PROCEEDINGS OF SCIENCE

INFN EPIC Cloud: Building ISO/IEC 27001-Certified Secure Cloud Regions for Trustworthy AI and Open Science

Barbara Martelli,[a,*] **Salvatore Aurnia,**[c] **Alessandro Brunengo,**[f] **Patrizia Belluomo,**[c] **Diego Bettoni,**[h] **Stefano Bovina,**[b] **Eleonora Bovo,**[b] **Luca Carbone,**[g] **Renato Carletti,**[b] **Gianpaolo Carlino,**[i] **Daniele Cesini,**[a] **Lorenzo Chiarelli,**[l,a] **Andrea Chierici,**[a] **Alessandro Costantini,**[a] **Domenico D'Antonio, Antonella d'Isidoro,**[b] **Luca dell'Agnello,**[a] **Giacinto Donvito,**[d] **Enrico Pasqualucci,**[b] **Antonio Falabella,**[a] **Nadina Foggetti,**[m,a] **Jacopo Gasparetto,**[a] **Carmen Giuliano,**[a] **Claudio Grandi,**[n] **Valentina Ientile,**[c] **Leandro Lanzi,**[e] **Stefano Longo,**[a] **Vito Manzari,**[d] **Mauro Patano,**[d] **Diego Michelotto,**[a] **Salvatore Monforte,**[c] **Valeria Moretta,**[b] **Carmelo Pellegrino,**[a] **Riccardo Rotondo,**[c] **Luigi Scarponi,**[a] **Attilio Gaetano Sequi,**[b] **Giusy Sergi,**[a] **Francesco Sinisi,**[a] **Vincenzo Spinoso,**[d] **Giuseppe Telesca,**[b] **Alessia Rita Tricomi,**[c] **Veronica Valsecchi,**[b] **Vincenzo Ciaschini,**[a] **Cristina Vistoli,**[a] **Stefano Zani**[a] **and Stefano Zotti**[a]

[a] *INFN CNAF,*
Viale Berti Pichat 6/2, Bologna, Italy
[b] *INFN Central Administration,*
Via Enrico Fermi 40, Frascati, Italy
[c] *INFN Catania,*
Via Santa Sofia 64, Catania, Italy
[d] *INFN Bari,*
Via Orabona 4, Bari, Italy
[e] *INFN Firenze,*
Via Sansone 1, Sesto Fiorentino, Italy
[f] *INFN Genova,*
Via Dodecaneso 33, Genova , Italy
[g] *INFN Milano Bicocca,*
Piazza della Scienza 3, Milano , Italy
[h] *INFN Headquarters,*
Piazza dei Caprettari 70, Roma , Italy
[i] *INFN Napoli,*
Via Cintia, Napoli, Italy
[l] *Consortium GARR*
Via dei Tizii 6, Roma, Italy

[*] Speaker

© Copyright owned by the author(s) under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License (CC BY-NC-ND 4.0) All rights for text and data mining, AI training, and similar technologies for commercial purposes, are reserved. ISSN 1824-8039 . Published by SISSA Medialab.

PoS(ISGC2026)016

[m] *CNR IBIOM,*
Via Amendola, Bari, Italy
[n] *INFN Bologna,*
Via Berti Pichat 6/2, Bologna, Italy
E-mail: bmartell@infn.it

The increasing use of artificial intelligence techniques and data-driven approaches in scientific research, specifically in the realm of the life sciences and healthcare sector, have raised the requirements concerning security, privacy, compliance, and trust in scientific research computing infrastructures. On the other hand, initiatives like the European Open Science Cloud (EOSC) [1], the European Health Data Space (EHDS) [2], and AI Act call for infrastructures that offer both openness and data governance control. This article presents EPIC Cloud (Enhanced PrIvacy and Compliance Cloud), an ISO/IEC 27001 27017 27018 certified [3] secure cloud region of the INFN DataCloud [4] designed to host compliant AI processes and trusted research applications. In this paper, we describe the EPIC Cloud development process toward becoming a multiregion cloud region, including its process-based Information Security Management System, alignment with EOSC and EHDS standards, and how the EPIC Cloud is capable of supporting AI workflows by means of selected European and national use cases. Moreover, we analyze the experience gathered in implementing the first multiregion EPIC Cloud deployment at the INFN data centers of Bologna, Bari, and Catania.

International Symposium on Grids and Clouds (ISGC2026)
15-20, March, 2026
Academia Sinica, Taipei, Taiwan

PoS(ISGC2026)016

1. Introduction

The scientific research infrastructure landscape is witnessing profound transformations driven by cloud computing, big data analysis, and artificial intelligence. On one hand, such technologies offer new possibilities for discovery. At the same time, these technologies introduce strict demands concerning data protection, compliance, transparency, and trustworthiness, especially in life sciences, biomedical research, and technology transfer areas. Initiatives at the EU level such as EOSC, EHDS, and AI Act emphasize the need for infrastructures able to foster open science while providing rigorous guarantees on governance and accountability. INFN has re-engineered its national cloud infrastructure to meet both requirements for openness and compliance. This paper discusses the EPIC Cloud, the certified secure region of INFN DataCloud, designed for regulated and AI-driven research. Sections below describe the INFN DataCloud and EPIC Cloud architecture, the underlying Information Security Management System, and EPIC Cloud integration with EOSC, EHDS, and AI governance frameworks, finishing with use cases and lessons learned.

2. INFN DataCloud and the EPIC Cloud Region

INFN DataCloud is the national cloud infrastructure developed by the Istituto Nazionale di Fisica Nucleare aimed at harmonizing and evolving the Italian distributed computing ecosystem towards the federated cloud-native paradigm. INFN DataCloud builds upon the integration of the Italian WLCG distributed computing infrastructure with cloud technologies developed within European initiatives such as INDIGO-DataCloud [5] – and is now delivered as a unified portfolio of services available via web and CLI interface. Leveraging the composable, scalable, and open-source nature of its technologies, INFN DataCloud is geographically distributed among multiple INFN sites and continually evolving within national and European programs, including NRRP-funded projects.

Among the many components of this ecosystem, EPIC Cloud (Enhanced PrIvacy and Compliance Cloud) stands out as the ISO-certified secure cloud region of INFN DataCloud. EPIC Cloud tackles increasing challenges related to confidentiality, integrity, availability, privacy, regulatory compliance, and data sovereignty. These challenges become crucial when addressing regulated research activities in the life science and biomedical domains. Like the INFN DataCloud, EPIC Cloud delivers IaaS, PaaS, and SaaS services within the Community Cloud model but uses a stricter organizational and governance framework in line with international information security standards. Even though EPIC Cloud is currently deployed as the dedicated secure region, including the INFN datacenters of CNAF (Bologna), Catania, and Bari, it is supported by the same technological stack, operational team, and roles as the entire INFN DataCloud ecosystem, thus making its Information Security Management System easily extendable, as discussed in Section 4. In table 1 are summarized the hadware resources available at present on the three sites.

3. Information Security Management System

EPIC Cloud operates under a formal Information Security Management System (ISMS) aimed at integrating security, privacy, and compliance into the governance and operations of a research

PoS(ISGC2026)016

Site	CPU (cores)	RAM (TB)	Storage (PB)	GPU
Bologna	12500	55	10.5	62
Catania	600		6	0
Bari	1112		3	0

Table 1: Multi-site EPIC Cloud HW resources

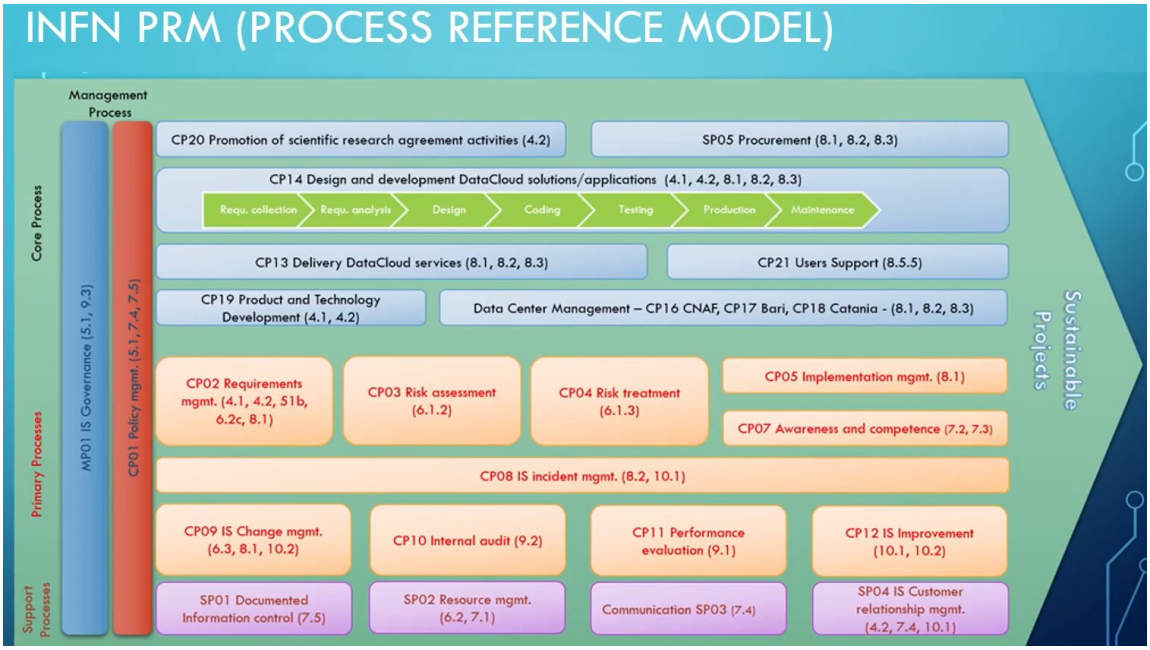

Figure 1: EPIC Cloud Process Reference Model

cloud infrastructure. According to the ISO/IEC 27001 standard, and extended to ISO/IEC 27017 and ISO/IEC 27018, the ISMS governs the entire EPIC Cloud service portfolio, supporting organizational processes and ensuring systematic risk management, accountability, and continuous improvement. **Instead of treating information security as an additional technical layer, the EPIC ISMS uses a process-oriented governance approach**. Security controls are embedded into the operational lifecycle of cloud services, from onboarding to access management, change management, incident handling, and service continuity. Such a practice increases transparency and auditability **without reducing operational flexibility and agility.** As a result, security becomes the enabler of trust and service quality.

3.1 Risk Management and Business Impact Analysis

Risk management in EPIC Cloud is governed by ISO/IEC 27001 and supported by the controls and guidance provided by ISO/IEC 27002. The EPIC Cloud approach is inspired by Enterprise Risk Management (ERM) principles and follows the guidance of ISO 31000, which provides a common framework for managing technical, operational, strategic, and compliance risks. The reference to ISO 31000 reflects the objective of integrating information security risks within a

PoS(ISGC2026)016

broader organizational governance model rather than managing cyber-security risks in isolation. This holistic approach enables the consideration of both threats and opportunities, while supporting alignment between information security, service continuity, compliance, and operational objectives. ISO/IEC 27005 was also considered, as it provides specific guidance for information security risk management within an ISMS. However, the current edition of ISO/IEC 27005:2022 is structurally aligned with ISO 31000 and adopts the same fundamental risk management principles. Consequently, the EPIC Cloud approach remains fully consistent with ISO/IEC 27005 while using ISO 31000 as the overarching reference for risk governance across the entire infrastructure. Risks are identified and evaluated in terms of threats, vulnerabilities, opportunities, and impacts on information assets and services, with particular attention to confidentiality, integrity, availability, privacy, and regulatory requirements relevant to research environments. The results of risk assessments are used to select and implement adequate controls, ensuring proportional and accountable action. All ISMS processes use the continual improvement philosophy based on the PDCA Deming Cycle (Plan-Do-Check-Act) and formalized by the ISO/IEC 27001 standard.

Business Impact Analysis (BIA) supplements this process by estimating the impact of any disruption to EPIC Cloud service operations. It helps identify critical services, recovery objectives, and tolerable downtime to **prioritize the implementation of resilience and continuity measures**. Thus, risk management and BIA provide an operational basis for EPIC Cloud governance.

3.2 Process-Oriented Governance and the Value Chain Model

To make the ISMS practical, EPIC Cloud adopts a process-oriented governance model as depicted in Fig. 1, where information security practices are embedded into the lifecycle of cloud service design, delivery, and operation. Governance is based on documented processes for

- primary activities (e.g., provisioning and operation);
- support activities (e.g., infrastructure management, competency development, and compliance).

This model aligns with Michael E. Porter's value chain concept [6], distinguishing between primary and support activities that contribute to value creation. Security controls are essential to value generation.

Drawing inspiration from ISO/IEC TS 27022 and translating it into a value chain perspective, EPIC Cloud shows explicitly how each security control contributes to service value, efficiency, and trust. By tying security to processes and not to isolated assets, the EPIC Cloud ISMS enhances continuous monitoring and improvement, providing a scalable framework that can be extended across sites and services.

3.3 Support for EOSC and European Data Spaces

While all INFN DataCloud services have been built to be infrastructural blocks that will contribute to EOSC federation, EPIC Cloud concentrates its effort on integrating the specificities of emerging governance requirements of European Data Spaces with the already well-established framework of the EOSC. EOSC FAIR principles and federated access with EOSC-aligned identity and access management have been the starting points for building EPIC Cloud; then additional layers

PoS(ISGC2026)016

have been added, such as security and compliance, for cases where such needs arise. The process-oriented governance approach of EPIC ISMS is compatible with EOSC operational requirements and allows the implementation of appropriate assurance mechanisms for onboarding of projects, access control, and incident handling. In this way, INFN can make its services accessible to EOSC, remain accountable for those services, and at the same time prepare itself for supporting sector-specific data governance models.

3.4 EPIC Cloud and the European Health Data Space

EHDS is directly supported by EPIC Cloud due to its ability to provide secure and publicly governed cloud environments where data can be securely used as part of innovation processes. EHDS governance model assumes the use of **Health Data Access Bodies** and such criteria as **purpose limitation**, **traceability**, and **accountability** that are implemented by means of the EPIC Clouds certified ISMS and a controlled execution environment which imposes stringent log management rules, formal appointment and registration of System Administrators, signature of Non-Disclosure Agreements when needed, and clear assignments of roles and responsibilities following the *segregation of duties* principle. Health data can be processed within secure cloud-based research environments, minimizing the necessity of data transfers to avoid data leaks. Fine-grained access control, federated identity management, and logging will ensure full transparency and auditability across the entire process, allowing cross-border research aligned with EHDS requirements. As EHDS becomes increasingly dependent on artificial intelligence, having proper infrastructure will become critical not only for protecting EHDS data but also for supporting EHDS data governance and AI Act-related requirements for AI governance.

4. Scientific Use Cases - Trustworthy AI workflows on EPIC Cloud

The convergence of EOSC federation, EHDS governance, and the AI Act places new requirements on research infrastructures supporting AI-driven science. Trustworthy AI workflows require controlled data access, traceability, reproducibility, and accountability across the entire AI lifecycle. EPIC Cloud addresses these challenges by providing ISO-certified environments in which AI pipelines can be designed, executed, and audited.

4.1 IRCCS AOUBO-Sant'Orsola Computational Genomics Platform (BOSCO)

One case study in which process-oriented governance was utilized effectively is the development of the Computational Genomics Platform, created by IRCCS Azienda Ospedaliero-Universitaria di Bologna (Sant'Orsola) and managed by the Bologna Sant'Orsola Computational Genomics (BOSCO) group. The platform represents a comprehensive suite of bioinformatic algorithms and processes for massive genomic dataset analysis, such as whole-exome and whole-genome sequencing, variant handling, and workflow reproducibility. The software elements of this platform, which leverage technologies like Galaxy and OpenCGA and include containerized bioinformatics tools, are publicly described and maintained by the BOSCO group [7]. In the cooperation between INFN and IRCCS AOUBO-Sant'Orsola, the main task has been the redefinition of how computational genomics services are delivered and operated, in particular the adoption of a cloud-native paradigm to separates infrastructure provisioning, workflow execution, and user access management, while

PoS(ISGC2026)016

maintaining strict control over data locality and security. The computational genomic platform implementation details have been already described in a previous article [8]. Since then, more software has been integrated and enabled to run on the ISO-certified platform, which is now provided in PaaS mode to the IRCCS. An additional effort is ongoing to also add the [9] portal, which will complete the platform with a comprehensive tool for omics data manipulation and analysis.

In terms of clinical aspects, IRCCS AOUBO-Sant'Orsola offers genomic data obtained via sequencing, supported by validated bioinformatics pipelines and expert clinical know-how. On the other hand, the INFN contributes with the provision of the secure cloud environment, computational power and storage capabilities, as well as orchestration necessary to run the genomic pipelines. The link between both areas occurs through the implementation of controlled access to data, making the EPIC Cloud environment one where the certified security boundary makes it suitable for running pipelines on sensitive genomic data under GDPR guidelines.

Besides the use case itself, the collaboration between INFN and IRCCS Sant'Orsola can be seen as a model of integration between the clinical research infrastructure and INFN as a national-scale scientific cloud integrator. The platform can be viewed as an example of a production-ready service for genomics analysis.

4.2 ICSC Spoke 8: AI for Health and Biomedical Research

In the context of Italian National Recovery and Resilience Plan (NRRP) EPIC Cloud offers support to the development of AI-related research activities designed in the context of ICSC and, more specifically, in the framework of Spoke 8 addressing health, biomedical, and life sciences applications. Such applications include the analysis of heterogeneous datasets such as genomics, imaging, and clinical information, and therefore require execution environments with strict guarantees in terms of confidentiality, integrity, and compliance with relevant regulations. By providing isolated controlled cloud-based environments, EPIC Cloud allows AI pipelines to be co-designed and executed with domain scientists, combining computation, data management, and security from their early development.

The Information Security Management System (ISMS) enables data access, training, and result generation processes to be properly organized into formalized workflows, allowing for reproducibility, traceability, and accountability while remaining flexible enough to allow experiments to be conducted.

4.2.1 The Universal Immune System Simulator

A representative implementation is the deployment of the Universal Immune System Simulator (UISS) as a *Software-as-a-Service* (SaaS) within a dedicated OpenStack tenant in the EPIC Cloud region, in particular in the INFN-Catania datacenter.

In this model, each use case, including UISS, is instantiated as an isolated project with defined resource quotas, segregated networking, and policy enforcement aligned with the EPIC operational framework. UISS is exposed to end users as a managed service, abstracting infrastructure complexity while ensuring controlled and secure access to computational resources.

User interaction is performed through a web-based interface for data submission and retrieval, while access to the execution environment is enforced through multi-factor authentication (2FA) and VPN-based network isolation. As illustrated in Fig. 2, users authenticate using strong authentication

PoS(ISGC2026)016

mechanisms and establish a secure VPN tunnel before accessing the *UISS Isolated Network*, where application services are hosted. Within this environment, data exchange is mediated by a controlled storage interface, and computation is performed by the UISS simulator and associated machine learning components.

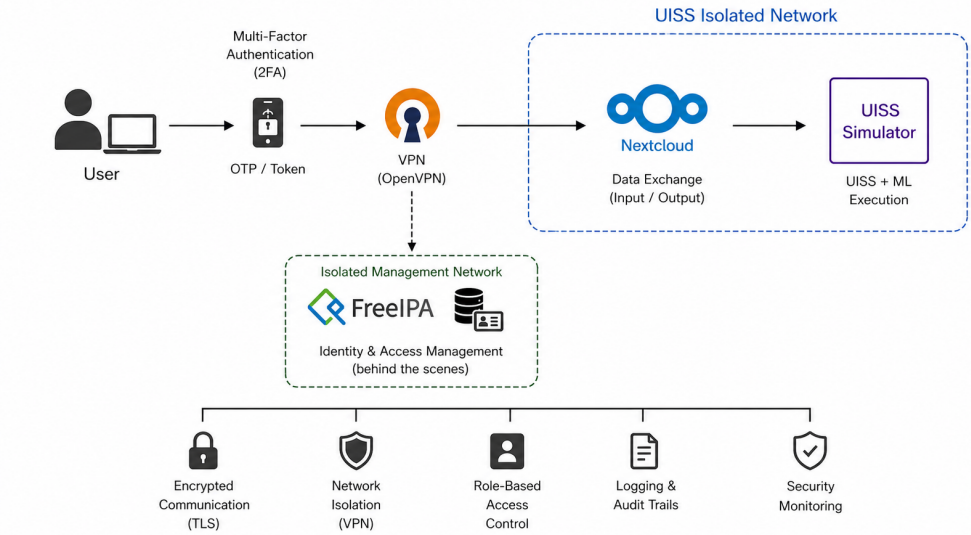

Figure 2: High-level architecture of the secure access workflow to the UISS application

The architecture enforces a strict separation between user-facing services and backend execution. Identity and access management is provided by FreeIPA, deployed within an isolated management network and not directly exposed to end users. In this configuration, FreeIPA operates as a backend identity provider, supporting authentication and authorization decisions (e.g., VPN access control) and ensuring a clear separation between control plane and data plane.

Security is implemented through a multi-layered approach consistent with the ISMS, including encrypted communication (TLS), network segmentation, role-based access control, and centralized logging and monitoring. Threat modeling based on the STRIDE methodology supports the identification and mitigation of risks such as unauthorized access, data tampering, information disclosure, and privilege escalation.

Secure software development practices are integrated into the platform lifecycle. In particular, Static Application Security Testing (SAST) is applied to application code and container images to detect vulnerabilities at early stages. These activities are embedded within controlled CI/CD pipelines and configuration management processes, ensuring compliance with EPIC Cloud security requirements.

Data lifecycle management mechanisms further reduce risk exposure: input data are processed within controlled environments and automatically removed after execution, supporting data minimization principles. The adoption of containerization and orchestration technologies enhances reproducibility, portability, and scalability while maintaining alignment with the EPIC Cloud governance model.

Overall, the UISS use case demonstrates how EPIC Cloud enables the delivery of secure

PoS(ISGC2026)016

SaaS applications for regulated biomedical research, providing a trusted execution environment for AI-driven workflows in alignment with the objectives of ICSC Spoke 8.

4.2.2 The SECUREMED project

Leveraging an ICSC Spoke 8 Cascade Funding Grant, we commissioned an independent security review of RUCIO and FTS software [14, 15], which are core components of INFN DataCloud platform. The main objective of the review was to verify the feasibility of the exploitation of RUCIO/FTS data management system, already proven rock-solid in the context of particle phyiscs data movement, also in the context of health research. The SECUREMED [16, 17] performed such a review and reported promising results about the robustness and security of RUCIO/FTS, corroborating our idea to adopt them in medical research.

4.3 The DARE project Predictive Medicine

The DARE project [10], funded by the Ministry of Universities and Research as part of the National Plan for Complementary Investments to the National Recovery and Resilience Plan (NRRP), aims to unlock the potential of data for enhancing health promotion and prevention with a lifelong perspective. DARE achieves this goal by enhancing and validating digital prevention tools, knowledge and processes for the effective use of data in order to define, monitor and predict health trajectories. The DARE project's technological platform is EPIC Cloud, which is improved and expanded to enhance interoperability and governance across hospitals. EPIC Cloud supports DARE by providing a secure environment where AI algorithms can be executed and validated in a federated fashion across multiple participating healthcare institutions without requiring full data consolidation. In this context, the term "federated" refers primarily to the distributed nature of the participating hospitals and data providers, where datasets can remain under the control of the respective institutions while AI workflows can be coordinated through a common governance framework. The multi-region deployment of EPIC Cloud across the INFN sites of Bologna, Bari, and Catania further provides the infrastructure foundation required to support such distributed processing models. By leveraging federated identity management and selective access control, EPIC Cloud enables AI processes that respect data localization requirements and institutional responsibilities while enforcing governance rules consistently across all participating nodes.

4.4 EOSC Italian Node and the BBMRI MCVAL Use Case

The European Open Science Cloud (EOSC) provides a federated framework for delivering interoperable digital services, computing, and data resources to diverse scientific communities. Within this context, the collaboration between the Italian EOSC Node [11], coordinated by ICSC [18], the BBMRI-ERIC EOSC Node, and INFN represents a concrete example of how national and thematic research infrastructures can be jointly exploited to support data-intensive and security-critical scientific use cases in the life sciences.

The Italian EOSC Node brings together national providers of computing and data services, with INFN acting as one of the main infrastructure operators through its long-standing expertise in large-scale distributed computing, cloud platforms, and secure environments. On the other hand, BBMRI-ERIC, as a European Research Infrastructure Consortium dedicated to biobanking and biomolecular

PoS(ISGC2026)016

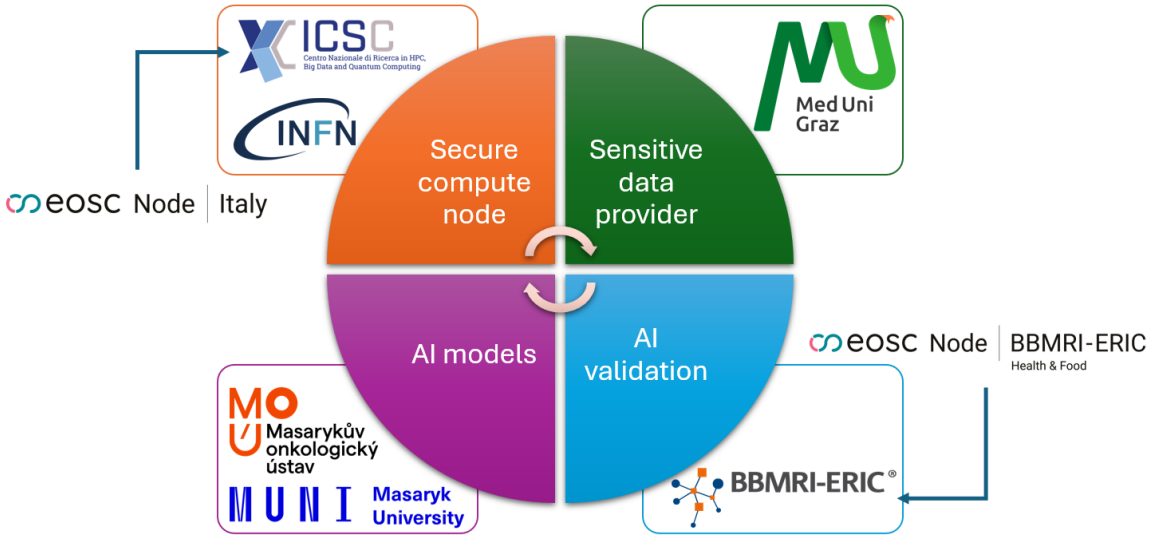

Figure 3: List of institutions, and the respective role, within the EOSC scientific collaboration.

resources, contributes to a domain-specific knowledge and access to sensitive biomedical data originating from multiple clinical institutions. The integration of these complementary actors enables the creation of a trusted cross-domain environment able to integrate together the EOSC principles of federation, interoperability, and reuse.

Figure 3 summarizes the main actors involved in the collaboration. The Italian EOSC Node, exploiting the INFN EPIC Cloud, provides the secure compute layer required to execute AI-based workflows, while the BBMRI-ERIC EOSC Node acts as the thematic entry point for the health and life sciences community, coordinating access to sensitive datasets and ensuring compliance with ethical and legal constraints. Academic and clinical partners, such as Masaryk University, the Masaryk Memorial Cancer Institute, and the Medical University of Graz, contribute both data and AI models, forming an end-to-end experimental chain that spans model development, validation, and evaluation across institutional boundaries.

From an architectural perspective, the logical organization of the computing environment supporting this collaboration is illustrated in Figure 4. The main use case supported is the MCVAL (Multi-centric validation of AI models for prostate-cancer screening) [12]. As is it clear from the figure, all the resources are deployed within a dedicated OpenStack tenant within the ISO 27001 certified zone at INFN (EPIC Cloud), expressly created to host the joint activities of the Italian EOSC Node and the BBMRI-ERIC EOSC Node. This approach allows strict isolation from other workloads, fine-grained control over network boundaries, and the enforcement of security policies consistent with regulated environments. The tenant hosts the core services required to support collaborative AI experimentation, including authentication, logging, and orchestration components.

Beyond the specific use case addressed in this work, the collaboration reflects a broader strategic vision. Rather than building bespoke infrastructures for individual projects or institutions, the joint exploitation of EOSC-aligned nodes enables the reuse of established services and operational practices. This model reduces duplication of effort, lowering the barrier to entry for research

PoS(ISGC2026)016

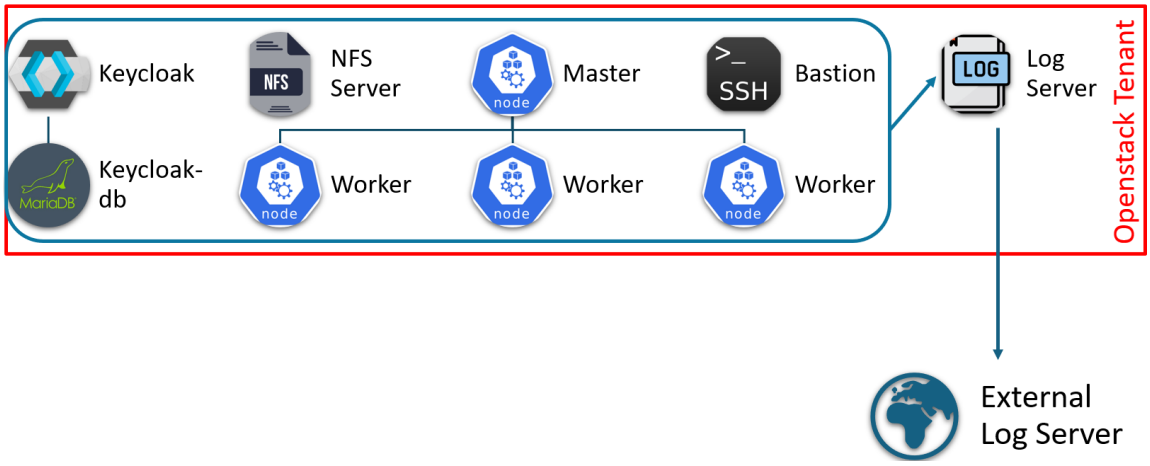

Figure 4: List of the VMs, and related role, in the OpenStack tenant in the ISO certified zone.

communities, and facilitates the evolution toward federated catalogs of services and compute resources accessible at the European scale.

In this sense, the collaboration between the Italian EOSC Node, ICSC, BBMRI-ERIC, and INFN can be seen as a reference implementation of EOSC federation principles applied to the health domain. It demonstrates how infrastructural providers and thematic research infrastructures can jointly support complex, multi-institutional workflows while preserving data sovereignty, security, and compliance, defining the way for scalable and sustainable digital ecosystems for biomedical research.

4.5 Health Big Data: Large-Scale AI on Sensitive Health Datasets

The Health Big Data project (HBD) [13] is an Italian Ministry of Health funded project lasting 10 years (2020-2030) aimed at building the federated cloud platform for all the Italian IRCCS (research hospitals). This project represents one of the most demanding application contexts for trustworthy AI, combining large-scale datasets with strict legal and ethical constraints. EPIC Cloud supports HBD use cases by hosting AI workflows that operate on population-scale health datasets within secure cloud environments designed to minimize data movement and enforce purpose limitation.

In order to perform secure, high-throughput, policy-based data management, we are working to adapt the RUCIO/FTS software to the very heterogeneous HBD use cases. AI pipelines—including data preprocessing, feature extraction, model training, and inference are executed within monitored and access-controlled infrastructures, ensuring that sensitive data remain within trusted boundaries. By integrating technical safeguards with ISMS-driven governance, EPIC Cloud enables the application of AI methods to health data at scale, while supporting transparency, auditability, and compliance with EHDS and AI Act-related expectations.

PoS(ISGC2026)016

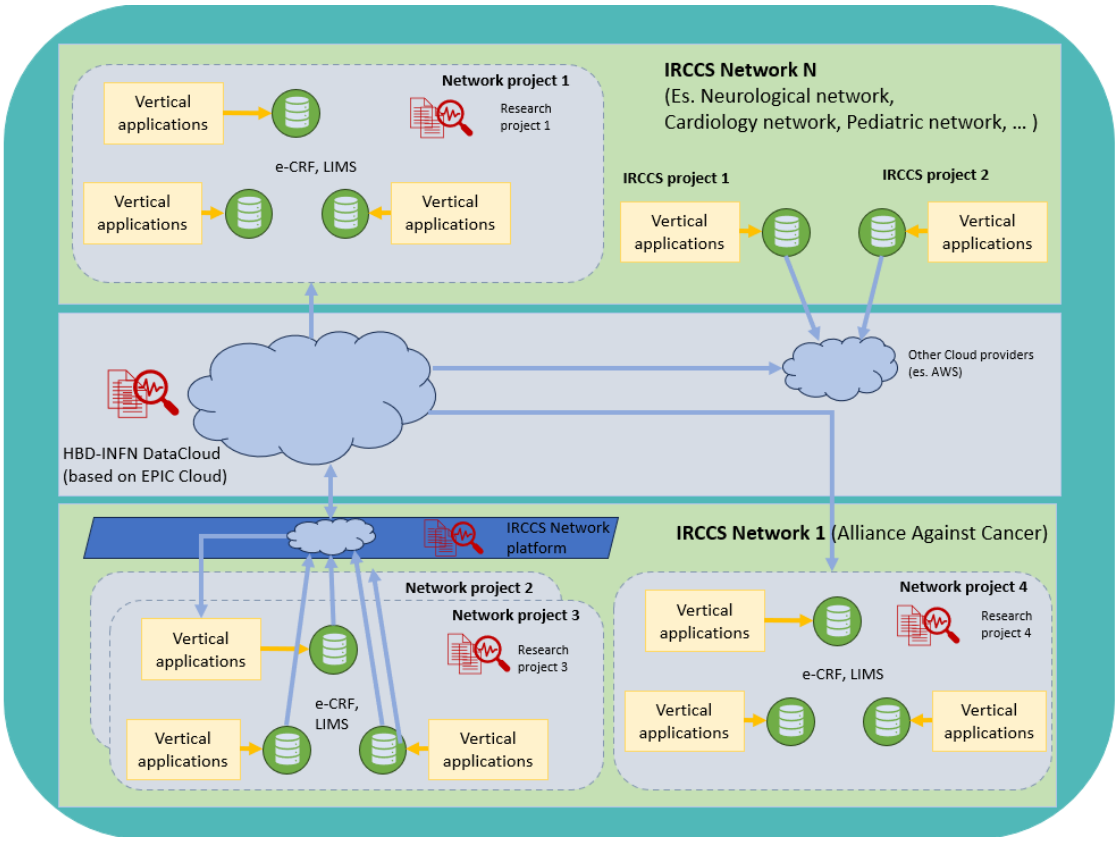

Figure 5: Health Big Data federated platform based on EPIC Cloud

5. Lessons Learned, Operational Benefits, and Multi-Region Scalability

The insights gained from designing, certifying, and operating EPIC Cloud prove that embedding security and compliance considerations into governance and operations of the INFN cloud computing research infrastructure is crucial and feasible. One lesson learned is that a process-oriented approach to Information Security Management System, which is well-aligned with internal organizational roles and technologies, allows improving operational efficiency rather than limiting it. The implementation of processes around onboarding services, access management, incidents handling, performing changes etc. has helped to make processes clearer, avoid confusion about responsibilities and collaborate effectively between infrastructure operators, security officers, and scientific stakeholders. This is particularly important for AI-driven workflow because of the necessity to ensure the reproducibility and traceability of computation.

On the operational side, EPIC Cloud shows how ISO-aligned governance can lead to practical benefits besides compliance itself. The use of standardized methodologies like risk management and Business Impact Analysis allowed us to better understand what our priorities were, where potential threats to business continuity lay, and plan corresponding actions. For AI workloads, this meant better predictability of execution environments as well as better operational guarantees, which made it easier for users to rely on the infrastructure.

PoS(ISGC2026)016

Another benefit of running EPIC Cloud is multi-region architecture, which spans on three different INFN sites: Bologna, Bari, and Catania. This approach not only enables scalability and high availability of the cloud but also provides flexibility for AI-driven workflows, allowing distributing the processes across multiple data centers while keeping all operations governed by one ISMS. The ability to deploy the same governance framework, processes, and controls on all EPIC sites while maintaining consistency, is crucial and critical when running federated workflows. This approach could be also extended to more complex environments involving several institutions.

Finally, using the multi-region approach will allow us to enable load balancing and achieve higher levels of fault tolerance for data-intensive and computationally intensive workloads. Since the same technologies, operational processes, and organizational roles have been applied to operate multiple INFN sites, the implementation of the ISMS was eased. It allowed extending our platform further with more AI-centric services and other platforms without any significant issues. Alongside with EOSC federation and EHDS, EPIC multi-region cloud represents a model of national Research Infrastructures for running AI-enabled research workflows.

6. Conclusions and Outlook

Thus, the development of the INFN DataCloud from pilot initiatives to fully-fledged and certified cloud regions can be viewed as an example of how to respond to the increased challenges of modern scientific computing through designing a cloud region based on the principles of *security and compliance by design*. In this regard, the EPIC Cloud project can be credited as a proof of concept: through the design of an ISO-aligned ISMS and the implementation of process-oriented governance in its operations, **INFN has demonstrated that it is possible to run cloud services capable of meeting the most sophisticated needs of AI-powered research workflows without sacrificing security and governance.**

Among the key achievements of this initiative should be mentioned the demonstration of the capability of open science infrastructures to coexist with regulated data environments and support complex data processing workflows. Integration of EPIC Cloud into the overall INFN DataCloud and EOSC ecosystems, and the application of the FAIR principles, federated access, and interoperability in combination with high levels of control in dealing with health and biomedical data is particularly important in the light of ongoing efforts in Europe, including the creation of the European Health Data Space and the adoption of the AI Act, which require precisely such guarantees for enabling secondary data use and trustworthy artificial intelligence.

The experience of deploying EPIC Cloud in three cloud regions, namely Bologna, Bari, and Catania, and operating them in a consistent manner under the umbrella of the same ISMS and governance system has demonstrated that such an approach is not only feasible but also highly beneficial both in terms of resilience and scalability of AI workflows as well as consistency in their management at different sites.

Finally, the experience of implementing the EPIC Cloud will facilitate the subsequent progress towards aligning more cloud regions in the overall INFN DataCloud according to the ISO standards, making use of shared technological infrastructure, roles, and processes. From another point of view, the EPIC Cloud experience can serve as a template for other countries and institutions aiming to

PoS(ISGC2026)016

establish a trusted research infrastructure based on a solid technological, organizational, and legal foundation.

Based on the Process Reference Model, EPIC Cloud could evolve to automation and agents' coordination capabilities. Adopting *process-based automation* and *agents-based architecture*, once the processes, roles, and control points are identified, the system would allow autonomous or semi-autonomous agents to execute actions according to predetermined governance constraints. The coordination between these agents will ensure the evolution towards the **Large Action Model (LAM)** to facilitate the execution of complex processes. Benefits expected from such an approach could be scalability, consistency of controls, responsiveness, governance alignment.

From the security perspective, such an approach requires consideration of agent identification and authentication, authorization and segregation of duties, monitoring and traceability, AI risks management. In summary, the above future evolution allows for **greater integration between the three dimensions of automation, governance, and security.** This approach aligns perfectly with the EPIC Cloud strategic goal of integrating security, governance, and operational intelligence through a digital architecture.

References

[1] *European Open Science Cloud* https://www.eosc.eu Last seen, April 2026.

[2] *European Health Data Spaces regulation* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202500327 Last seen, April 2026.

[3] *INFN ISO/IEC 27001 27017 27018 certificate* https://www.cnaf.infn.it/wp-content/uploads/2026/03/CERT_15739_ENG_ISO_27001.pdf

[4] *INFN DataCloud* https://www.cloud.infn.it Last seen, April 2026.

[5] D. Salomoni et al. *INDIGO-DataCloud: a Platform to Facilitate Seamless Access to E-Infrastructures* Journal of Grid Computing 2018 https://doi.org/10.1007/s10723-018-9453-3

[6] Porter, M. E. The Competitive Advantage: Creating and Sustaining Superior Performance. NY: Free Press, 1985. (Republished with a new introduction, 1998.) *ISBN 0-02-925090-0*

[7] *BOSCO Project*, https://bosco-aosp.github.io/computational-genomics-platform/ Last seen, April 2026.

[8] J. Gasparetto et al. *Computational Genomics platform: a Cloud-enabled approach* Proceedings of International Symposium on Grids and Clouds (ISGC) 2024 10.22323/1.458.0042

[9] *Galaxy Project*, https://galaxyproject.org. Last seen, April 2026.

[10] The DARE project: Digital Life Long Prevention https://www.fondazionedare.it/en. Last seen, April 2026.

PoS(ISGC2026)016

[11] The EOSC Italian Node website https://eosc.eu/building-the-eosc-federation/eosc-node-italy. Last seen, April 2026.

[12] Multi-centric validation of AI models for prostate-cancer screening https://eosc.eu/wp-content/uploads/2025/10/EOSC-Federation-scientific-use-case-MCVAL.pdf. Last seen, April 2026.

[13] The Health Big Data Project https://www.healthbigdata.it/en/Last seen, April 2026.

[14] RUCIO https://rucio.cern.ch/Last seen, April 2026.

[15] File Transfer Service https://fts.web.cern.ch/fts/Last seen, April 2026.

[16] SECUREMED Project https://www.sogetel.it/securemed-the-project/?lang=en

[17] Securemed Results https://doi.org/10.5281/zenodo.17544823

[18] *ICSC Foundation*, https://www.supercomputing-icsc.it/en/icsc-home/. Last seen, April 2026.

PoS(ISGC2026)016