NEONCUBE

Cloud-Driven Medtech & Mediatech 2025

Radpoint. medical innovation institute Teranode silesian startup foundation

Media partners

MY COMPANY POLSKA Innovations Hub Foundation

Agenda

Introduction

This report explores the key challenges and opportunities of implementing cloud solutions in the Medtech and Mediatech sectors. Digital transformation in these industries is no longer optional - it's a necessity. Cloud computing - powered by technologies like artificial intelligence (AI), machine learning (ML), and blockchain - is driving current trends in modern IT systems.

The report addresses both strategic and technological aspects, including the role of security and scalability, automation opportunities, and emerging service delivery models. At the heart of this transformation are Neoncube and Radpoint - companies leveraging experience and innovation to shape the future of cloud in the health and media sectors.

> Why does this matter? Digital transformation is no longer optional. For Med-tech and Mediatech, cloud computing is becoming a strategic necessity - not just a technical upgrade.
>
> **Jacek Nosal**
> Co-founder Neoncube

Why is the cloud important?

Cloud solutions benefit both large organizations and startups - though their needs differ.

For large companies

Cloud solutions help reduce infrastructure maintenance costs, simplify service scaling as demand grows, and boost operational resilience. It supports integration with new technologies (AI, Big Data, automation) and reduces time to innovation.

For startups

Low entry costs, rapid prototyping, and the ability to test products without investing in physical infrastructure make the cloud a natural environment for innovation development. PaaS and serverless models speed up iteration, and flexible billing allows better budget

In both cases, the cloud supports meeting stringent security and compliance requirements - from HIPAA and GDPR to industry standards and audits. For those handling medical data or high-value digital content, cloud is the foundation - not an optional layer.

Organizers of the report

NEONCUBE

Neoncube is a company founded by six technology experts who don't just implement solutions - they take full responsibility for their success. Specializing in cloud transformation for the Medtech and Mediatech sectors, the team delivers scalable backend platforms, mobile and web applications, and intelligent systems based on AI and ML. Neoncube prioritizes a partnership approach and a strong sense of ownership - from initial concept, through design and development, to implementation and long-term maintenance. The team integrates seamlessly with client organizations, offering flexible collaboration models that always focus on security, regulatory compliance, and business continuity.

> At Neoncube, it's not just about technology - it's about delivering real business value and standing behind the entire process from start to finish.
>
> **Jacek Nosal**
> Co-founder Neoncube

Radpoint.

Radpoint is a leader in advanced diagnostic imaging technology, delivering comprehensive, integrated IT solutions for hospitals, diagnostic networks, teleradiology providers, and small labs. By leveraging artificial intelligence, process automation, and flexible integration models, Radpoint supports workflow optimization for radiologists, helping improve medical service quality and operational efficiency.

> We are developing a cloud-based SaaS platform that unifies RIS, PACS, VNA, AI, and teleradiology into a secure, comprehensive working environment. Intelligent automation, seamless integration, and full data control - everything is designed to make diagnostics faster, simpler, and more reliable.
>
> **Michał Smoliński,**
> CTO at Radpoint

Partners of the report

Media partners

MY COMPANY POLSKA

Innovations Hub Foundation

Technical partners

Radpoint.

medical innovation institute

Teranode

silesian startup foundation

Bodislav & Associates

RIG CHAMBER OF COMMERCE AND INDUSTRY IN KATOWICE

BIOCAM CAPSULE ENDOSCOPY

upmedic

AI w zdrowiu

1

Migration to the cloud – costs and ROI

1.1

Does the cloud optimise costs?

Migration to the cloud – costs and ROI

Cloud migration costs – how much does it really cost and how not to overpay?

Jacek Nosal
Co-founder & Full Stack-Engineer at Neoncube

Co-founder and Full-Stack Engineer at Neoncube, with deep expertise in supporting Medtech and Mediatech companies in their cloud transformation journeys. He works with both established organizations and startups, helping them migrate to the cloud and build scalable, secure, and future-proof systems. His portfolio includes projects such as 21 Seconds to Know for ITV. Jacek values relationships built on mutual respect and shared commitment, believing that effective collaboration is the founda-

Migrating to the cloud is a strategic investment for companies aiming to enhance the scalability, security, and flexibility of their IT infrastructure. But when does it truly make sense?

Primarily when existing solutions begin to limit growth-whether due to technological constraints or rising operational costs. It's essential to understand that cloud migration involves more than just paying for servers or virtual instances. The total cost includes consulting, tool and data migration, integration efforts, staff training, and ongoing maintenance. In this article, we take a closer look at the real costs behind cloud adoption and how to approach them strategically-so the investment leads to long-term gains, not unnecessary overspending.

What really makes up the cost of migrating to the cloud?

Migrating to the cloud is not a single cost - it is a comprehensive package of activities that require careful planning, experience, and the right team. Using the example of a medium-sized website (e.g., an e-commerce or SaaS platform with an active customer base), we can break down the following costs:

- **DevOps consulting (design, planning, supervision): PLN 10,000 - 50,000**
- **Migration of software and tools (e.g. CI/CD, databases, web applications): PLN 5,000 - 20,000**
- **Server and data migration (backups, configurations, staging/production environments): PLN 5,000 - 20,000**
- **Cost of virtual instances or container services (e.g. EC2, ECS, GKE): PLN 500 - 2,000 per month**
- **Data transfer (outgoing traffic, file synchronization): up to PLN 500 per month**
- **Support, monitoring, maintenance of the environment (SLA, updates, security): up to PLN 5 000 per year**

For MVPs, these costs can be significantly lower-especially when leveraging free plans offered by cloud providers and using automated open-source tools. It's crucial to remember that each implementation must be analyzed on a case-by-case basis. Migrating a simple CMS is a vastly different process compared to transitioning a microservices architecture that handles sensitive patient or customer data.

How not to overpay? 7 proven cost optimization strategies

At Neoncube, we follow a clear principle: the cloud should be a flexible tool, not a fixed cost, tailored to the specific needs of the business. This approach means we implement targeted strategies that help companies maintain control over their expenses while scaling efficiently:

1. **Matching instances to actual computing requirements -** rather than "stocking up", it is worth matching resources exactly to the load.
2. **Real-time scaling -** we use autoscaling mechanisms to increase resources only when necessary.
3. **Use of free plans (Free Tiers)** - e.g. AWS, Google Cloud, and Azure offer many services at no cost during the MVP phase.
4. **Implement open source tools (e.g. Terraform, Ansible)** - these allow infrastructure to be automated without additional licenses.
5. **Monitoring and alerts (e.g. Prometheus, Grafana)** - help to quickly detect excess consumption and optimize operations.
6. **Using specialised services for specific tasks** - e.g. DynamoDB, AWS Lambda, Spot Instances - is a real money saver with high traffic.
7. **Regular audits of resource consumption -** allow unused components to be eliminated and consumption reduced without compromising performance.

These strategies save our clients real money - both at the implementation stage and in the long term when the scale of operations begins to grow.

How to act on the MVP? Low-cost and iterative

For new products or startups, the most effective approach is the iterative method. We begin with a low-cost MVP, utilizing free or affordable services, and then gradually develop the system, continuously monitoring and optimizing costs along the way.

- **Avoid over-investment at the start**
- **Learn real patterns of resource consumption**
- **Make decisions based on data, not assumptions**

> In practice, this means that companies can begin with a minimal budget, only investing in more robust infrastructure as traffic and requirements grow. Continuous cost monitoring and expert analysis of data are crucial-these insights help avoid potential pitfalls and guide the best decisions at each stage of product development.
>
> **Jacek Nosal**

Summary

Migrating to the cloud is not just a technical transformation; it's also a critical business decision. The cost depends on several factors, including scale, system type, service selection, and the quality of planning. A well-executed migration and optimization strategy can not only reduce costs but also speed up product development and improve reliability. It's essential to view the cloud as a scaling partner-but only if you have experts by your side who know how to

- Avoid over-investing early
- Learn from real usage patterns
- Make better, data-driven decisions
- Scale only when necessary
- Iterate without accumulating technical debt

Cloud ROI – what financial benefits can be achieved by implementing cloud solutions?

Migrating to the cloud isn't just about cost savings-it's an investment that can deliver returns faster than many managers realize. From lower maintenance costs to enhanced productivity, flexibility, and even competitive advantages, well-designed cloud solutions can provide a solid return on investment (ROI) for both startups and large enterprises. In this article, we will present concrete figures and highlight specific areas where the cloud can have a significant impact on a business's bottom line.

From cost to savings - where does the cloud generate the greatest return?

Based on the experience of the Neoncube team and data from leading cloud providers, the ROI from cloud deployments can be measured across several key areas:

Reduce IT operating costs by 20-50%
Maintaining physical infrastructure, server rooms, or local systems is a significant expense. Moving to the cloud means spending less on hardware, energy, human resources, and maintenance.

Scalability of resources by 30-70%
By automatically adapting computing power to current business needs, companies avoid redundant costs and gain flexibility.

Improving energy efficiency by 15-30%
Modern data centers in the cloud model are energy-optimized and significantly more efficient than local servers.

Reducing the risk of cyber-attacks by 25-50%
Cloud providers invest heavily in security at a level that would be unattainable for most companies - from automatic backups to advanced threat detection.

These are not just ‚soft' benefits – they are concrete numbers that translate into an operating budget and competitive advantage.

Faster to market, faster to return

- **Ready-made components and platforms (PaaS, SaaS)** allow businesses to implement functions without having to build them from scratch.
- **CI/CD automation** speeds up testing, deployment, and updating of applications, ensuring faster iteration cycles.
- **Elimination of infrastructure constraints** enables teams to focus on product development instead of managing servers and hardware.

The result? Faster time-to-market leads to a quicker path to generating revenue and an earlier return on investment (break-even point).

Cloud is no longer just a technological shift - it's a strategic business lever. Used properly, it pays for itself quickly.

Cloud ROI – what financial benefits can be achieved by implementing cloud solutions?

Better cost control = better business decisions

In the traditional IT infrastructure model, costs can sometimes be unpredictable and difficult to account for. In the cloud, the opposite is true - you gain:

1.

Pay-as-you-go model
You only pay for the actual consumption of resources.

2.

Precise reports and alerts
Allowing you to react quickly to changes and optimise costs.

3.

Flexible deployment models (PaaS, SaaS, serverless)
Enable you to create exactly the systems you need here and now, without wasting resources.

This makes the cloud a financial tool – enabling more predictable budgeting and better management of IT development expenditure.

Your business is ready for ROI from cloud if:

- → You're scaling and want to avoid upfront CAPEX
- → Time to market is a critical factor
- → Your team is slowed down by on-prem infrastructure
- → You lack real-time cost control
- → You need global availability and uptime guarantees

Summary

Investing in the cloud isn't a cost-it's a strategy to accelerate growth, enhance agility, and achieve real cost savings. It enables faster time to market, provides access to world-class services, and offers a broader range of capabilities that ensure the security and scalability of your business. A well-executed cloud deployment not only pays for itself, but also helps your business stay ahead of the competition.

On-premises vs. cloud – why might the cloud be more cost-effective in the long term?

Choosing between on-premises infrastructure and the public cloud is a decision that impacts not just technology, but the overall profitability of the business. At first glance, the cloud may appear more expensive, but the reality is quite the opposite. With a well-planned approach, the total cost of ownership (TCO) can be lower, and the flexibility is significantly greater. Below, we'll compare the two models with concrete figures and explain why, especially in the long run, the cloud is often the smarter choice.

How much does it really cost to maintain infrastructure?

Let's compare the real costs of running an undersized, poorly optimized IT environment in an on-premises model and in the cloud:

On-premises model (local infrastructure)

- **Location maintenance (power, cooling, space):** PLN 10,000 – 50,000 per year
- **Network and equipment maintenance:** PLN 5,000 – 20,000 per year
- **Staff costs (admin, helpdesk, supervision):** PLN 1,000 – 5,000 per month
- **Total:** PLN 15,000 – 75,000 per year (not including equipment investment)

Cloud model

- **Computing and storage costs (instances, storage):** PLN 500 - 2,000 per month
- **Data transfer (outbound traffic, API):** PLN 100 - 500 per month
- **Support, monitoring, maintenance:** PLN 1 000 - 5 000 per year
- **Total:** PLN 600 - 7,500 per month

As you can see, both models can cost similarly - but in the cloud, it is much easier to optimize this expenditure, and the input investment threshold is lower. And this is just the beginning of the cloud's advantages.

On-premises vs. cloud – why might the cloud be more cost-effective in the long term?

Why does the cloud give you more for the same (or less) money?

Cloud infrastructure not only works differently - it changes the way a company uses technology. Here are the specific advantages that affect long-term profitability:

1. **Scalability on demand** – you only add resources when you need them.
2. **No capital costs** – you don't buy equipment, you don't wait for implementations.
3. **Automatic updates and patching** – increases security and relieves the burden on IT teams.
4. **Advanced monitoring and access management** – from a single console.
5. **Flexible billing models** – matched to consumption, not to forecasts.
6. **Possibility to change supplier or region** – without rewriting the entire architecture.
7. **Easier integration with other systems and business partners** – especially in API-first environments.
8. **Greater service availability (SLA), global presence and 24/7 technical support.**

As a result, the cloud offers a better cost-to-value ratio, especially for digital services that need to respond to changes in real-time.

Expert perspective: the cloud is flexibility and security

> Cloud services offer higher levels of flexibility, scalability, and availability, allowing businesses to respond quickly to changing customer needs and reduce service costs.
>
> **Jacek Nosal**
> Neoncube

It is the ability to adapt quickly, scale instantly, and err on the side of volatile market conditions that is driving more and more companies away from in-house infrastructure. Especially where time, efficiency, and business continuity are key.

Summary

The on-premises model may appear cheaper in the short term, but in practice, it comes with higher maintenance costs, limited scalability, and a greater risk of failure. The cloud, on the other hand, enables continuous optimization of costs while providing access to cutting-edge solutions that directly boost profitability and competitiveness. Over the long term, it is simply the more cost-effective option.

2

Cloud Security

2.1

How does cloud technology strengthen data protection?

Cloud Security

AWS Shield and AWS WAF - safeguarding against DDoS attacks and cyber threats

Michał Ślaga Co-founder & Full Stack-Engineer at Neoncube

Companies worldwide are falling victim to sophisticated DDoS attacks that can quickly cripple online services and result in significant financial losses. Meanwhile, cybercriminals are continuously developing new tactics to bypass defenses, prompting organizations to adopt multi-layered security measures. In this article, I'll take a closer look at AWS Shield and AWS WAF-two services that work together to prevent server overloads and block unauthorized traffic. With these tools, businesses in Medtech and Mediatech can greatly reduce the risk of costly incidents.

Why does the cloud give you more for the same (or less) money?

According to the Cloudflare, DDoS Threat Report Q3 2024, the number of DDoS attacks increased by

49% quarter on quarter

55% year on year

This escalation is largely driven by the easy availability of tools that enable massive waves of network requests. In some cases, all it takes is a simple script or renting a botnet. When a server is flooded with fake requests, its bandwidth or processing power quickly becomes overwhelmed, rendering the service inaccessible to real users.

The impact of such attacks can be devastating. For streaming platforms, downtime can result in lost subscribers, while in Medtech, blocking access to patient systems could have serious health repercussions. High availability has become a standard expectation, meaning that every minute of downtime translates into reputational and financial damage.

According to Veeam, Data Protection Trends Report 2023, 85% of enterprises reported that each hour of downtime generates at least USD 50,000 in losses for them (taking into account operating costs, lost revenue and image damage).

AWS Shield and AWS WAF – safeguarding against DDoS attacks and cyber threats

AWS Shield – a defense against massive attacks

AWS Shield is designed to protect against both volumetric attacks and more sophisticated attempts to overwhelm a system. The basic version, AWS Shield Standard, provides protection for resources running on Amazon CloudFront and Route 53 at no additional cost. For more complex threats, AWS Shield Advanced is worth considering, offering:

- **Deeper traffic analysis (so-called flow-based monitoring).**
- **A dedicated AWS DDoS Response Team (DRT) for support.**
- **Protection against skyrocketing costs from sudden scaling during an attack (known as AWS Cost Protection).**

In short, AWS Shield offers multi-layered protection against complex DDoS attacks, automatically detecting and neutralizing traffic that could overwhelm a system. The Advanced version provides additional benefits, including expert support through the DDoS Response Team (DRT) and protection against unexpected costs related to the sudden scaling of resources during an attack.

AWS WAF – a firewall for suspicious traffic

AWS WAF (Web Application Firewall) is ideal for scenarios that require fine-grained control over HTTP and HTTPS traffic. It allows you to define rules that block requests based on specific patterns, such as incorrect headers or sequences commonly associated with malicious code injections (e.g., SQL injection). Integration with services like Amazon CloudFront or Application Load Balancer enables you to position the firewall closer to the end user, reducing latency.

73% **of web application security breaches are caused by inadequate Layer 7 protection. Deploying AWS WAF helps mitigate this risk by providing customizable rules and automated signature updates. (Forrester, Web App Security Trends)**

What can AWS WAF block?

- → **Requests with malicious headers**
- → **SQL injection patterns**
- → **XSS attacks**
- → **Bad bots or IP ranges**
- → **Traffic from unsupported geographies**
- → **Requests not matching expected behaviour**

Cyber-security with a trusted partner

Modern DDoS attacks and advanced cyber threats impact nearly every industry that relies on online services. AWS Shield and AWS WAF are two essential components of any security strategy: one defends against large-scale infrastructure attacks, while the other ensures that malicious requests never reach sensitive application resources.
To protect your platform from major incidents and avoid costly downtime, consider integrating these services into your environment.

Sources

1. Cloudflare, DDoS Threat Report Q3 2024, https://www.cloudflare.com
2. Veeam, Data Protection Trends Report 2023, https://20937100.fs1.hubspotusercontent-na1.net/hubfs/20937100/data-protection-trends-report-2023.pdf

Case Study Neoncube: Securing PACS Systems Against DICOM Malware

Jacek Nosal Co-founder & Full Stack-Engineer at Neoncube

Is it truly possible to protect radiology devices from malware hidden in DICOM files? One medical facility learned the hard way how dangerous it can be when security procedures are neglected. After several servers responsible for image processing began showing unusual errors, it became clear that the situation was more serious than initially thought. By swiftly deploying AWS services and restructuring their PACS systems, the organization not only eliminated the threat but also enhanced diagnostic efficiency.

Context

The facility was relying on outdated PACS infrastructure, which - according to internal estimates - extended patient diagnosis times by about:

40%

The image archiving process was inefficient, and the system lacked robust defense mechanisms against DICOM malware.

Success

After migrating to AWS, the time needed to analyze diagnostic files fell to just 15 minutes, while also strengthening protection against potential DICOM malware attacks.

Challenges Before Implementation

The main challenges included years of unpatched servers and software, creating vulnerabilities that cybercriminals could exploit. The facility was also concerned about escalating storage costs as the volume of images grew. Moreover, the IT team had limited experience with major cloud migrations.

According to Neoncube, TOP Medtech Trends in 2024, DICOM is a foundational standard in modern facilities, but a lack of regular file monitoring can lead to attacks leveraging hidden malicious code in metadata.

Jacek Nosal
Neoncube

Implementation process

AWS Shield is designed to protect against volumetric attacks as well as more sophisticated attempts to overwhelm a system. The basic version, AWS Shield Standard, safeguards resources running on Amazon CloudFront and Route 53 at no extra charge. For more complex threats, it's worth considering AWS Shield Advanced, which offers:

Phase 1

Selecting AWS Services for Image Storage and Processing
The team chose Amazon S3 as the data repository, ensuring scalability and built-in encryption. AWS Lambda was also deployed to scan every newly uploaded DICOM file, ensuring security at the point of entry.

Phase 2

Automated File Analysis and Malware Protection
The scanning software was integrated with Amazon Macie to detect unusual metadata structures. Additionally, AWS GuardDuty monitored network operations for suspicious activity. These steps enabled the facility to block malicious files before they could infiltrate the PACS system.

Phase 3

Team Training and Standardizing Procedures
The IT staff underwent intensive cybersecurity training focused on the new tools and technologies. The team also standardized the update process, eliminating previous delays in patching known vulnerabilities and ensuring proactive security measures were in place.

Results

By adopting cloud solutions, the infrastructure cost dropped by 60%, primarily due to resource optimization and the pay-as-you-go model. Diagnostic processing sped up by 40%, significantly reducing patient wait times for test results and boosting patient satisfaction rankings. AWS enabled us to scale resources during peak demand while protecting PACS from malicious DICOM files. According to DICOM standards, this environment not only ensures interoperability but also provides a high level of data security.

DICOM Security and success Post-AWS migration

This facility's experience demonstrates that migrating to AWS and adopting advanced security measures can effectively neutralize threats related to DICOM malware. In addition to enhanced protection, day-to-day operations for medical staff have improved, and operational costs have been reduced. In an era of rising cybersecurity requirements, every healthcare organization should consider taking similar steps.

After all, it's not just about safeguarding infrastructure; it's about protecting patients and ensuring seamless workflows for healthcare professionals.

2.2

Practical approach to risk management

Cloud Security

Zero Trust Security in the Cloud – how to implement a restricted access policy?

The rising frequency of attacks on cloud infrastructures has made it clear that traditional security methods are no longer enough. Zero Trust Security has evolved from an industry buzzword into a proven strategy for limiting access based on the principle of "trust = zero". In this article, we'll explain why Zero Trust is so effective in mitigating risks in the cloud and outline the key elements you can implement to protect both corporate data and sensitive user information.

Why is the Zero Trust Model becoming so important?

In an era of widespread digital transformation, more corporate resources are being moved to the cloud. Many managers still believe that a basic firewall and sufficiently strong passwords provide adequate protection. However, as ENISA's Threat Landscape 2022 report highlights, there is an increasing number of incidents where cybercriminals gain access to endpoint login credentials and exploit overly broad permissions to infiltrate critical internal resources.

Such configuration vulnerabilities can lead to the takeover of critical services, which is especially concerning for companies migrating to the cloud-often unaware that a firewall and "good" passwords alone are no longer sufficient to ensure full security.

Under the Zero Trust model, every component in a system-whether it's a user, device, or application-is treated as a potential threat. Instead of automatically granting trust, you verify identity and permissions every time, regardless of location or device status. **This approach reduces the risk of lateral movement within a network and limits potential points of entry.**

Zero Trust in the Cloud – 4 Key Components

1. **Resource Segmentation** – dividing infrastructure into security zones
2. **Strong Authentication** – MFA as a mandatory login standard
3. **Least Privilege Access Control** – only necessary privileges
4. **Continuous Monitoring (SIEM/SOAR)** – real-time detection and response

Putting a restricted access policy into practice

The first step in implementing Zero Trust in the cloud is to take an inventory of your applications and data. Next, you need to identify which services are mission-critical and require the most stringent access controls. A great example of this is AWS Identity and Access Management (IAM), which allows you to establish detailed permission policies that specify exactly how users log in and what operations they can perform. When combined with Amazon GuardDuty, you gain an additional layer of protection-AI that detects unusual traffic patterns, enabling you to respond to incidents almost in real-time.

CASE STUDY

Zero Trust in Medtech

As we highlighted in the Mission: How using AWS improves teamwork in Medtech? Business aspects, medtech companies are migrating to the cloud for scalability and cost optimization. However, working with patient data requires a heightened level of protection.

In practice, beyond basic access control through IAM, many organizations also implement encryption both at rest and in transit (e.g., using AWS KMS), along with micro-segmentation. This approach ensures that a data analysis module, for example, doesn't have direct access to the entire patient database. As a result, if an attacker compromises one component, they won't automatically gain visibility into the entire system.

Conclusions and next steps

Zero Trust in the cloud is rapidly becoming the standard for more companies aiming to gain full control over data flows and enhance their security measures. This approach focuses on restricting access to resources, granting permissions only to the necessary roles and scopes of authority, thereby minimizing the risk of unauthorized activity. In practice, this involves properly configuring IAM, continuously monitoring activity, and implementing clear network segmentation. This ensures that even as cloud services scale, there is constant oversight of who can access a system and to what extent. Given the rising threat landscape and increasingly sophisticated attacks, such solutions enable organizations to maintain control, flexibility, and a high level of data protection.

Sources

1. ENISA, Threat Landscape 2022, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Minimising the impact of technical debt

Artur Grzybowski
Co-founder & Full Stack-Engineer at **Neoncube**

Artur Grzybowski is the Co-founder of Neoncube and a seasoned technology leader with over 20 years of experience in web development and cloud systems architecture. From the outset of his career, he has been driven by the principle, “Don’t focus on problems-look for solutions”. He specializes in designing and implementing modern web and backend solutions, with a strong emphasis on quality, performance, and scalability.

Technical debt is an inherent risk in long-term projects. As new features and elements are added to the system, outdated technologies or libraries can begin to affect its stability and performance. This raises important questions: How can we effectively manage technical debt so that it doesn’t hinder future development? How can we ensure our systems remain flexible and adaptable over time?

In the fast-paced Mediatech environment, where competition is fierce and the time to implement new features is critical, overlooking these issues can have serious consequences. For this reason, we’ve decided to develop a strategy to minimize the impact of technical debt on system performance.

Read full article

AWS Security Hub – automated detection and neutralization of threats

Jakub Mrowiec Co-founder & Full Stack-Engineer at Neoncube

Did you know that even a small security gap in the cloud can lead to major expenses and a loss of customer trust? In sectors like Medtech and Mediatech, where critical patient data or streaming services for thousands of users are involved, rapid incident response is crucial. AWS Security Hub is a tool that automates threat detection and streamlines the process of neutralizing potential risks before they escalate into serious problems.

Intelligent detection of vulnerabilities

The growing number of services running in the cloud means greater challenges in monitoring their security.

40%

of data breaches involved data stored across multiple environments (IBM, Cost of a Data Breach Report 2024)

This is especially true for environments that have grown rapidly, such as through scaling streaming services or telemedicine deployments.

For IT teams, one of the most challenging tasks is detecting unusual traffic patterns or incorrect permissions across multiple accounts. AWS Security Hub simplifies this by aggregating data from various services, such as Amazon GuardDuty and AWS Config, and automatically categorizing and prioritizing alerts. This allows administrators to quickly assess which incidents require immediate attention, eliminating the need to sift through hundreds of notifications daily.

Without a centralized security approach, critical alerts can easily be overlooked, potentially leading to data breaches. In sectors like healthcare and media, every hour of delay can result in significant financial and reputational losses. By implementing a unified system like Security Hub, you eliminate fragmented information and gain a comprehensive view of your entire cloud infrastructure.

1 Gap = millions in losses

- 40% of data breaches involved multi-cloud environments (IBM, 2024)
- Delayed response = data leakage or service interruption
- Medtech/Mediatech: every minute matters

Rapid problem resolution through automation

The key advantage of AWS Security Hub is its ability to launch corrective actions automatically.

When the tool detects suspicious activity, it can trigger the necessary procedures - such as cutting off access to specific resources or running a script in AWS Lambda to restore proper firewall rules. The Neoncube team emphasizes that automation reduces human error and speeds up incident response. In projects requiring continuous uptime - like live broadcast - every minute counts.

> Combined with regular framework updates and the elimination of technical debt, you can substantially lower the risk of outages.
>
> **Jakub Mrowiec**
> Co-Founder and Full-Stack Engineer at Neoncube

To fully leverage the power of Security Hub, be sure to integrate it with other AWS services such as AWS Config, Amazon Macie (for sensitive data protection), and Amazon Inspector (for vulnerability scanning). This multi-layered approach allows you to detect and address a wide range of issues, from configuration

Proactive > Reactive

AWS Security Hub is not just a tool - it's a mindset:

- → **You react before an incident happens**
- → **You reduce human error**
- → **You maintain system resilience while scaling rapidly**

Embrace Proactive Defenseautomation

Implementing AWS Security Hub moves you toward a proactive defense strategy - rather than waiting for an attack to occur, you can quickly respond to any suspicious activity. Regular security audits, automated alerts, and framework updates help maintain stability in even the most complex cloud environments.

If you're in an industry where service interruptions can lead to significant losses, adding AWS Security Hub to your infrastructure is a wise choice. Consult with experts, plan your deployment, and leverage automation to lighten the load on your IT team. This approach will not only enhance resilience against outages but also give you confidence that your resources remain secure, even under the most dynamic conditions.

Sources

1. IBM, Cost of a Data Breach Report 2024, https://www.ibm.com/reports/data-breach

Best practices for cloud security: Which steps should you take to protect your data in the cloud?

According to a report by The Business Research Company, the healthcare cloud computing market is set for rapid growth, projected to reach US$89.11 billion by 2029, with a compound annual growth rate (CAGR) of 18.2%. Similarly, the global broadcast and medical technology market is expected to grow to USD 99.12 billion by 2029, at a CAGR of 13.1%

However, despite this growth, many companies still overlook the critical need to strengthen data protection - particularly as new legal requirements and escalating incident costs come into play. In this article, we explore proven cloud security practices, drawing on industry experiences and the insights of teams who have successfully implemented AWS in their projects.

Understanding the challenge

According to Gartner's Information Security Spending Through 2028 report, global information security spending is forecast to grow at an average annual rate of 11.7% between 2023 and 2028, reflecting the growing scale of data protection challenges. With the growing popularity of public cloud computing, companies are often faced with the need to secure sensitive information - medical, financial, or authored digital content.

What does the data say – where are companies failing?

Too few companies are implementing good practice (UK Gov, 2024)

75% - have firewalls
72% - enforce strong passwords
Only 39% use 2FA
Only 34% implement updates up to 14 days

Failing to recognize configuration gaps in the cloud can result in losing customer trust and incurring significant costs. The case study "Mission: How using AWS improves teamwork in Medtech?" confirms that modernizing your cloud architecture must go hand in hand with implementing measures to limit the risk of cyberattacks.

> However, our experience from the Radpoint project, for example, shows that the implementation of AI-based tools has reduced diagnostic times for medical images by up to 30%, resulting in smoother radiology sessions and a significant reduction in the risk of downtime during critical examinations.
>
> **Paweł Gołda**
> Co-Founder and Full-Stack Engineer at Neoncube

Key steps for cloud security

1. **Multi-factor authentication (MFA)**
Even at the login stage, it's worth introducing mandatory MFA to block attacks that rely on stolen passwords. Neoncube (2024) notes that AWS Identity and Access Management (IAM) allows you to assign roles and permissions precisely, limiting access only to necessary resources.

2. **Data encryption at rest and in transit**
In healthcare environments, encryption is crucial - AWS KMS (Key Management Service) helps secure patient data in line with HIPAA, while in Mediatech, it protects content from unauthorized use.

3. **Continuous monitoring and support**
The ITV project showed that ongoing application monitoring using tools like Amazon CloudWatch is essential. Around-the-clock support teams also accelerate incident response and lower downtime costs.

2. **Regular updates and audits**
Ignoring technical debt in long-term projects leads to outdated libraries and greater vulnerability. Neoncube's strategy includes periodic (every two years) reviews of framework versions, preventing the buildup of security gaps.

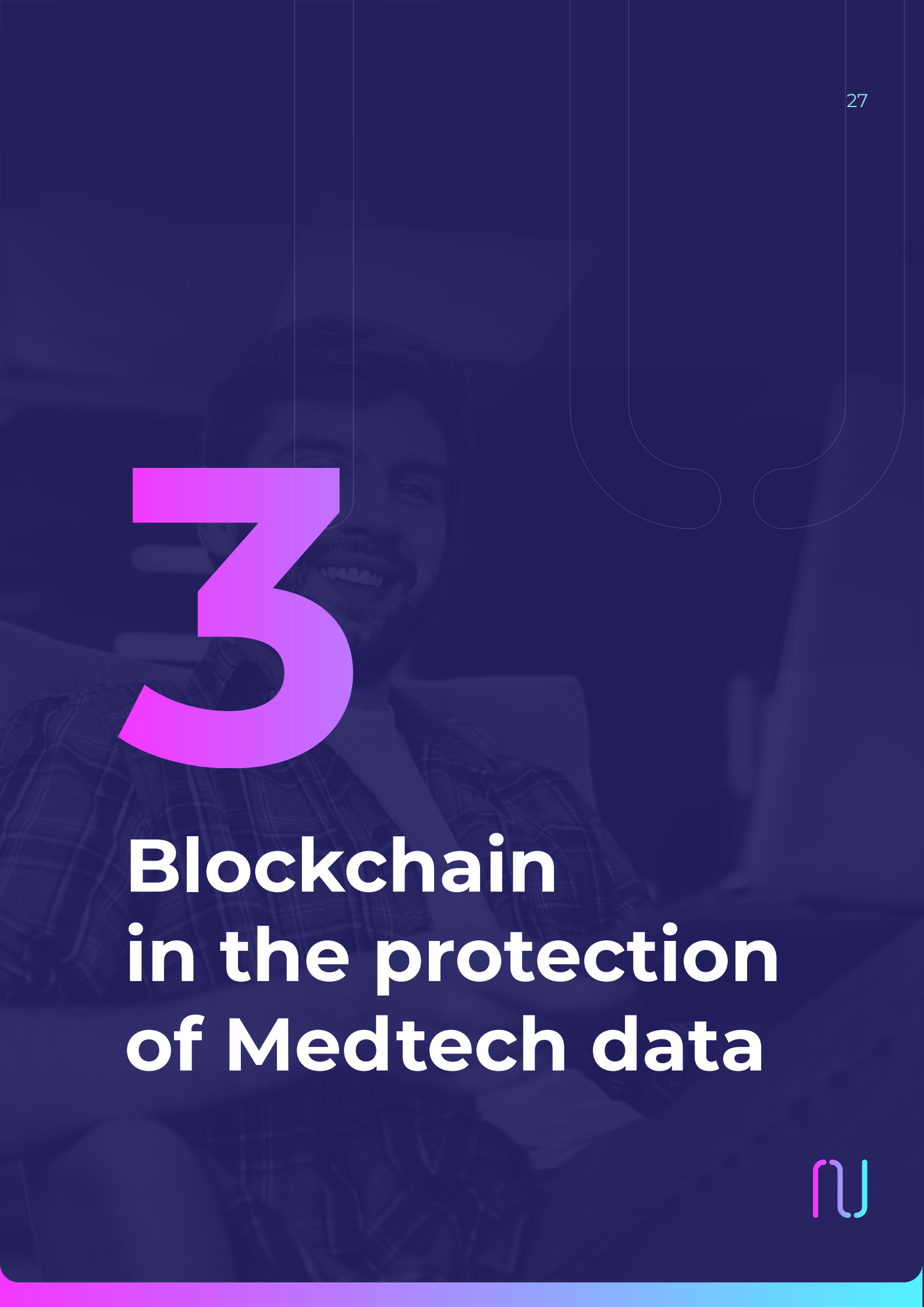
A layered approach

Effective data protection in the cloud involves far more than installing a firewall. A layered strategy is key, encompassing MFA, encryption, monitoring, and audits. Because Medtech and Mediatech often process highly sensitive information, specialized procedures and solutions are essential for meeting stringent legal requirements and avoiding costly disruptions.

If you want to avoid financial and reputational damage, then consider putting the above advice into practice. Prepare an implementation plan, starting with permission verification, integration of monitoring tools and team training. Remember that investing in security earlier today means less risk in the future - and that, in turn, increases customer confidence and growth stability.

Sources

1. The Business Research Company, Broadcast And Media Technology Global Market Report 2025, https://www.thebusinessresearchcompany.com/report/broadcast-and-media-technology-global-market-report
2. The Business Research Company, The Business Research Company, https://www.thebusinessresearchcompany.com/report/healthcare-cloud-computing-global-market-report
3. Gartner, Information security forecast: What to expect through 2028, https://www.gartner.com/en/articles/information-security
4. Cyber security breaches survey 2024, https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024



3

Blockchain in the protection of Medtech data

3.1

Regulatory landscape and technology response

Blockchain in the protection of Medtech data

Blockchain in medtech: how to reconcile data immutability with RODO and new EU regulations?

Aleksander Góra
Teranode Group

Aleksander Góra is a senior technology strategist and venture builder focused on turning emerging technologies into business opportunities. As Head of Identity & Digital Trust, he leads strategy, development, and commercial growth, driving the adoption of privacy-preserving credential ecosystems across regulated industries.

Previously, Aleksander shaped decentralized solutions for enterprise and government clients at a blockchain technology company and led product experience design and IoT data-driven initiatives at a major facilities management firm in UK. His work focuses on building commercially viable ventures that bridge emerging technologies, business models, and customer needs.

If you ask me, this moment is a pivot point: We have the technology, the standards, and now the regulatory mandate. Organizations that move first to operationalize decentralized identity will define the new rules of healthcare interaction – while everyone else tries to catch up later.

Teranode Group

Teranode Group is a global group of 18 startup companies active in the blockchain space since 2015. We expertise in delivering innovative, blockchain-based solutions for enterprise clients. Our expertise spans fintech, digital trust, supply-chain, data integrity and entertainment services – each designed to enhance operational efficiency and reduce costs.

By leveraging blockchain technology, we enable secure, transparent, and scalable solutions that foster growth and success for our customers.

Teranode

When considering blockchain in medtech, one must start with the reality that European regulations – especially the General Data Protection Regulation (GDPR) – are designed to protect individuals' rights first, and technology must adapt around that. Health information is classified under GDPR as "sensitive personal data", requiring the highest standard of care. This presents an immediate tension: blockchain is built for immutability; GDPR, however, demands that personal data can be erased.

GDPR vs. blockchain: a conflict of philosophies

From my experience leading projects in decentralized identity and data compliance, I can say that misunderstanding this tension often leads to critical design mistakes. One of the most common is assuming that encrypting personal data before putting it on a blockchain solves the GDPR problem. It does not.

Under GDPR, there is a clear and vital distinction:

- Anonymised data – data that can never, by any means, be linked back to an individual – falls outside GDPR's reach.
- Pseudonymised data – where re-identification remains possible, even if difficult (such as via encryption) – remains fully under GDPR.

Encryption, while valuable, does not make data anonymous. If decryption keys are lost or stolen, the data can again be linked to an individual. Thus, encrypted personal data on a blockchain is still a GDPR liability – and worse, it's on an immutable network where deletion is extremely difficult.

How to design in compliance with regulations? Practical off-chain approach + cryptographic hash

The correct architectural principle is clear: no personal data, even encrypted, should be placed directly on a blockchain. Instead:

1. The original personal data must be stored off-chain, in controlled environments (e.g., secure cloud storage).
2. Only a cryptographic hash – a unique fingerprint of the data – should be placed on-chain.
3. Proof of data integrity: If the off-chain data is altered, its hash changes, and tampering is immediately detectable.
4. GDPR compliance: If a user exercises their right to erasure, the off-chain data can be deleted. The hash left on-chain, without a file it points to, becomes meaningless and no longer concerns GDPR.
5. Preservation of blockchain's strengths: Transparency, auditability, and security remain intact.

Beyond regulatory compliance, these architectures unlock new possibilities for trusted data sharing, patient-driven research, and cross-border digital health services – laying the groundwork for a more dynamic and patient-centric healthcare ecosystem.

What are the European institutions saying? Legal status and regulatory sandboxes

European regulators are aware of the potential of blockchain, but they are equally aware of the risks. A 2018 European Parliament resolution, reaffirmed in 2020, encouraged blockchain exploration in healthcare – provided that patient rights, especially data protection, are fully respected. European health authorities, including the European Medicines Agency, have not yet issued blockchain-specific regulations, but existing rules around data integrity, auditability, and patient safety are highly relevant.

The EU is also taking proactive steps to foster compliant innovation. Notably:

- The ***European Blockchain Regulatory Sandbox*** will allow live testing of healthcare blockchain applications in collaboration with regulators.
- The ***European Blockchain Services Infrastructure (EBSI)*** is setting the groundwork for trusted cross-border digital services, including identity verification.

eIDAS 2.0 and digital identity: a new foundation for medtech solutions

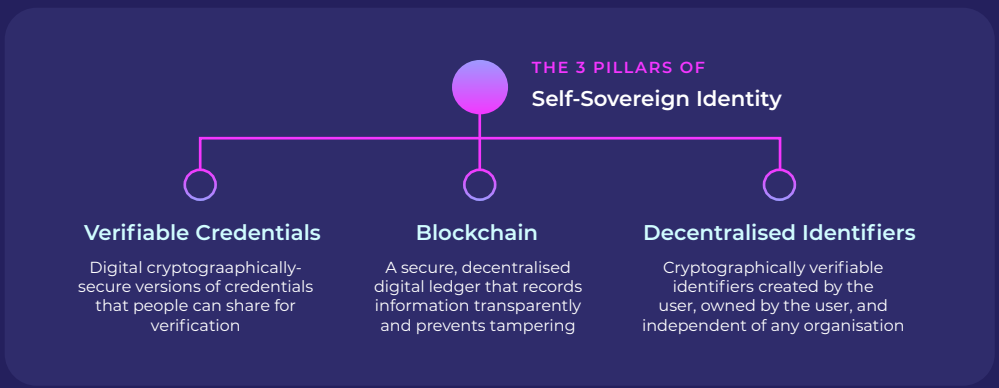
The upcoming eIDAS 2.0 regulation will formalize the legal status of digital wallets and verifiable credentials – a major step for self-sovereign identity in health contexts.

In this context, the forthcoming eIDAS 2.0 regulation represents a particularly important development. Building on the original European framework for digital trust services, eIDAS 2.0 introduces the concept of European Digital Identity Wallets, enabling individuals and organizations to manage and share verified identity attributes securely across the EU.

Significantly, it embeds two global open standards – Verifiable Credentials (VCs) and Decentralized Identifiers (DIDs), developed by the W3C – into European law for the first time. These standards are fundamental for enabling decentralized models of identity, where users can control their data without relying on centralized authorities. To support this ecosystem, eIDAS 2.0 also establishes the framework for trusted registries, allowing verification of credential issuers in a secure and standardized way. Although the regulation itself does not explicitly mandate the use of blockchain, the majority of real-world implementations are based on Distributed Ledger Technology (DLT) to ensure transparency, auditability, and decentralization at scale.
In my view, eIDAS 2.0 marks a genuine shift: decentralized identity solutions based on DLT and open global standards now have a clear regulatory pathway across Europe.

Decentralised Identity VS Self-Sovereign Identity

Self-Sovereign Identity (SSI) is a form of Decentralised Identity that enables individuals to fully control their digital identity, managing crenentials without relying on a central authority or service provider.



For medtech companies, this creates a major opportunity to rethink how patient consent, credential verification, and cross-border health data sharing can be implemented with trust, privacy, and compliance embedded from the ground up. For example, patients could carry verified prescriptions, clinical trial participation proofs, or vaccination records securely in their digital wallets – enabling safer, faster, and more transparent interactions across the health ecosystem.

Critically, the regulation sets clear timelines: by the end of 2026, all EU Member States must offer a Digital Identity Wallet to their citizens, and by the end of 2027, all public sector services will be required to accept these wallets for authentication and credential exchange. Decentralized identity will soon move from an emerging innovation to a core infrastructure for interacting with both public and private digital services across the European Union.

The risks of mismanaging patient data are not theoretical

We have already seen significant GDPR penalties – including a €400,000 fine for a Portuguese hospital aover poor access controls. Blockchain, properly applied, can reduce such risks: for example, Estonia's national e-Health system uses blockchain to create immutable access logs for health records, without ever placing medical data on-chain. Every access attempt is recorded transparently, giving patients and auditors full oversight while protecting confidentiality. In summary, blockchain, if architected correctly, can be a powerful compliance tool – and a catalyst for trusted innovation in healthcare.

Aleksander Góra
Senior Technology Strategist and Venture Builder

As regulators create new frameworks like the European Health Data Space, the companies that act early – embracing privacy-by-design architectures and trusted digital identity – will not only ensure compliance but position themselves as leaders in shaping the next generation of digital health innovation across Europe.

However, this depends on strict adherence to privacy-by-design principles:

1. Off-chain storage of sensitive data
2. On-chain hashes only
3. Consent management embedded in system architecture
4. Clear boundaries between what is governed by GDPR and what is not

Technology Foundations: Blockchain, Digital Identity, and Verifiable Credentials

Before exploring specific use cases, it is critical to first understand the foundational technologies enabling a new era of trust in healthcare: Blockchain, Verifiable Credentials (VCs), and Decentralized Identifiers (DIDs).

Blockchain: Enabling Trust, Transparency, and Data Integrity

> Traditional databases allow records to be written, edited, and deleted. Blockchain restricts operations to just writing and reading. Once a record is written to the blockchain, it becomes immutable – it cannot be altered or erased without detection.
>
> **Aleksander Góra**

Blockchain should be seen not merely as a technical innovation, but as a new class of database designed for environments where trust, transparency, and data integrity are critical – yet where parties may not fully trust each other. In healthcare where proof of what happened – and when – is vital, this immutability is a powerful asset. It transforms blockchain into a single source of truth shared across hospitals, manufacturers, regulators, and patients.

In my experience, this brings three major advantages:

1. **Streamlining operations:** Events can trigger smart contracts, automating service approvals or compliance checks.
2. **Enhancing auditability:** Every action leaves a permanent, tamper-evident trace.
3. **Improving resilience:** Distributed networks eliminate single points of failure and make unauthorized changes easy to detect.

Major European initiatives such as the **European Blockchain Services Infrastructure (EBSI)** have highlighted blockchain's ability to:

- **Ready-made components and platforms (PaaS, SaaS) allow functions to be implemented without writing them from scratch.**
- **CI/CD automation speeds up the testing, deployment and updating of applications.**
- **The lack of infrastructure constraints allows teams to focus on the product rather than the servers.**

Crucially, and as discussed earlier, **blockchain's immutability can be fully GDPR-compliant even on public networks**, if personal data is kept off-chain and only cryptographic proofs (hashes) are recorded on-chain. Modern blockchain solutions are increasingly designed to integrate with existing enterprise applications through API-first architectures. This allows organizations to enhance trust, auditability, and data integrity without needing to rebuild their core systems from scratch – a critical consideration for regulated sectors like healthcare. In practical terms, blockchain acts as a tamper-proof digital logbook, shared across stakeholders. Each recorded event – whether a device audit trail, a clinical trial milestone, or a hashed consent receipt – becomes independently verifiable, strengthening compliance and collaboration without relying on intermediaries,

In my experience, blockchain, when properly architected, offers the healthcare sector far more than secure data storage: it provides a foundation for building entirely new, trusted digital ecosystems across organizational and national boundaries.

Beyond Data: Why Digital Identity Matters

Healthcare is not just about transactions; it is about people – patients, doctors, nurses, insurers, researchers.

To fully unlock blockchain's potential, we need a trusted, portable, and verifiable way to manage identities. In a fragmented healthcare ecosystem, ensuring that a professional credential or a patient's consent is authentic, current, and verifiable without unnecessary friction is a critical need.
This is where Self-Sovereign Identity (SSI) enters the picture.

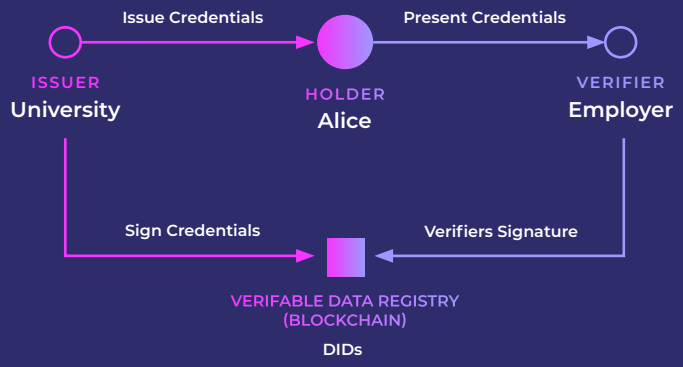
Here's how it works in simple terms:

- **Issuers** – trusted organizations like medical councils, universities, health authorities – create Verifiable Credentials (VCs).
- **Holders** – doctors, patients, researchers – store these credentials in secure digital wallets.
- **Verifiers** – employers, hospitals, insurers – validate them without ever having to call the issuer again.

Self-Sovereign Identity: Trust at the Identity Level

Blockchain gives us data integrity. But in healthcare, real transformation only happens when we solve trust at the identity level too – who the data belongs to, who is accessing it, and under what rights.
This is where Self-Sovereign Identity (SSI) comes in – and in my view, it's one of the most misunderstood, and most powerful, shifts now happening under the surface.
At its core, SSI addresses three problems that healthcare – and most regulated industries – struggle with every day:

- **Efficiency:** Allowing individuals to prove who they are and what they hold, without going through intermediaries each time.
- **Privacy:** Enabling verifiers to check documents' authenticity without the issuer knowing – which radically reduces data exposure and surveillance risk.
- **Compliance:** Embedding the principles behind GDPR and eIDAS 2.0 – user control, data minimization, portability – into the architecture itself, not just the legal paperwork.



Critically, each party anchors its presence using **Decentralized Identifiers (DIDs)** – unique references on a blockchain that prove control over an identity without exposing private data.

A DID is just a secure pointer – think of it like a verified username that anyone can trust, but that doesn't leak personal information by default

In my experience, when you deploy this properly, three things happen immediately:

1.

First, the friction disappears. A medical professional moving between hospitals can onboard in seconds, not days – credentials are presented and verified instantly.

2.

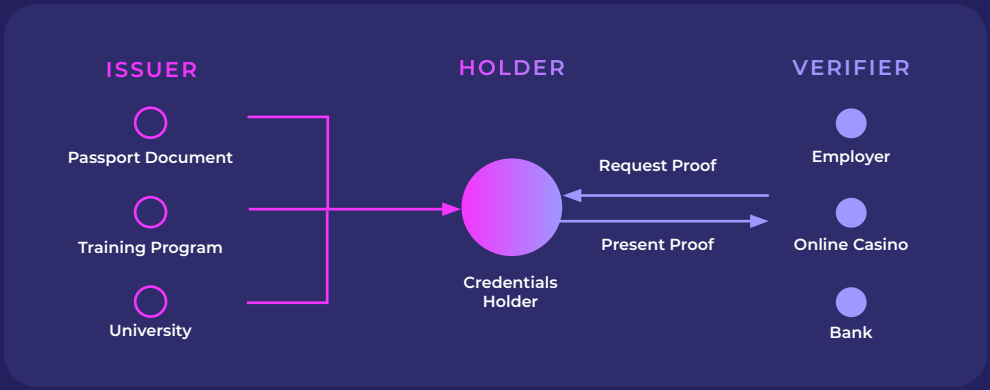
Second, privacy protection becomes real. The issuer doesn't know where the credential is being checked. The verifier doesn't need to ask the issuer anything. The holder controls everything.

3.

Third, compliance shifts from defensive to proactive. You're not scrambling to bolt GDPR or eIDAS compliance onto systems – you're building it into the foundation, with verifiable records, auditability, and user control as defaults.

What is Decentralised Identity

A type of identity management that allows people to control their own digital identity without depending on a specific service provider.



Operational gains are just the beginning - there's a major opportunity that deserves more attention: Verifiable credentials aren't just a compliance cost. They're an asset.

When you issue a credential that's trusted and portable, you create opportunities for new services, new monetization models, new loyalty ecosystems – built around verified, reusable trust.

This is no longer theoretical. The global standards – Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) – are finalized by the W3C. And in Europe, eIDAS 2.0 has formally endorsed them, giving SSI a clear legal runway across all member states.

If you ask me, this moment is a pivot point:

We have the technology, the standards, and now the regulatory mandate. Organizations that move first to operationalize decentralized identity will define the new rules of healthcare interaction – while everyone else tries to catch up later.

Use Case: Patient Identity and Consent Management

One of the clearest areas where blockchain and decentralized identity can deliver immediate impact in healthcare is putting patients back in control of their own data.

Today, consent management is fundamentally broken:

- Patients rarely know where their data flows, what they've agreed to, or how to revoke permissions later.
- Consent forms are often paper-based, fragmented across IT systems, or missing altogether.
- Meanwhile, every new provider interaction demands fresh identity checks, repeated document uploads, and manual data sharing – frustrating for patients, costly for providers.

In my view, this broken consent architecture is one of the biggest roadblocks to trust and efficiency in digital healthcare.

The Opportunity: A Patient-Centric Consent and Identity System

With blockchain and Self-Sovereign Identity (SSI), we have the opportunity to flip the model entirely:

- Each patient holds a **digital identity wallet.**
- **Verifiable credentials** issued by trusted authorities (e.g., national health services, hospitals) represent the patient's identity, insurance coverage, and consents.
- When accessing a new service, the patient presents these credentials directly.
- **Verification happens instantly** – checking cryptographic signatures and DIDs anchored on blockchain – without the hospital needing to photocopy IDs or chase paperwork.

Consent, too, becomes a living digital asset:

- After a consultation, a patient signs a digital consent credential that specifies what data, for what purpose, for how long.
- The consent is stored in the patient's wallet, with a proof recorded on blockchain.
- If the patient changes their mind, they can revoke consent with a tap – instantly updating the record across the system.

This is not theoretical. Projects like PharmaLedger have already demonstrated clinical trial eConsent systems where every version of a patient's consent is auditable, tamper-evident, and user-controlled.

Aleksander Góra
Senior Technology Strategist and Venture Builder

Use Case:
Patient Identity and Consent Management

Why This Matters: Efficiency, Privacy, Compliance

Efficiency improves mmediately:

- **Patients no longer re-upload documents or re-sign redundant forms.**
- **Hospitals and clinics eliminate manual identity checks and consent paperwork.**
- **Processes that take hours or days today happen in minutes.**

Privacy is fundamentally strengthened:

- **Verifiers check the authenticity of a credential against blockchain records – without ever contacting the issuer.**
- **The patient shares only the information needed, not their full history.**
- **Issuers remain unaware of when and where credentials are verified, breaking the surveillance cycle.**

Compliance becomes proactive:

- **Every data access can be cryptographically tied to a consent record, supporting GDPR's requirements for demonstrable consent.**
- **Revocations, expirations, and updates are traceable in real time – providing an automatic audit trail for regulators.**

As European Union experts have noted, blockchain's auditability makes it uniquely well-suited to solving GDPR's consent tracking challenges – not by trying to control systems after the fact, but by **building compliance into the data infrastructure itself.**

How It Looks in Practice: A Poland-Specific Perspective

Poland is already well-positioned to take advantage of blockchain and Self-Sovereign Identity (SSI) in healthcare. With the widespread use of Profil Zaufany, mObywatel, and the Internetowe Konto Pacjenta (IKP) platform, Polish citizens already have trusted digital identity and access to their health records. Building on this foundation, the next step could be to empower patients to control and share their medical data dynamically through verifiable credentials:

- Every citizen could be issued a patient digital ID credential – linked to their PESEL and authenticated via existing tools like Profil Zaufany or mObywatel.
- Each medical encounter (e.g., doctor visit, hospital admission, lab test) would generate health data credentials – encrypted summaries like discharge reports or lab results – stored under the patient's control.
- When a new provider, researcher, or insurer needs access, the patient would digitally consent through their health wallet, specifying exactly what data, for what purpose, and for how long access is granted.

Importantly, the data itself could still be transferred securely via APIs integrated with the national P1 platform – but the permission to access and the proof of consent would be immutably logged on a blockchain layer.

This architecture would bring several immediate advantages:

- Patients would gain clear visibility over who accessed their records, and when.
- Providers would have instant, verifiable confirmation of consent before accessing data.
- Auditors could trust that no data was accessed or used without legitimate patient authorization.

Other countries like Estonia have shown that blockchain-backed e-health systems work. In Estonia, patients can actively monitor and restrict access to their data, with blockchain providing an immutable audit trail that protects against internal abuse or system tampering.

Poland could follow a similar path – without needing to rebuild the existing P1 system – by layering patient-driven consent control and verifiable record integrity over the digital health services that already exist.

In my view, this is not a distant vision. Given Poland's strong digital ID adoption and relatively centralized e-health infrastructure, piloting a blockchain + SSI consent system – perhaps starting with research consents or cross-hospital data sharing – would be a realistic and high-impact next step.

Business Value for Healthcare Providers

1. **Reduced administrative burden:** Automating identity verification and consent collection saves time, money, and reduces errors.
2. **Lower legal risk:** With immutable, verifiable consent records, the threat of non-compliance penalties is drastically reduced.
3. **Improved user experience:** Patients engage more easily when onboarding is fast, permissions are transparent, and trust is built into every interaction.

Analyses show that integrating blockchain into EHR systems for consent management could reduce administrative overhead to the bare minimum, freeing up clinical resources for patient care. More strategically, a healthcare provider offering patients clear, controllable access to their data is positioning itself as a trusted digital health brand – essential for long-term adoption and competitive advantage.

Final Thought: Why This Is the Smart Starting Point

In my view, patient identity and consent management is the natural entry point for healthcare organizations exploring blockchain and SSI.

- It solves real, visible pain points for both patients and providers.
- It enhances privacy and compliance – without challenging core medical processes.
- It can be deployed incrementally alongside existing systems.
- It builds digital trust at a time when patient confidence is critical.

Early movers here won't just improve internal efficiency – they will define the new trust expectations for healthcare in the digital era.

To implement sovereign data management in healthcare, we must take a pragmatic approach. The goal is not binary ownership, but shared stewardship. Patients remain in control of their data – while trusted institutions like hospitals and clinics act as responsible partners.

Access should be default where necessary, revocable at will, and auditable at all times. This ensures that medical teams can respond quickly in emergencies, without compromising patient oversight and authority.

This model – balancing privacy with operational reality – positions Self-Sovereign Identity (SSI) as a foundational framework for restoring trust in digital healthcare.

Use Case: Interoperability and Trustworthiness of Medical Documentation

In healthcare today, data needs to move, but trust struggles to follow.

Medical information is spread across hospital systems, labs, imaging centers, personal health apps, and national health databases. When records need to cross organizational or national boundaries – for referrals, treatment, billing, or research – providers face two chronic problems:

- Interoperability: Data exists in different formats, databases, and standards, making access complex and error-prone.
- Trustworthiness: How can the receiving party be sure that the information is complete, current, and unaltered?

Without solving these two challenges, digital health remains fragmented, expensive, and vulnerable to fraud. In my view, tackling data interoperability and trust is one of the most valuable – and achievable – blockchain opportunities in healthcare.

The Opportunity: A Tamper-Proof Medical Information Layer

Blockchain enables healthcare systems to create a unified, tamper-proof reference layer for medical documentation.

1. Every time a medical document is created (e.g., a lab report, discharge summary, imaging result), a hash – a digital fingerprint – is generated.

2. This hash is recorded immutably on a distributed ledger shared across participating healthcare providers.

3. The actual medical data stays within each institution's system (off-chain) – but its authenticity and existence are now provable by all authorized parties.

Consent, too, becomes a living digital asset:

- **That a document exists,**
- **That it hasn't been modified since creation,**
- **When and by whom it was registered.**

Hospital A can confirm that Hospital B's discharge summary for a patient is legitimate – without relying solely on B's internal systems. If any tampering occurs – even subtle – the discrepancy with the blockchain record will reveal it immediately.

Use Case: Interoperability and Trustworthiness of Medical Documentation

Why This Matters: Efficiency, Trust, Compliance

Efficiency

- Blockchain becomes a neutral trust layer across systems.
- Providers don't have to fully harmonize their internal EHRs or APIs – they simply anchor document references on the ledger, enabling faster discovery, validation, and secure sharing.

Trust

- Data integrity is independently verifiable, without needing to trust the sending institution or a centralized intermediary.
- Forgery, tampering, and data loss become much harder to conceal.

Compliance

- Regulators can access immutable logs proving when documents were created, modified, or accessed.
- In clinical trials, device maintenance, or adverse event reporting, this reduces legal exposure and strengthens audit outcomes.

How It Works in Practice

Imagine a patient journey across multiple hospitals:

1. **Hospital A generates a diagnosis and records a blockchain reference.**
2. **Hospital B, months later, treats the same patient. Before relying on Hospital A's report, B requests the document, hashes it locally, and checks that the hash matches the blockchain record.**
3. **If it matches, B can trust the record. If not, there's immediate red flag.**

All without forcing hospitals to adopt identical EHR systems or centralize all patient records.

> In a European context, where cross-border health information exchange is a priority, blockchain can complement emerging standards (like the European EHR Exchange Format, HL7 FHIR, DICOM) by adding verifiable trust without creating new privacy risks.
>
> **Aleksander Góra**

Rather than building a giant, centralized health database – which introduces new governance challenges – blockchain enables a federated model, where each institution retains data locally but contributes to a shared trust fabric.

Examples from Real Deployments

Estonia's e-Health system uses blockchain to timestamp and integrity-protect every patient record and access log. Auditors can easily verify whether any unauthorized viewing or alteration occurred – without accessing the underlying patient data.

PharmaLedger demonstrated a Digital Trust Ecosystem where pharmaceutical data, IoT device readings, and clinical trial records could be immutably logged across multiple organizations. Importantly, PharmaLedger showed how blockchain could integrate with legacy standards like HL7, DICOM, and GS1 – enhancing interoperability rather than replacing existing systems.

Use Case: Interoperability and Trustworthiness of Medical Documentation

Examples from Real Deployments

Estonia's e-Health system uses blockchain to timestamp and integrity-protect every patient record and access log. Auditors can easily verify whether any unauthorized viewing or alteration occurred – without accessing the underlying patient data.

PharmaLedger demonstrated a Digital Trust Ecosystem where pharmaceutical data, IoT device readings, and clinical trial records could be immutably logged across multiple organizations. Importantly, PharmaLedger showed how blockchain could integrate with legacy standards like HL7, DICOM, and GS1 – enhancing interoperability rather than replacing existing systems.

These projects prove that blockchain's role isn't to store healthcare data – it's to ***make healthcare data trustworthy and interoperable across systems and borders.***

Business Value for Healthcare Providers and Medtech Firms

1. **Reduced reconciliation costs:** Shared ledgers eliminate disputes over what data was sent, received, or modified.
2. **Stronger cybersecurity:** Even if one hospital's internal system is compromised, blockchain records provide an immutable recovery path.
3. **Simplified compliance audits:** Immutable evidence trails for data handling reduce the time and complexity of regulatory inspections.
4. **Better patient experience:** Patients can more easily share their medical history without carrying paper records or CDs – and know the data is authentic and intact.

For medtech firms, particularly those managing medical device data, diagnostics, or compliance documentation under the EU Medical Device Regulation, blockchain offers a powerful tool to prove traceability, integrity, and transparency – attributes increasingly demanded by both regulators and customers.

Final Thought: Why This Is the Smart Starting Point

From my perspective, investing in blockchain to enhance interoperability and trustworthiness is not just a defensive play (compliance and cybersecurity) – it's a strategic enabler.

Healthcare organizations that can move data securely and confidently across internal and external boundaries will be able to deliver better patient outcomes, faster innovation, and more trusted partnerships.

Blockchain doesn't replace health IT systems – it upgrades trust between them.

And in a future of borderless, digital health ecosystems, trust will be the ultimate currency.

Use Case: Transparency and Accessibility of Clinical Trials

In clinical trials, trust is everything – between researchers, regulators, participants, and the public.

Trials generate enormous volumes of critical data:

- Who enrolled, when. What procedures were performed. What results were recorded.
- Any breakdown in integrity – whether intentional or accidental – puts patient safety, regulatory approvals, and public confidence at risk.

Yet today's clinical trial processes are riddled with friction:

- Trial protocols evolve, requiring frequent re-consents.
- Data is collected across decentralized sites and contract research organizations (CROs).
- Cases of data fraud, selective reporting, or delayed transparency are still too common.

In my view, blockchain and decentralized identity offer a unique opportunity to modernize how trials manage consent, protect data integrity, and ensure continuous transparency.

How It Works in Practice

At enrollment, participants receive a **verifiable credential** representing their consent to the study protocol.

- If the protocol changes, a new consent request is issued to their SSI wallet.
- If accepted, a new credential is minted, linked to the updated protocol version.

During the trial, key events – enrollment, randomization, adverse event reports, data lock points – are **timestamped on blockchain.**

- Any attempt to alter data after the fact would leave a clear mismatch against the ledger.
- Regulators could monitor trial conduct in near real-time, rather than waiting for end-of-study audits.

The Opportunity: End-to-End Trust for Trial Data and Consent

Blockchain enables clinical trials to build an **immutable, verifiable audit trai**l for:

1. **Patient consent management** – including re-consents over time.
2. **Data integrity** – timestamping each critical step from enrollment to results.
3. **Transparency** – giving authorized stakeholders real-time visibility into trial progress.

When combined with **Self-Sovereign Identity (SSI),** participants can control their consent credentials dynamically – accepting new protocol changes, revoking permissions, and tracking how their contributions are used. This transforms trials from opaque, fragmented systems into **transparent, participant-centered ecosystems.**

For transparency, stakeholders like ethics committees or regulatory authorities can be given permissioned access to a live node – receiving continuous updates, not just static reports. PharmaLedger's pilot projects demonstrated exactly these concepts:

Secure trial data collection, dynamic eConsent updates, tamper-evident patient-reported outcomes – all integrated into existing trial workflows without adding friction.

Why This Matters: Efficiency, Trust, Compliance

Efficiency

- Blockchain reduces manual data reconciliation between sites, CROs, and sponsors.
- Consent updates happen digitally, cutting paperwork and re-verification cycles.

Transparency

- Participants, regulators, and even the public (where appropriate) can trace the lifecycle of a trial – when data was collected, by whom, and under what consent.

Compliance

- GDPR, EU Clinical Trials Regulation, and growing public demands for open data all push toward provable consent and data authenticity.
- Blockchain provides a ready-made infrastructure for demonstrating compliance.

In simple terms: You can't just say you followed the rules – you can prove it automatically.

Business Value for Sponsors and Medtech Firms

1. **Reduced regulatory risk:** Immutable proof of compliance reduces audit findings, speeding time to approval.
2. **Operational efficiency:** Less reconciliation between trial sites and central databases; smoother inspections.
3. **Enhanced public trust:** Transparency practices differentiate sponsors in an era of rising scrutiny and demand for open science.
4. **Patient empowerment:** By managing their own consent lifecycle, participants become more engaged, loyal, and ethically protected.

There's also potential competitive advantage: Faster audits and cleaner regulatory submissions can get life-saving therapies to market sooner – creating real commercial impact.

Final Thought: Why Trials are the Natural Next Step

In my experience, clinical trials are one of the most compelling places to apply blockchain and SSI today.

- The processes are already well-defined but complex.
- The regulatory pressures are intensifying around transparency and patient rights.
- The value of real, verifiable trust is enormous – for both operational efficiency and brand reputation.

Using blockchain and decentralized identity, clinical trials can shift from „trust me" to „trust the system itself."

And that, in the future of healthcare innovation, could be the ultimate differentiator.

4

Cloud-based AI and ML

4.1

AI in medical diagnostics

Cloud-based AI and ML

Mission: AI in modern radiology, the Radpoint project

Michał Smoliński
Co-founder Neoncube
Co-founder and CTO at Radpoint

Michał is transforming the field of radiology through cloud technologies and artificial intelligence. With over 20 years of experience in building software systems, the past decade has been focused on healthcare and medical imaging. Michał is responsible for product development, system architecture, and leading the technology team at Radpoint. He is also the co-creator of a SaaS platform used by 43% of radiologists in Poland, a solution that significantly enhances everyday diagnostic practice.

Every new technology emerges from a need for change, but it is artificial intelligence (AI) that is truly redefining modern medicine. The integration of AI into radiology is not just transforming how patients are diagnosed; it's also accelerating the process and enhancing the precision of analyses. The Radpoint project stands as a prime example of how cutting-edge technology is revolutionizing medical diagnostics. Together, we've built a system that not only speeds up diagnoses but also improves their accuracy and overall quality.

R

Need: We want to shorten the time spent on the diagnostic process and reduce the risk of mistakes.

Solution: Implementation of AI into the system supporting the diagnostic process of radiologists.

Read full article

From Pilot to Practice: How to Enable Scalable AI Adoption in Public Healthcare

Jakub Chwećko

Founder of the Medical Innovation Institute, which supports the development of medical innovations and their implementation into the healthcare ecosystem. Medical director of the Ancillary Division of the Children's Hospital in Dziekonów Leśny. Physician and expert with extensive experience in healthcare innovation, medical technology and artificial intelligence. He co-founded the Network of Innovator Doctors, Supreme Chamber of Physicians (NIL IN). His main area of interest is creating an innovation ecosystem in healthcare, supporting medical startups, public-private partnerships, innovation development and pilot implementation. He has worked in leadership positions at EIT Health InnoStars, uPacjenta, Infermedica, Roche Diabetes Care Germany, K.I.D.S. Foundation, among others.

Michał Jeska

Chief Growth Officer (CGO) and co-founder of the Medical Innovation Institute (MII), committed to advancing healthcare innovation and transforming patient outcomes. He has over a decade of experience spanning startups, corporate leadership and academia. His specialty is creating strategies that bring together research, technology and market needs to deliver scalable and impactful solutions. At MII, he's on a mission to shape the future of the medtech and biotech industry by: Executing growth strategies to scale innovation. Building partnerships and fostering collaboration in the CEE healthcare ecosystem. Supporting the acceleration of startups, optimising healthcare processes and developing breakthrough R&D projects.

Medical Innovation Institute (MII)

medical innovation institute

Medical Innovation Institute (MII) is a consulting company specialising in the development, commercialisation and implementation of medical and technological innovations in healthcare. We support startups, research institutions and medical institutions in implementing R&D projects, raising funding and optimising clinical and business processes. We bring together the worlds of technology and medicine to create solutions with a real impact on the quality of healthcare and the efficiency of the healthcare system.

In recent years, healthcare systems around the world have seen a dramatic increase in the development and availability of AI-powered tools. Yet, one crucial question remains: how can we ensure these solutions are not only tested, but successfully adopted and scaled across public hospitals? At the Medical Innovation Institute (MII), we recently addressed this question in our white paper dedicated to AI and HealthTech pilot projects in Polish hospitals. The report examines 10 real-world implementations - from AI-powered ECG interpretation to clinical decision support tools - and distills practical lessons that apply far beyond the Polish context. This article summarizes key insights from that work, offering a practical roadmap for public healthcare institutions, innovators, and policymakers interested in turning small-scale pilots into sustainable, system-wide solutions.

The Pilot is Not the Goal - It's the Entry Point

Too often, pilot programs are treated as a success in themselves. But real transformation starts when the pilot ends. What we've observed is that the best pilot projects are not just about demonstrating that a technology works - they're about testing whether the conditions for adoption exist: technical readiness, clinical workflow integration, regulatory alignment, and stakeholder buy-in.

For example, one startup successfully implemented its AI diagnostic tool in a children's hospital by co-developing the implementation plan with clinicians and ensuring that medical staff were not just passive recipients, but active contributors. Another focused on embedding their AI service into the hospital's IT infrastructure from day one, avoiding the risk of creating yet another disconnected tool.

Michał Jeska
CGO and co-founder of the Medical Innovation Institute

Barriers Are Predictable - And Surmountable

Our research identified five recurring challenges across pilot implementations:

1. Lack of clear ownership on the hospital side
2. Absence of clinical workflow integration
3. Long and fragmented procurement procedures
4. Uncertainty about legal and ethical compliance
5. Limited financial capacity to sustain the solution post-pilot

Each of these can be anticipated and addressed. Successful pilots include early legal and IT consultations, pre-pilot workflow mapping, and ongoing stakeholder communication. In one case, an AI tool for radiology triage was paired with training sessions and simulation testing, significantly improving clinician trust and usability.

Recommendations for Public Hospitals

To move from pilot to practice, hospitals must rethink how they approach innovation. Based on the 10 case studies we analyzed, we propose the following actionable recommendations:

- Designate an innovation lead or unit responsible for new technology implementation.
- Prioritize long-term value over short-term results when assessing pilot outcomes.
- Include IT, legal, and procurement teams early in the process - not just after the pilot ends.
- Co-create implementation plans with startups and include frontline clinicians from the beginning.
- Document and share best practices internally to scale success across departments or locations.

A European Perspective

Although our report focuses on Poland, its findings are highly relevant across the EU. Public healthcare systems throughout the continent face similar tensions: the desire to innovate, and the inertia of legacy structures. The European Health Data Space and the AI Act are now shaping a common regulatory ground. But true innovation will come from practice-based learning - where hospitals become innovation partners, not just users. That's why we advocate for more structured piloting frameworks, greater visibility of successful projects, and shared platforms for cross-border collaboration.

Looking Ahead

If we want to build a future-ready healthcare system, we must move beyond isolated experiments. Pilot projects are a vital first step - but their true value lies in how we use them to create lasting, system-level change.

By connecting startups with hospitals, co-creating implementation roadmaps, and building trust in AI, we can enable the scalable, responsible, and impactful use of new technologies in public healthcare.
The future of AI in medicine is not just about what's possible - it's about what's adopted.

How AI Models Can Support Physicians in Diagnosing Diseases

Paweł Paczuski
Co-founder and CEO of upmedic

A company that specialises in providing intelligent software for structured medical documentation. His experience in IT and passion for innovation has allowed him to develop tools that significantly improve the work of doctors, reducing the time needed to create documentation by up to sixteen times. Thanks to numerous implementations, upmedic is currently used by thousands of doctors across Europe, and more than one million examination descriptions have already been created using the software.

Physicians are only human, and under pressure, mistakes can occur. By analyzing millions of historical medical cases, AI can point out the most likely diagnoses and help clinicians avoid common errors.

upmedic

upmedic is a platform that uses artificial intelligence to streamline the creation of medical records. It automates the process of creating descriptions of diagnostic imaging examinations, helping doctors create precise and consistent analyses of examination results. By integrating with the IT systems of healthcare facilities, it improves data flow and increases the efficiency of medical staff. It is a modern solution supporting the digitalisation of the healthcare sector.

upmedic

How can AI models support doctors in diagnosing diseases?

Artificial intelligence is increasingly making its way into the field of medicine, transforming the way physicians diagnose diseases and make treatment decisions. With the help of advanced algorithms, AI can process vast amounts of clinical data, detect patterns, and assist medical professionals in their everyday tasks. This doesn't mean machines will replace doctors, but rather, they can become invaluable assistants, improving diagnostic precision and enhancing the efficiency of patient care. However, does theory align with practice in this case?

The Most Accurate Analysis

Every day, physicians review hundreds of diagnostic results – from X-ray images to complex blood tests. AI systems can analyze these datasets much faster than any human, identifying subtle changes in imaging studies or atypical values in lab results. This ability allows for the early detection of serious conditions, such as cancers or neurological disorders. Some diseases are so rare or complex that their diagnosis requires a detailed review of symptoms and patient history.

By leveraging extensive medical databases, AI can offer suggestions for potential diagnoses and recommend further tests. This kind of assistance is particularly valuable when dealing with rare diseases, which might otherwise be missed without access to comprehensive information.

Accurate Diagnoses and Reduced Human Error

Physicians are only human, and under pressure, mistakes can occur. By analyzing millions of historical medical cases, AI can point out the most likely diagnoses and help clinicians avoid common errors. This doesn't imply that doctors should blindly follow AI suggestions, but rather, these insights should serve as an additional tool to guide their clinical judgment. AI is designed to support physicians, not replace them.

upmedic – Intelligent Support for Healthcare Professionals

> Modern technologies like upmedic assist physicians not only in diagnosing but also in efficiently managing medical documentation. By automating and streamlining the reporting process with AI, upmedic allows for faster and more intuitive generation of clinical reports. This enables healthcare professionals to spend less time on paperwork and more time with their patients.
>
> **Paweł Paczulski**

This is a perfect example of how technology can enhance routine medical tasks. No matter how detailed the analysis provided by AI may be, the most immediate benefit for a physician is the reduction in time spent on accurate and compliant documentation.

Challenges and the Future of AI in Diagnostics

Despite its tremendous potential, the use of AI in healthcare still faces several challenges. Ensuring transparency, establishing robust oversight mechanisms, and maintaining high-quality data are essential. Patient privacy protection and clear regulatory frameworks for the use of AI in diagnostics are also crucial.

The future of AI in medicine looks promising. As technology continues to evolve and becomes more seamlessly integrated into daily clinical practice, physicians will increasingly rely on these modern tools to provide more accurate diagnoses and deliver higher-quality patient care.

Practical decision support algorithms and AI in patient monitoring and diagnosis

Adam Konka

Chairman of the AI Expert Team at RIG Katowice
Member of the Medtech and Biotech Expert Team at RIG Katowice

Adam Konka, MBA, has over 25 years of experience managing comprehensive projects across various management positions. His expertise spans roles such as coordinator, manager, executive director, research and implementation director, as well as serving on committees and as chairman for research and development initiatives. He has held positions as a director, board member, and president of the board. Adam is an expert in healthcare management and has served as an advisor to the Minister of Health of the Republic of Poland. His projects have

RIG

The Chamber of Commerce and Industry in Katowice was established by 103 founders on February 13, 1990 and registered on March 21, 1990. It is an organization of economic self-government bringing together business entities engaged in economic activity. The Chamber has legal personality under the Act of May 30, 1989 on Chambers of Commerce (Journal of Laws 35/89, item 195) and its own Statute. CCI is a continuation of the tradition of the Chamber of Commerce established in Katowice in 1922, and since 1927 the Silesian Chamber of Industry and Commerce – operating until 1950.

RIG CHAMBER OF COMMERCE AND INDUSTRY IN KATOWICE

Artificial intelligence (AI) solutions are making significant strides in the field of medicine, offering valuable support to doctors in monitoring patient health and making accurate diagnostic decisions. Key research projects such as Nomed-AF, DeepRhythmAI by MedicAlgorithmics, and the VCAST system illustrate how AI can enhance the quality of medical care. In this article, we explore the practical applications of these technologies and review the results of studies confirming their effectiveness.

Nomed-AF: Early detection of silent atrial fibrillation

This innovative project developed a special waistcoat for long-term ECG monitoring, designed to record heart signals over a 30-day period. Advanced AI tools were then employed to analyze the ECG data and identify cardiac arrhythmias. A core component of this solution was the Comarch Medical Analysis Platform (CMAP), which leverages machine learning algorithms to process

The Nomed-AF project, funded by the NCBIR STRATEGMED II programme, focuses on the early detection of silent atrial fibrillation (AF) in Polish patients aged 65 and older. Silent AF is one of the most common heart rhythm disorders and increases the risk of stroke by up to five times. CMAP analyzes ECG readings to identify significant episodes of cardiac arrhythmia, helping doctors make faster and more accurate diagnoses. The Nomed-AF project, aimed at detecting silent atrial fibrillation in patients over 65, was a collaborative effort involving several key partners: Silesian Medical Technology Park Kardio-Med Silesia, the project leader, who coordinated the R&D activities; Comarch Healthcare, the technology provider responsible for the ECG data analysis platform and telemedicine solutions; ITAM Institute of Medical Technology and Equipment (now part of the Łukasiewicz Research Network), which contributed to the design and implementation of the medical technologies; and academic partners such as Gdansk Medical University, Pomeranian Medical University in Szczecin, Warsaw Medical University, and Jagiellonian University - Collegium Medicum. The project has been approved by the Bioethics Committee, and all participants provided informed consent to take part.

Nomed-AF study results: the scale of the problem is greater than thought

The Nomed-AF study revealed that the prevalence of atrial fibrillation (AF) is far higher than previously estimated. Among the 3,014 participants, the study found that:

19.2% of patients suffer from AF, which is twice as high as previously estimated for the Polish population over the age of 65

Of those with AF, **41%,** were diagnosed with silent or asymptomatic atrial fibrillation

Earlier medical reports had suggested that only **20%** of the population might suffer from this condition

DeepRhythmAI (DRAI)

DeepRhythmAI (DRAI) is an advanced solution designed for autonomous analysis of ECG signals. It leverages deep neural networks, including convolutional neural networks (CNNs) and Transformer models, to detect and classify cardiac arrhythmias with high precision and speed. CNNs, a type of deep neural network, efficiently analyze spatial data such as images or ECG signals.

In the case of DRAI, CNNs are used to identify and classify various heart rhythms, including arrhythmias like atrial fibrillation and ventricular tachycardia. Meanwhile, Transformer models-originally developed for natural language processing-have been adapted to analyze sequential ECG data. Thanks to their ability to capture long-range dependencies within the data, these models enable accurate classification of heart rhythms, even for subtle arrhythmias. DeepRhythmAI was developed based on the clinical trial DRAI MARTINI, which was presented at the ESC Congress 2024, the largest cardiology conference in Europe.

MedicAlgorithmics: AI proving more effective than traditional ECG techniques?

One of the leading companies in the use of decision support algorithms and AI for patient monitoring and diagnosis is MedicAlgorithmics. I want to draw your attention to two of their key systems: DeepRhythmAI (DRAI) and the Virtual Cardiac Stress Test (VCAST).

Details of the DRAI MARTINI study

The aim of the study was to evaluate the effectiveness of the DRAI algorithm in detecting cardiac arrhythmias compared to traditional ECG analysis conducted by technicians. The study included over 14,600 patients who exhibited symptoms indicative of cardiac arrhythmias, such as palpitations, syncope, or dizziness. It compared the results of ECG analysis by DRAI with those generated by ECG technicians.

The conclusions from the DRAI MARTINI study revealed that the DRAI artificial intelligence system made 14 times fewer errors in detecting critical cardiac arrhythmias than ECG technicians. DRAI's sensitivity in detecting critical arrhythmias was 98.6%, compared to 80% for the ECG technicians.

This study confirmed that the DRAI algorithm is more effective than traditional ECG analysis methods conducted by technicians, underscoring its potential to enhance the quality of cardiac diagnostics. The DRAI system has received CE certification, Health Canada license, and FDA 510(k) approval, verifying its compliance with international standards and regulations. It serves as an adjunctive tool in diagnosing ECG recordings for cardiologists.

VCAST (Virtual Cardiac Stress Test)

VCAST (Virtual Cardiac Stress Test) is an innovative, non-invasive diagnostic tool designed to assess the hemodynamic significance of coronary artery stenosis. It utilizes cardiac computed tomography (CT) data to create 3D models of the coronary vessels, which are then analyzed using artificial intelligence (AI) algorithms.

VCAST is particularly valuable in diagnosing coronary artery disease, enabling clinicians to assess patients more accurately and make better-informed therapeutic decisions.

The system was developed based on a clinical trial conducted in collaboration between Medicalgorithmics and the American Heart of Poland Clinics - the largest private network of cardiology departments in Poland. This comparative study of predictive models for coronary stenosis analysis involved 200 patients with suspected coronary artery disease. Its goal was to evaluate the effectiveness of AI algorithms in automatically detecting coronary stenosis using cardiac computed tomography (CT) data.

Currently, VCAST technology has received CE certification, permitting its commercialisation in the European Union. Medicalgorithmics also plans to pursue FDA approval in the United States, which will enable the technology's entry into the

Key features of VCAST:

- **Non-invasive:** VCAST eliminates the need for invasive procedures such as coronary angiography or Fractional Flow Reserve (FFR) measurements. This reduces the risk of complications and lowers diagnostic costs.
- **Speed and efficiency:** VCAST's analysis of CT data is both fast and efficient, providing clinicians with detailed diagnostic information in a short amount of time. This quick turnaround enhances the overall patient care process, allowing for more timely decision-making.
- **Advanced analysis:** the software provides detailed information on blood flow, pressure, and velocity within the coronary vessels, enabling an accurate assessment of the patient's condition.
- **Personalisation:** VCAST offers personalized models of coronary anatomy, enabling clinicians to tailor treatment plans more precisely to individual patient needs.
- **Predicting treatment effects:** The software also allows for the simulation and prediction of revascularization effects, supporting informed

AI as a support, not a replacement for the doctor

As demonstrated by the examples provided, decision-support algorithms and AI solutions are increasingly being integrated into the realm of patient monitoring and diagnosis. However, it's essential to remember that these technologies serve as supportive tools, with the final diagnostic decision always remaining in the hands of the doctor.

It's also important to consider that the development of such tools for the medical sector is subject to numerous regulations, especially concerning medical data. This often requires obtaining approval from the

Sources

1. MedicAlgorytmics, https://www.medicalgorithmics.com/

AI in medical image analysis from capsule endoscopy

Martin Tabakow PhD. Eng.
AI Research and Development Director
at BioCam

A long-time Wrocław University of Technology employee, specializing in medical image processing and analysis. Currently serves as Director of Artificial Intelligence Research and Development at Biocam. Martin's main scientific interests include the application of fuzzy logic techniques and, in his recent work, deep learning methods for medical image analysis. He is the author of numerous scientific publications in this area. Outside of work, Martin is passionate about sports and travel.

Processing, storing and analysing hundreds of thousands of images requires not only high computing power, but also scalability and flexibility – qualities that are ideally suited to the capabilities of cloud computing.

BioCam S.A.

BioCam is a medtech and pettech company developing endoscopic capsules for remote diagnostics of humans and pets' entire gastrointestinal (GI) tract. The technology enables painless, at-home examinations, eliminating the need for hospitalization and anesthesia. BioCam enhances diagnostic speed and accuracy, integrating a capsule, mobile app, and telemedical platform supported by AI algorithms for a comprehensive and accessible healthcare solution. AI algorithms automatically detect pathological changes, supporting physicians in faster and more accurate diagnosis. BioCam offers an affordable, convenient, and effective solution that increases access to preventive screening and improves the overall quality of healthcare.

BIOCAM
CAPSULE ENDOSCOPY

AI in medical image analysis from capsule endoscopy

Capsule endoscopy is a modern, non-invasive diagnostic method transforming gastrointestinal imaging. The procedure involves swallowing a miniature capsule equipped with a camera that captures thousands of images as it naturally passes through the intestines. This enables the detection of abnormalities that are often difficult to identify using traditional techniques, especially in hard-to-reach areas such as the small intestine. As a result, the technology enhances patient comfort and opens new possibilities for the early diagnosis of inflammatory diseases, cancers, and gastrointestinal bleeding.

In recent years, artificial intelligence has become a key enhancement to this method. Machine learning algorithms enable automatic analysis of images generated by endoscopic capsules, significantly reducing the time required to review recordings and improving the detection of pathologies such as polyps, bleeding, or inflammatory lesions. Thanks to AI, more precise, faster, and personalised diagnosis is now possible.

BioCam – AI and cloud-supported technology

BioCam S.A. is developing capsule endoscopy technology that enables non-invasive examination of the entire digestive tract in both humans and animals. The diagnostic process is conducted remotely: the patient swallows a capsule, and data from the device is transmitted to a telemedicine platform, where it is analysed by physicians and proprietary AI algorithms.

A key component of the system is the use of advanced deep learning solutions that support the identification of pathological changes.

Challenges in training AI models

One of the main challenges in implementing deep learning models in medical imaging is the limited availability of large, well-annotated image datasets. Unlike publicly available data (such as facial or object images), capsule endoscopy images are difficult to obtain, both due to patient data protection regulations and the high cost of manual annotation by clinical experts. Furthermore, many existing datasets remain confined to research projects, which hinders the development and validation of machine learning models.

The BioCam solution: synthetic data and self-supervised learning

To overcome the limitations in data availability, we focused on two key areas:

1. **The generation of high-quality synthetic data that reflects the specific characteristics of the gastro-intestinal pathologies under study.**
2. **The development of a dedicated deep learning–based classification model.**

The first challenge was addressed by introducing algorithms for blending and/or locally generating pathological tissue features into images of healthy tissue. To tackle the second challenge, we developed a dedicated classifier, initially trained using a Self-Supervised Learning (SSL) approach.

Martin Tabakow PhD. Eng.
AI Research and Development Director at BioCam

The role of cloud computing in scaling AI

In an era of rapid advancement in artificial intelligence and growing medical datasets, cloud computing has become an indispensable tool in deep learning-based medical imaging.

Capsule endoscopy generates a vast number of images, most depicting healthy tissue, with only a small fraction containing pathological changes. Processing, storing, and analyzing hundreds of thousands of images requires not only substantial computing power but also scalability and flexibility – qualities perfectly matched by cloud computing capabilities.

Thanks to cloud computing infrastructure, it is possible to train advanced deep learning models on massive datasets in parallel, significantly reducing experimentation time and accelerating the integration of AI solutions into clinical practice.

By pre-training the model in Self-Supervised Learning (SSL) mode using cloud resources, BioCam was able to efficiently and securely process as many as 1,151,600 endoscopic images. In contrast, local processing was limited to only 50,000 images.

Improvements in this area, along with the introduction of additional synthetic data solutions, resulted in the best performance on the publicly available capsule endoscopy dataset in the public challenge for predicting gastrointestinal pathology from capsule endoscopy images – Kvasir-Capsule.

4.2

AI in business process optimisation

Cloud-based AI and ML

AI and ML in the Cloud Improve Mediatech and Medtech Automated Decision-Making

Bodislav Dumitru Alexandru
Bodislav & Associates & Global Chairman
- Infinitum Group

Dr. Dumitru Alexandru Bodislav is an economist, businessman, professor, and strategic advisor with over 20 years of experience in macroeconomics, governance, and business innovation. He is a tenured professor and PhD supervisor at the Bucharest University of Economic Studies, Managing Partner at Bodislav & Associates, Global Chairman at Infinitum Group and lead mentor and expert advisor to NATO's DIANA accelerator and the Harvard Business Review Advisory Council. His work spans public policy, artificial intelligence, and corporate strategy, with published research in top-tier journals and international recognition including the „40 under 40" award and the Nicholas Georgescu-Roegen Prize from the Romanian Academy.

Intelligent, cloud-native AI strategies will put organizations in a better position to deliver value, resilience, and sustainable growth as they navigate increasingly complex environments.

For data-intensive sectors like Mediatech and Medtech, the combination of cloud computing, machine learning, and artificial intelligence (AI) signifies a paradigm shift. These industries work in hectic settings where they must deal with enormous amounts of both structured and unstructured data, intricate compliance requirements, and changing patient or user expectations. Data-driven decision-making, operational planning, and resource management can all be greatly improved by intelligent cloud-based AI systems, which are becoming strategic assets.

Bodislav & Associates
Consultancy. Public Affairs. Crisis Management.

AI in Resource Management: From Reactive to Predictive Systems

A key component of performance in both Medtech and Mediatech is effective resource allocation. Large datasets can be quickly and accurately examined by ***specialized AI systems*** to find trends and inefficiencies that might be missed by human analysis. Forecasting hospital bed demand, predicting medical device maintenance cycles, or optimizing staff deployment based on real-time patient loads are all examples of this in the Medtech context. AI may be used in mediatech to forecast bandwidth spikes during content releases or dynamically distribute computational resources for rendering high-resolution videos.

Predictive resource planning is made possible by cloud-based machine learning models that are continuously trained on both historical and real-time data, which minimizes downtime and redundancy**.**

> Furthermore, AI supports prescriptive analytics – not just predicting what will happen, but recommending what should be done. This is especially powerful in large organizations where decision latency can translate into lost revenue or compliance risk.
>
> **Bodislav Dumitru Alexandru**

AI-enabled cloud platforms such as AWS, Azure, and Google Cloud, for example, provide real-time adaptive infrastructure that scales resources according to workload patterns. This further demonstrates how AI is enhancing economic decision-making by examining past data to spot patterns that human analysts might overlook.

AI-Enhanced Planning and Forecasting

AI-driven forecasting tools that highlight their function in simulating policy scenario outcomes and offering ***high-accuracy simulations*** that take into account complex interdependencies – insights directly applicable to corporate planning in regulated industries – are increasingly supporting strategic planning in both Medtech and Mediatech.

AI in Medtech can model the financial impact of a pandemic on the volume of elective procedures or simulate how new regulations would affect product development schedules. AI can be used in mediatech to predict the virality of content, model the effectiveness of advertisements in various market conditions, and schedule production more efficiently. These features are similar to those of the economic modeling applications discussed, in which AI models various economic situations and assesses exogenous factors like geopolitical events.

AI in Data Analysis and Intelligent Automation

By turning unprocessed data into useful insights, AI improves analysis. This includes analyzing genomics, electronic health records, and imaging data in the context of Medtech. Semantic video tagging, audience clustering, and predictive content performance analytics are all made possible by AI in mediatech. AI can process unstructured text, like doctor's notes or viewer feedback, and uncover patterns that rule-based systems are unable to see thanks to its capacity for natural language analysis.

Additionally, ***AI is essential to process automation in big businesses*** and offers a strong basis for comprehending how AI can replace tedious tasks, such as trade optimization, risk assessment, and fraud detection. These capabilities, when applied at the enterprise level, result in intelligent workflows in Mediatech (e.g., automated subtitle generation, rights management, or content quality control) and Medtech (e.g., automated regulatory submissions, claims processing, or patient onboarding).

These use cases highlight the need for AI systems that make consistent, traceable, and data-informed decisions because even minor mistakes in judgment can lead to significant losses.

CASE STUDY

Process Automation in Large Organizations

Consider a multinational Medtech business that has to handle intricate processes like supplier audits, clinical trials, and regulatory paperwork. These procedures are typically time-consuming and prone to bottlenecks. These businesses can free up expert staff for higher-value work by automating repetitive tasks like document classification, anomaly detection in trial data, or regulatory rule-checking by integrating cloud-based RPA (Robotic Process Automation) systems enhanced with AI.

In a similar vein, automation is used to optimize production in a major Mediatech company. Personalized content feeds can be automatically curated and published by AI models that have been trained on user preferences. Speech-to-text engines, metadata tagging, and automated copyright verification increase output speed and accuracy while decreasing manual editing work.

AI systems are able to spot subtle data changes and new trends, providing decision-makers with a crucial window of opportunity to act. Preventing crises before they arise, streamlining processes, and upholding compliance all depend on this early-warning capability.

Conclusion

Operational excellence in Mediatech and Medtech companies is being redefined by cloud-based AI and ML. These technologies, which range from real-time analytics and process automation to intelligent resource planning, offer a basis for ethical, scalable, and agile innovation. As we can see, AI holds promise not only for its technical effectiveness but also for its ***capacity to promote more intelligent, human-centered decision-making.***

Intelligent, cloud-native AI strategies will put organizations in a better position to deliver value, resilience, and sustainable growth as they navigate increasingly complex environments.

4.3

AI and data ethics and privacy

Cloud-based AI and ML

Ethics, privacy and artificial intelligence in health care: challenges and recommendations

Karolina Kornowska
Chief Operating Officer, wZdrowiu,
Coalition for AI and Innovation in Health

Karolina Kornowska serves as the Operational Director of wZdrowiu and the Coalition for AI and Innovation in Health, and as Project Manager at the Polish Hospital Federation. She is the author of the international medical startup report Top Disruptors in Healthcare. Within the Coalition, Karolina co-develops regulatory documents that foster innovation growth in Poland. She also leads the organization of international events-including conferences, reports, podcasts, and training programs-focused on advancing healthcare innovation. Karolina is a regular speaker and moderator at national and international conferences.

AI holds promise not only for its technical effectiveness but also for its capacity to promote more intelligent, human-centered decision-making.

The Coalition for AI and Innovation in Health

The Coalition for AI and Innovation in Health is an initiative dedicated to unlocking the full potential of innovation, including artificial intelligence, in healthcare, and supporting the digital transformation of the sector. Its mission is to shape policies that drive AI and innovation development within the Polish healthcare system, creating an environment that promotes rapid and widespread adoption of the latest AI advancements. The Coalition currently brings together over 150 organizations committed to healthcare innovation in Poland.

In an era of rapid artificial intelligence development, significant challenges arise concerning ethics and data privacy. The healthcare sector, in particular, requires special attention due to the sensitivity of the information it processes when implementing AI systems.

AI Act – European regulation for high-risk systems

In the European Union, the primary document regulating AI is the Artificial Intelligence Act (AI Act). This legislation classifies AI systems used in healthcare as "high-risk", which brings with it several requirements, including a compliance assessment before market introduction, operational transparency, the ability to explain AI-driven decisions, human oversight, and risk management and quality assurance of the data used.

Additionally, the AI Act underscores the importance of adhering to data protection regulations, such as GDPR, as well as ethical standards and fundamental rights. In the healthcare sector, ensuring the security of medical data and maintaining patient trust in AI systems is particularly critical.

The problem of explainability: AI as ‚black box'

One of the ethical problems with the use of AI is the lack of explainability. Many modern AI systems, especially those based on deep learning, function as "black boxes". While they can deliver highly accurate results, the mechanisms behind their decisions remain unclear. As a result, end-users-whether doctors, patients, or health system administrators-are unable to comprehend how the algorithm arrived at a particular conclusion or recommendation.

Clinical practice and the ethics of patient information

"The AI in Clinical Practice White Paper" is a study prepared by the AI and Health Innovation Coalition, offering practical guidance on the use of AI in medicine. The document highlights, in alignment with the revised Code of Medical Ethics, that patients should be informed about the use of AI in their diagnostic and treatment processes, particularly when AI significantly impacts decision-making.

The use of AI does not necessarily require informing the patient, obtaining consent, or recording the information in the patient's record if the AI systems are merely supporting the doctor's activities. What is crucial is assessing the relevance of AI in the diagnostic and therapeutic process.

However, neither extreme should occur: the doctor failing to inform the patient about AI involvement, nor overwhelming the patient with data they do not understand or need. It is important to note that the patient has the right to seek clarification, provided the information is presented in a way they can understand.

This lack of explainability gives rise to several ethical and practical issues, including a lack of trust, auditability, and understanding of the reasoning behind an incorrect decision. Both patients and doctors may be hesitant to rely on algorithmic decisions if they cannot understand the rationale behind them. In healthcare, where people's lives and well-being are at stake, trust is a fundamental pillar of any therapeutic relationship and clinical decision-making.
When an AI system operates opaquely, it becomes challenging to assess its accuracy, identify errors or biases, and ensure that decisions align with clinical and legal standards. Both the AI Act and the White Paper highlight the importance of transparency in AI systems to ensure that end-users can understand and trust them.

Algorithmic bias – a threat to equality in care

Artificial intelligence in healthcare has the potential to enhance the quality of care and address inequalities in access to services. However, numerous studies and research indicate that AI systems can also perpetuate, and even amplify, existing social and structural biases. The issue of algorithmic bias lies in the fact that AI decisions are not inherently neutral-they are shaped by the quality, scope, and representativeness of the data on which the system has been trained.

For example, diagnostic systems may be less effective for ethnic minorities if the training data predominantly reflects the majority population. To mitigate this, it is essential to use diverse and representative datasets, as well as to conduct regular audits to identify and eliminate any biases.

Privacy of personal data – the foundation of trust

One of the most frequently raised ethical and legal concerns regarding the use of artificial intelligence in healthcare is the issue of privacy and data security. AI systems, particularly those based on machine learning, rely on vast amounts of data to function effectively-data that may include medical, genetic, behavioral, or demographic information. This data is highly sensitive, and its processing carries a significant risk of privacy breaches, which could have serious consequences for patients.

In the context of protecting patients' personal data, it is crucial to implement advanced technical and organizational measures, including data encryption, access control, security audits, regular penetration testing, and ensuring a high level of cybersecurity.

Karolina Kornowska
Chief Operating Officer, wZdrowiu, Coalition for AI and Innovation

Moreover, compliance with data storage and processing regulations is essential, alongside the establishment of proper procedures for handling any potential data security breaches.

Data donation – an ethical pathway to advancing AI in medicine

In the context of medical data, promoting the idea of data donation as good practice is also worth considering. Data donation involves patients voluntarily sharing their medical data for research and development purposes, while ensuring anonymity, the right to revoke consent, and compliance with relevant regulations. This practice can play a crucial role in advancing medical progress, facilitating the development of more accurate and effective AI systems.

Intelligent Solutions for Medtech and Mediatech. Ethics and Data Privacy at the Core of Innovation

Bodislav Dumitru Alexandru Bodislav & Associates & Global Chairman - Infinitum Group

As Artificial Intelligence (AI) and Machine Learning (ML) mature and integrate with cloud computing platforms, their transformative potential becomes increasingly evident across industries. In Medtech and Mediatech, AI is already enhancing diagnostics, content delivery, operational planning, and user personalization. However, these benefits bring with them substantial ethical and data privacy challenges, especially in sectors where trust, compliance, and human well-being are paramount.

Drawing from both current industry practices and theoretical frameworks outlined in the current research, this paper critically examines the ethical dimensions of AI use in Medtech and Mediatech, with a particular focus on data privacy protection in cloud environments.

Ethical Challenges in AI-Driven Medtech and Mediatech Systems

Bias and Fairness in Decision-Making

Algorithmic bias, where AI systems unintentionally reinforce inequalities in their training data, is a major ethical issue in business and advanced research. This can lead to biased diagnostic tools that fail minorities and women in Medtech. A diagnostic AI trained on data from a specific population may misdiagnose people outside that group, compromising patient safety and equity.

Biased recommendation algorithms in Mediatech can reinforce echo chambers, exclude diverse creators, and favor dominant cultural narratives. According to previous research by the same author, AI systems can inherit unintended biases from their training data, resulting in unequal consequences in economic decision-making, especially for disadvantaged groups.

Transparency and Accountability

AI systems, especially those deployed in the cloud at scale, often operate as ***"black boxes"***, producing results without clear explanations. This opacity raises ethical concerns around ***accountability*** in both healthcare and media production. If a Medtech AI misdiagnoses a patient or a Mediatech algorithm promotes harmful content, who is to be held responsible - the developers, the platform, or the organization?

Previous research rightly notes that the transparency and auditability of AI systems must be a priority, calling for "mechanisms that ensure AI-influenced decisions can be examined and justified when necessary." In healthcare, explainable AI (XAI) becomes critical, especially when decisions affect life and death. In media, transparency helps combat misinformation and fosters trust in recommendation systems.

Job Displacement and Social Impact

Human labor displacement is another ethical issue. AI can disrupt the workforce by automating repetitive or complex tasks like medical image analysis and content tagging. While efficiency improves, ethical considerations require ***re- and up-skilling*** employees for inclusive technological transitions.

Retraining programs should be considered to reduce job loss and social inequality. This recommendation supports the ethical obligation to make AI-driven progress ***socially sustainable.***

Ensuring Data Privacy Protection in the Age of AI

Data privacy is a moral issue in Medtech and Mediatech. AI systems use sensitive personal data like health histories and viewing habits to improve performance. These datasets may be exposed to more actors, geographies, and risks in the cloud.

Secure Data Governance and Compliance

AI systems handling financial and economic data must comply with strong privacy and data security regulations. This is especially important in healthcare, where HIPAA and GDPR strictly regulate data access and use.

Cloud security requires encryption, access control, and data residency management. Azure's Confidential Computing and AWS's HIPAA-eligible services are AI-ready infrastructures with compliance frameworks. These let Medtech and Mediatech use AI while complying with privacy laws.

Data Minimization and Differential Privacy

Data minimization, which is collecting only the data needed for specific tasks, and differential privacy, which injects statistical noise into datasets to prevent re-identification, are necessary for ethical AI deployment.

Anonymizing records and applying differential privacy prevents reverse-engineering when training an AI model to detect patterns in patient recovery data. This shows that secured data management is essential for continued trust in AI-based decision-making.

Human-Centric Collaboration with AI

AI should augment, not replace, human judgment. In medical environments, AI can support clinicians in diagnosing complex conditions but should not overrule human expertise without review. In media, AI can streamline editing and personalization but cannot fully understand the cultural nuance or creative context that human producers bring.

> This collaboration between humans and AI leads to more innovative and efficient economic solutions and should be the ethical foundation for AI deployment in sensitive sectors.
>
> **Bodislav Dumitru Alexandru**

Ethical AI by Design

Ethics must be integrated into algorithm development, deployment, and feedback loops for ethical AI implementation. ***AI ethics review boards*** are being established in the Medtech industry to evaluate algorithmic fairness, potential harms, and compliance before tool release. Some Mediatech platforms are adding ***ethical audits*** to their content recommendation pipelines.

AI should be constrained by moral standards and the commitment to the common good, especially in economic and public domains. Developers of cloud-based AI tools must follow ***Ethics Guidelines for Trustworthy AI (EU)*** ***or IEEE's Ethically Aligned Design*** to ensure robust, lawful, and socially aligned AI.

Conclusion

The integration of AI and ML in the cloud holds immense potential for revolutionizing both Medtech and Mediatech. However, these intelligent solutions must be deployed with careful attention to ethics and data privacy. From algorithmic fairness and transparency to secure data governance and human oversight, ethical considerations must guide the design, implementation, and evolution of AI systems.

AI must serve the public good, and its adoption should be constrained by both regulatory frameworks and moral imperatives. In doing so, we ensure that intelligent systems not only enhance performance but also foster trust, inclusion, and long-term sustainability in our most human-centered industries.

4.4

AI and ML in content personalisation at Mediatech

Cloud-based AI and ML

How AI and ML personalises content in real time – and what's in it for your business?

Jacek Nosal Co-founder & Full Stack-Engineer at Neoncube

One thing matters: relevance. Thanks to artificial intelligence and machine learning algorithms, platforms such as Spotify and Netflix can predict what a user wants before they even think of it. Well-implemented recommendation systems increase engagement, loyalty, and sales - and today, they are not just available to the giants. See how they work and what they can do for your business.

Personalization = competitive advantage

Users today expect technology to 'understand' them – offering only the content that truly interests them. Instead of searching through catalogues, they want tailored suggestions: music, films, articles, products. Personalization is becoming one of the most important competitive advantages in the digital world.
Behind this mechanism are sophisticated recommendation systems based on artificial intelligence (AI) and machine learning (ML). When well-designed and properly implemented, they become not just an add-on to the platform - but a key element of the user retention, sales, and loyalty strategy.

Key types of recommendation algorithms

Today's recommender systems use a number of techniques - often in combination - to increase the precision and relevance of their proposals. Here are the most important approaches:

Collaborative Filtering (CF)
A foundational method in recommendation systems. Algorithms analyze the behavior of other users - such as listening history, clicks, or ratings - and suggest content based on similarities. It works particularly well when there's a large user base and extensive historical data.

Neural Collaborative Filtering (NCF)
An advanced evolution of CF that incorporates neural networks. It captures deeper, more nuanced relationships between users and content, boosting relevance, especially when data is sparse or inconsistent.

Wide & Deep Learning
This hybrid method combines linear (wide) and deep (non-linear) models. It leverages both straightforward correlations - like gender influencing music preference - and complex behavioral patterns. Especially powerful in data-rich environments with

Content-Based Filtering (CBF)
This technique focuses on the attributes of the content itself - for example, video length, article author, music genre, or tags. Recommendations are generated based on what the user has previously liked and what resembles it.

Natural Language Processing (NLP)
By analyzing language in reviews, descriptions, comments, or ratings, algorithms can understand not just what users choose, but why. NLP enables emotion classification, tone analysis, and opinion segmentation.

Transfer Learning
This approach reuses pre-trained models for new tasks. For instance, a model trained to detect emotions in text can be repurposed to personalize content descriptions or refine recommendation accuracy.

Migration to the cloud – costs and ROI. Does the cloud optimise costs?

How the big ones do it: Spotify, Netflix and others

Spotify combines multiple algorithmic approaches to maximize the relevance of its recommendations. Among the technologies it uses are:

- **Matrix Factorization (MF)** - uncovers hidden patterns in user behaviour data.
- **Neural Collaborative Filtering (NCF)** - improves matching accuracy through neural networks.
- **Wide & Deep Learning** - connects contextual information (like location, time of day, or device) with user actions.
- **Graph-Based Methods** - treats users and tracks as a network of relationships from which preferences are inferred.
- **NLP** - analyzes song descriptions, reviews, and tags to extract meaning.

Netflix relies on similar strategies. It uses deep learning and NLP to predict which titles are most likely to appeal to a specific user profile. Its algorithms even consider fine-grained signals - such as when a viewer stops watching a series or which artwork draws their eye.

What does business gain?

Recommendation systems aren't just a convenience for users - they are a real increase in business value. Here are the key benefits:

1. **Greater engagement – users spend more time on the platform.**
2. **Higher conversion rate – more clicks, purchases or interactions.**
3. **Better use of data – the system learns with every user action.**
4. **Decrease in rejection rate (churn) – users return because they feel the offer is ‚tailor-made'.**
5. **Opportunities to monetise personalisation – e.g. through dynamic recommendations in e-commerce, media or education.**

Summary

Well-implemented AI and ML algorithms can transform how users perceive a platform - from generic to truly personalized. But the key to success lies not only in the technology itself, but in how it's implemented: iteratively, based on data, and supported by a flexible, cloud-based infrastructure. This is where recommendation systems can scale, learn, and respond - in real time. And for businesses? It's a chance to build an advantage that competitors can't replicate with a single click.

AI, cloud and content optimisation – voice search 2025

Paweł Gołda

Co-founder and Full-Stack Engineer at Neoncube

One of the six co-founders of Neoncube - a technology company born from the desire to create high-quality projects: free from corporate constraints, built on trust in the team, and grounded in responsibility for the product. He has been programming for over 20 years and finds the greatest satisfaction in long-term collaborations, where he can align his skills with the real needs of the client. At Neoncube, he is responsible for system architecture and the development of high-availability solutions - particularly in the fields of Mediatech and Medtech.

Voice search is no longer the future - it's the present. In 2025, users expect instant and relevant answers, and technologies like natural language processing (NLP), artificial intelligence, and cloud computing form the backbone of modern digital experiences. Companies that want to stay visible in a world led by voice assistants must understand the new rules of optimization - and act on them.

Why has voice search become so important?

With over a billion voice queries each month and a rising number of devices equipped with assistants like Alexa, Siri, and Google Assistant, it's clear that users prefer speaking over typing. Most of these queries now come from mobile devices - which means content has to be fast, concise, and context-aware. In 2025, it's no longer just about keywords - it's about intent and conversation.

AI, cloud and content optimisation – voice search 2025

Key elements of voice search optimisation (VSO)

Optimizing content for voice search calls for a fresh approach - one that feels more human, yet is fully supported by technology:

Natural Language Processing (NLP)
NLP enables devices to understand language nuances. It helps voice systems grasp context, recognize intent, and differentiate between phrases like “I’ll have a coffee please” and “where to get the best coffee in the area”.

Keyword and phrase research
Tools like Google Trends, Keyword Planner, or Ahrefs reveal the most common voice-style queries, often in the form of questions: “Where to buy concert tickets?”, “What to have for lunch today?”

Intention-based content
Content can’t be generic. It must respond clearly and efficiently to specific user questions. This makes FAQ sections, microcontent, and rich snippets more important than ever.

Entity-based optimisation
In voice search, specific entities - brands, places, organizations - play a central role. Voice systems map this data to better interpret and respond to queries.

Question-based structure
Instead of generic keywords, content should be structured around real user questions: “How do I get to...?”, “When is open...?”, “Which restaurant serves a vegan breakfast?”.

Mobility and efficiency
Voice searches happen on mobile - so page speed, responsiveness, and user experience are critical if we want voice assistants to prioritise our content.

The cloud as the foundation of effective voice search

Voice search is not just about the frontend. Behind the seamless user experience lies an infrastructure that operates in real time, scales with query volume, and integrates with machine learning algorithms. This is where the cloud plays a crucial role.

What is the significance of cloud computing?

- Real-time data processing and analysis - thanks to the cloud, thousands of queries can be processed simultaneously with minimal latency.
- Integration with AI/NLP - language models and voice assistants (e.g., Amazon Lex, Google Dialogflow) are developed and deployed within cloud environments.
- Scalability - companies can handle seasonal spikes in demand without risking slowdowns.
- Security and RODO compliance - cloud platforms provide encryption, access control, and auditing mechanisms, essential for protecting voice data.

What next?

As technology evolves, voice search will become even more integrated with AI, blockchain, and IoT. It’s no longer just about having a presence in voice search – it’s about how well your company can be heard there.

Voice + AI + Cloud = competitive advantage

In 2025, voice search is more than just a way to find a restaurant. It serves as a communication channel, sales support, and a valuable source of data on user intent. Companies that invest in cloud infrastructure, understand the importance of NLP, and create content that answers real questions will be able to:

- **attract users faster than the competition,**
- **offer a more tailored customer experience,**
- **build trust through immediate, relevant responses.**

5

Cloud scalability

5.1

Challenges facing the start-up

Cloud scalability

Don’t build an MVP in the blind. What does a startup really need to survive the first few months?

Kuba Nagórski

President of the Silesian Startup Foundation

Kuba supports startups at various stages of development - from idea, through MVP, to scaling and overseas expansion. As CEO of the Silesian Startup Foundation, he connects local talent with global opportunities, fostering an environment where innovation meets real business. Kuba Nagórski specializes in building growth strategies, linking teams with investors, and forging international partnerships. While actively developing the Silesian innovation ecosystem, his insights and network reach far beyond the region’s borders.

Want to build an MVP in the cloud without blowing your budget? Instead of asking, “Who’s going to do it for me?”, ask yourself: “Do I know why I’m doing it and what I want to test?” Then, choose a partner who can help you achieve those goals.

Silesian Startup Foundation

Silesian Startup Foundation was established to strengthen the foundations of the startup ecosystem. We help startups develop ideas and turn them into successful businesses. We connect young entrepreneurs with experienced business and investors. We create a space for representatives of different backgrounds, including representatives of local authorities, scientists or students who are just at the beginning of their career path to collaborate on innovative ideas.

silesian startup foundation

Don’t build an MVP in the blind. What does a startup really need to survive the first few months?

An MVP (Minimum Viable Product) is your ticket into the game. But building it thoughtfully is much harder than it sounds. Having worked with dozens of founders - and being one myself - I’ve seen recurring mistakes and risks that can bury a great idea before it even reaches the market.

Business vs. technology - conflict of interest at the core

The most common division of roles is between the technology founder and the business founder. The former knows the code but not the market, while the latter understands the market but not the code. Each faces different risks:

- **The technology founder** builds the MVP using the technology they know – which may not be the best fit for the product.
- **The business founder** doesn’t fully understand what is being outsourced and may overpay for unnecessary development and features.

Cheap and fast – the best way to start

Building an MVP is about validation - confirming there’s real demand. That’s why, as a first step, it’s better to focus on:

- low-code / no-code (even if you have to rewrite it later anyway),
- rapid prototypes,
- testing with real users rather than at conferences.

If an investor doesn’t see a working MVP, they are increasingly unlikely to engage. Even the simplest proof that something works and can be shown to a client means more than a polished presentation.

Mentoring instead of coding

Before spending your first development budget, invest in conversations with experts. Validation isn’t just “does anyone want this?” but also involves:

- → **market analysis,**
- → **competitive analysis,**
- → **business model,**
- → **way of go-to-market.**

MVP in the cloud – because it’s all about speed and being ready for growth

A cloud-based MVP gives you an advantage:

- speed of launch and deployment of subsequent versions, thanks to a ready-made infrastructure,
- automatic scaling with an increase in the number of users,
- data security and backups that are standard with large providers,
- time savings for the technology team, which doesn’t have to manage servers and infrastructure.

External technology partner or in-house team?

At the initial stage, it’s usually better to work with a technology partner – such as a software house. What matters is that the partner:

- **has experience with start-ups,** not just corporates,
- **understands the product in business terms,** not just in technical terms,
- **is open to handing over control of the technology in the future** (e.g. by transitioning the technical lead to an internal team).

> Should the MVP be cloud-based? In my experience: yes. The cloud saves time, and adaptability matters more than perfection.
>
> **Kuba Nagórski**

Building an in-house team only makes sense once you’ve validated your model and have the resources to support long-term product development.

How to avoid mistakes when building an MVP?

1. **Start by validating the problem,** not the product.

2. **Build a pitch deck and business hypothesis** before outsourcing development.

3. **Hire a technology advisor –** especially if you are an entrepreneur.

4. **Choose a partner who understands startups,** not just code.

The biggest risk?

Over-developed MVPs, overpriced teams, lack of validation, and no real customers - these are the most common reasons startups fail. That’s why it’s better to bet on an agile approach, a strong product team, and scalable architecture. In this context, the cloud isn’t a cost - it’s a safety net and a growth accelerator.

To summarize: An MVP is not a goal - it’s a tool to test whether your idea makes sense. Build it quickly, affordably, and wisely. And if you don’t know something - ask. A good startup isn’t the one that knows everything, but the one that knows when to ask the right people.

Scale smart, not expensive. How does scalability help startups minimise costs?

Jacek Nosal Co-founder & Full Stack-Engineer at Neoncube

Long periods without revenue, investor pressure, and uncertainty about growth direction make managing infrastructure costs critical. But this doesn't mean you have to give up on ambition or growth opportunities. That's why it's important to understand: scalability isn't just about growing -it's also about saving money. Especially when it's built into your product from day one.

What is scalability from a start-up perspective?

Scalability means that your application, product or system:

- works efficiently with 10, 1,000 or 100,000 users,
- doesn't require manual resource adjustments when traffic spikes,
- reduces costs when traffic drops or when you're still in the testing phase.

> A cloud solution is more than just a technology - it's a way of operating that allows you to grow without draining your budget.
>
> **Jacek Nosal**
> Co-founder & Full Stack-Engineer at Neoncube

Why does a scalable infrastructure save money?

You only pay for what you consume

With serverless and cloud solutions (e.g. AWS Lambda, GCP Cloud Functions), you don't have to keep idle servers running. Functions execute only when needed. When your system rests - so does your wallet.

You do not invest upfront

There's no need to buy servers, commit to expensive hosting plans or build a full DevOps team from day one. You can launch with a minimal setup and scale as traction builds. Costs only rise when real users start arriving.

You don't have to predict peaks

Startups rarely know when they'll hit a "viral moment". Traditional infrastructure would require maintaining unused capacity just in case. The cloud scales automatically - up or down - without manual configuration.

Faster testing = faster validation

Scalability also brings flexibility. You can roll out new features quickly, run A/B tests and react to market feedback in real time. That leads to fewer bad decisions - and fewer costly pivots.

Scale smart, not expensive.
How does scalability help startups minimise costs?

What should a startup have on its radar when designing for scalability?

- **Think cloud from the start**, but match the technology to your stage: serverless for MVPs, containers when traffic grows.
- **Design event-driven systems** - they respond better to fluctuations in load.
- **Set up cost monitoring and alerts** - platforms like AWS and GCP allow you to define spending thresholds and receive automatic notifications.
- **Delay building an in-house tech team until the business model is validated** - until then, rely on experienced partners.

Scale up when it's worth it. And only then pay.

Scalability isn't a corporate luxury - it's a survival strategy for startups. It enables testing, validation and growth with minimal financial risk. In a well-architected cloud setup, you can run lean for as long as you need. And when the time comes to scale, you won't have to start from scratch - just scale further.

5.2

Handling live events and high traffic

Cloud scalability

AWS vs GCP for serverless applications in mediatech

Jakub Mrowiec

Co-founder and Chief Technical Solutions Architect at Neoncube

Jakub Mrowiec is one of the six co-founders of Neoncube and serves as the company's chief technical solutions architect. He is responsible for software development, designing cloud architecture and implementing resilient systems - particularly in the Mediatech and Medtech sectors. A programmer for over 20 years, Jakub sees coding not just as a profession, but as a passion. He is known for his analytical mindset, perfectionism and ability to tackle complex challenges. At Neoncube, Jakub makes sure every project is the result of a deliberate, well-thought-out process - never a matter of chance.

Serverless computing is revolutionising how mediatech companies build applications. By removing the need to manage infrastructure, teams can focus entirely on developing functionality and increasing business value. This shift enables faster iteration, greater flexibility, and leaner operations. Among the leaders in this space are AWS Lambda and Google Cloud Functions (GCP). But which platform offers better support for scalability and performance?

The main problem

How do you choose the solution that best supports application development and optimises operational costs and ensures application stability and flexibility, while reducing costs and simplifying infrastructure management?

Effects of implementation AWS Lambda and return on investment:

- **Increase in scalability by 200%**
- **Reduction in operating costs by 25%**
- **Reduction in time to implement new features by 30%**

Read full article

Handling live events: Serverless solutions with Neoncube

Jacek Nosal Co-founder & Full Stack-Engineer at Neoncube

In live broadcasting, every second of delay can mean lost viewers and revenue. Managing traffic during such events is one of the biggest technological challenges. Traditional infrastructures often struggle with dynamic, unpredictable loads. That's why Neoncube relies on cloud-based architecture - in particular AWS Lambda - to guarantee scalability and reliability during peak demand.

Challenge: Managing dynamic traffic during live events

Live events like sports broadcasts or concerts can generate sudden spikes in user activity - from thousands to millions in seconds. Traditional servers are rarely able to handle such loads without prior planning and manual scaling. Maintaining infrastructure at full capacity just in case leads to significant, often unnecessary, costs when traffic is low.

Solution: Using AWS Lambda

As a serverless platform, AWS Lambda executes functions in direct response to events - such as HTTP requests or database updates. It scales automatically, adjusting to traffic in real time, and only consumes resources when needed. This model ensures cost-efficiency and operational flexibility. A critical component was configuring concurrency limits to ensure a guaranteed number of parallel executions, regardless of limitations in a given AWS region. This allowed Neoncube to maintain uninterrupted operation of key features, even during the highest traffic surges.

Business benefits

1.

Flexibility and scalability
The system automatically adapts to changing workloads, running functions only when they are needed.

2.

Cost-effectiveness
The pay-per-use model enabled a significant reduction in operational expenses by eliminating the costs of idle infrastructure.

3.

Speed of implementation
leveraging AWS's ready-to-use services shortened the time needed to prepare and launch the production environment.

Conclusions

By implementing AWS Lambda, Neoncube successfully managed the demanding traffic of live events, delivering high-quality service while keeping infrastructure costs under control. This case highlights how serverless cloud architecture can effectively address the scalability needs of the Mediatech sector.

Would you like to talk about your project?

Get in touch with us!

Jacek Nosal

Co-founder and Full-Stack Engineer at Neoncube

jacek@neoncu.be