health projects are not only technology projects, they are change management projects.

Finally, information security must be treated as a foundational requirement rather than an afterthought. Trust is the basis of digital health. Without secure, reliable, and well-governed data systems, interoperability, data sharing, and digital transformation cannot succeed.

If project managers consistently ask whether their interventions contribute to interoperable digital public infrastructure, support systems at scale, align with reform priorities, and are implemented with sufficient attention to governance, security, and political economy, they will significantly increase the likelihood that their projects generate sustainable impact.