

EVIDEN

Maintaining Healthcare Compliance: GDPR and HIPAA Regulations with Evidian's IAM Solutions

Table of contents

01	Executive Summary	3
02	Introduction	4
	How IAM helps HIPAA compliance	5
	The Three P's of IAM for Regulatory Compliance	5
	Isolating Healthcare Clearinghouse Functions	5
	Supporting the HIPAA Security Rule with IAM	6
	GDPR and HIPAA compliance: how they can benefit one another	7
03	The Diversity of Access Methods is a Source of Risk	8
	Potential Risks Linked to the Users	8
	Potential Risks Linked to Administration of Access Rights	8
04	Coherent Identity and Access Management	9
	Introduction	9
	The Separation of Roles in the Access Rights Allocation Process	9
05	High Availability and Contingency Plan	10
06	Audit Data	11
	Regulatory Requirements	11
	Audit Data Content with IAM Suite	11
07	Evidian's IAM Modules	12
08	Conclusion: Towards a Zero Trust approach in Healthcare	13
09	Glossary	14

Executive Summary

Maintaining compliance with the HIPAA regulation is one of the biggest challenges for Covered Entities (CE)¹ today. To ensure patient's information stay protected, identity and access management (IAM) solutions remain a must-have for healthcare organizations.

A comprehensive IAM tool fits the access control standards required by HIPAA.

This white paper explains how, based on Atos expertise on the HIPAA regulation, the Evidian IAM suite can help Covered Entities remain compliant with the requirements of the Code of Federal Regulations (CFR) pertaining to security and, thus, safeguard its Protected Health Information (PHI) by offering:

- Identity governance and administration solutions supporting strong identities and limiting PHI access to the right users with a role-based management approach,
- Enterprise access management tools that prevent any unauthorized access to healthcare information and simplify the staff daily work,
- Audit features on sensitive information accessibility and usability,
- A unique and technology-independent approach with clear return on investment assets.

Aligned to the Covered Entities' strategy and roadmap, the Evidian IAM Suite is extremely adaptable to the evolving needs of the healthcare while hiding from security administrators the complexity of systems and applications.

1. Covered Entity: any healthcare provider, health plan or healthcare clearinghouse

Introduction

Since the release of HIPAA since 1996, thousands of organizations had to comply with this regulation to protect patient’s sensitive information. However, maintaining this compliance may turn out to be challenging.

The U.S. Department of Health and Human Services regularly reviews if healthcare organizations violate the HIPAA rules. As of 2019, only 22 of the 298 investigations conducted after a complaint on breach compliance were considered as non-violating the HIPAA rules, meaning more than 90% of the cases led to corrective actions.² In 2019, impermissible uses & disclosures, safeguards and access were identified as the top 3 issues in the investigated cases.³

Year	Issue 1	Issue 2	Issue 3	Issue 4	Issue 5
2019	Impermissible Uses & Disclosures	Safeguards	Access	Administrative Safeguards	Minimum Necessary
2018	Impermissible Uses & Disclosures	Safeguards	Administrative Safeguards	Access	Technical Safeguards
2017	Impermissible Uses & Disclosures	Safeguards	Administrative Safeguards	Access	Technical Safeguards
2016	Access	Impermissible Uses & Disclosures	Safeguards	Administrative Safeguards	Technical Safeguards

Top Five Issues In Investigated Cases Closed With Corrective Action, By Calendar Year (Source: Hhs)

Staying aligned with the regulation and its updates, also means dealing with external security threats, evolving technology and user’s awareness:

- The question is no more if a cyberattack will happen but when. The healthcare sector is targeted by more and more inventive threats and motivated actors as stolen healthcare records are amongst the more expensive data sold in black markets.
- Healthcare organizations are getting digitalized. They are adopting new technologies and practices such as Cloud, BYOD (bring your own device) and connected medical devices and which come with their own vulnerabilities and need to be secured as well.
- Healthcare staff often does not have enough time to be trained on cybersecurity issues. This lack of awareness can lead to negligence or misuse of healthcare data.

The digitalization of health information means it is critical to control access to systems and applications containing that information. Covered Entities are required to implement technical safeguards and security measures in order to restrict access to users and patients on a need-to-know basis.

These technical safeguards can be very time-consuming and even ineffective if you restrict yourself to the out-of-the-box security provided by application or server vendors. Configuring each of these data repository – and workstation – individually to make them comply with the Security and Privacy Rule is not a good solution.

2. <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-results-by-year/index.html>

3. <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/top-five-issues-investigated-cases-closed-corrective-action-calendar-year/index.html>

Introduction

How IAM helps HIPAA compliance

Identity and Access Management (IAM) solutions can help Covered Entities implement the Security Rule requirements in a cost-effective and coherent manner by:

- Defining in one single location the HIPAA-mandated procedures pertaining to access control, then deploying them over the whole Covered Entity.
- Using simple yet systematic role-based rules to restrict access to Protected Health Information.
- Establishing governance to efficiently manage the policies, processes and standards aligned with the Covered Entity strategy and roadmap.
- Simplifying access attestation to verify and validate users' entitlement and access to Protected Health Information.
- Centralizing activity logs related to user access to Protected Health Information in one location, so that they can be easily audited.
- Controlling access to workstations and applications.
- Managing user identities systematically, even if the data stores containing these identities are located in various directories.

The Three P's of IAM for Regulatory Compliance

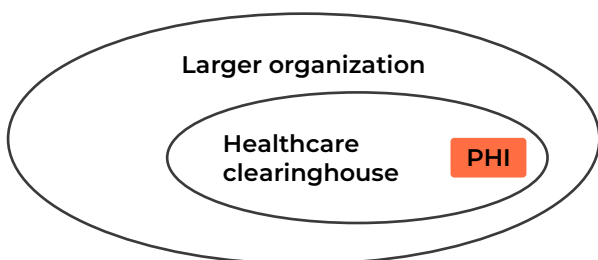
Implementing an IAM solution to ensure regulatory compliance involves the whole CE and goes beyond simple technology considerations. The most critical tasks are the organizational and human aspects, as well as the inventory of applications, data stores and workflows that concern Protected Health Information.

People	Regulatory compliance will require the cooperation of physicians, staff and other employees. A project can be helped greatly if it has the clear and public support of the Covered Entity's general management.
Process	Implementing regulatory requirements such as the HIPAA Security Rule means putting in place new processes. These processes represent a lot of changes in people's habits, and costly training for the entire organization. If some processes are automated, that can help reduce costs.
Product	This is the technology side of the equation. As the technological environment within the Covered Entity may be quite complex, it is best if the management of the entire solutions hides that technological complexity.

Getting the support of the end users will greatly help move it forward – even if the changes it brings are mandatory due to regulatory compliance. For instance, Single Sign-On (SSO) is not a requirement of the HIPAA Security Rule. On the other hand, SSO can offer physicians a lot of convenience in their daily work (they no longer have to manage tens of passwords). This can generate a lot of valuable goodwill, and internal allies, toward the implementation of the security project.

Isolating Healthcare Clearinghouse Functions

The HIPAA covers the case of a healthcare clearinghouse that is part of the larger organization. It requires that the PHI contained in the healthcare clearinghouse be protected against access by employees in the larger organization.



As the Security Rule requires policies and procedures to be put in place, another solution is to use an IAM solution to enforce partitioning rules. It does so by ensuring that no person in the larger organization has access to the resources and application in the smaller healthcare clearinghouse. Using role-based rules, administrators will specify that resources containing PHI are out of reach to all employees in the larger organization. As a result, if an employee of the clearinghouse leaves and takes up a job in the larger organization, he or she will automatically lose access rights for the PHI as soon as the changes have been made in the corporate user directory.

Introduction

Supporting the HIPAA Security Rule with IAM

The general requirements for security standards, as stated in the HIPAA Security Rule, are presented below. An IAM solution such as Evidian IAM Suite can help a Covered Entity achieve these requirements through features covering automated protection and control of access to protected health information.

45 CFR Paragraphs	Definitions/Requirements	Evidian IAM Suite contribution
§ 164.306.a	Covered Entities must do the following:	
§ 164.306.a.1	Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.	IAM Suite provides a range of features to protect PHI. Such protection can take effect during access to applications, through identity verification and role-based access granting.
§ 164.306.a.2	Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.	Protection against anticipated threats relating to access control can be easily integrated into the CE's security access policy using the IAM Suite tools.
§ 164.306.a.3	Protect against any reasonable uses or disclosures of such information that are not permitted or required [for maintenance].	Identity Governance and Administration (IGA) makes it possible to restrict PHI access to users on a need-to-know basis, using a role-based management approach.
§ 164.306.a.4	Ensure compliance with this subpart by its workforce.	IAM Suite helps ensure compliance by providing end-users with an unobtrusive but mandatory interface. Enterprise Access Management (EAM) clients work on the client workstations and do not require any additional software when accessing secured web resources. Moreover, IAM Suite provides demonstrable added value to users through its SSO features, thus aiding acceptance by the workforce.

In addition, IAM Suite helps Covered Entities comply with HIPAA requirements by covering most environments where Protected Health Information may be stored and managed. IAM Suite effectively provides secured access to workstations and restricts access to a large variety of resources using role-based access control:

- Client-server applications
- Web applications (on-premise/cloud)
- Mainframe access
- Desktop applications

For a detailed description, requirement by requirement, on how IAM Suite can help a Covered Entity achieve compliance with the HIPAA Security Rule, you can refer to our HIPAA Security Rule Compliance with IAM document

Introduction

GDPR and HIPAA compliance: how they can benefit one another

The General Data Protection Regulation (GDPR) is a regulation whose goal is to protect individuals' data privacy across EU countries. Having similar objectives as the HIPAA regulation, it may be important to understand if being compliant with the GDPR can help with HIPAA and vice versa to not duplicate efforts.

What differentiates GDPR from HIPAA is mainly scope and objectives. GDPR applies to all organizations controlling and processing sensitive personal data while HIPAA only focuses on protected health information held by covered entities.

For both regulations, IAM is essential to provide strong access control to personal data and centralized identity management as required. Regarding HIPAA, organizations must have the adequate system controls to ensure that only the authorized healthcare staff can securely access PHI to protect sensitive data. GDPR requires that only the right people can access personal data for the required amount of time. Depending on the data usage context and purpose, access controls can be managed at a granular level. In case of an audit, the data protection officer must be able to provide proofs of compliance.

Being HIPAA compliant means organizations already have the right tools to protect patient's data. To be GDPR compliant, IAM solutions must expand to all personal data.

For more information on the role of IAM on GDPR compliance, our white paper on requirements related to user access and security of processing is available [on our website](#).⁴

	HIPAA	GDPR	IAM Role
Scope	Covered entities and associates managing individual's health information in the US.	Any organization managing EU residents personal data.	IAM helps manage the full lifecycle of users' identities and access rights, taking into account role-based access control.
Consent	Patient data can be disclosed without consent for treatment purposes.	Explicit consent is needed for any PHI or communication operations.	IAM can be used to notify users in case of changes in data processing and can act as key tool for consent management.
Right to be forgotten	No right to be forgotten.	Right granted for people wanting their data to be deleted	IAM can be entirely configured around specific status (active/ inactive/in retention/deleted), enabling global data deletion when required.

⁴. White Paper - Powering GDPR: Identity and Access Management in your compliance journey - <https://www.evidian.com/documents/white-papers-compliance/white-paper-powering-gdpr-identity-access-management-compliance-journey/>

The Diversity of Access Methods is a Source of Risk

Covered Entities need to conduct audits to reveal potential vulnerabilities affecting PHI's confidentiality according to the HIPAA. The diversity of access methods can generate errors, fraud or breach of privacy. The absence of a unified method of managing identities and accesses is a clear source of risks and vulnerabilities for users and administrators.

Potential Risks Linked to the Users

These risks are primarily linked to the large number of passwords an employee has to use in his or her day-to-day work. In a typical hospital, physicians can have about 20 different passwords for various applications. These passwords need to be changed with varying frequency.

If the passwords are too many, the user will tend to note them down on an easily accessible medium (Post-It™ notes for example). Moreover, recurring password changes are handled by changing a numeral at the end of a password. All this facilitates internal fraud by facilitating wrongful access to PHI.

Shared passwords within a team is also a potential source of risk, as this can expose PHI to personnel who should not have access to it (secretarial staff, etc.).

As password management is considered an "Addressable" specification by the HIPAA Security Rule, Covered Entities should carefully consider the implications of their choices.

How to reduce these risks?

These risks can be significantly reduced by using a secure single sign-on solution (SSO).

With a secure SSO solution, the users only need to remember a single identifier/password pair, with all the others being entered invisibly at each access to an application. Biometric, smartcard, OTP, RFID Card, Smartphone ... solutions could reinforce this solution.

For a given application IAM Suite hides the real passwords from the user. These passwords can, therefore, all be different and non-intuitive; as a result, penetrating the security of an application does not compromise the other resources. Moreover, IAM Suite enables the Covered Entity to define and deploy a specific password policy by application.

Potential Risks Linked to Administration of Access Rights

It is increasingly difficult to satisfactorily manage the allocation of access rights. Although the number of administrators is stable or falling as a result of cost reductions, their work is increasingly complex:

- Access rights concern a wide variety of resources such as web sites, mainframe applications and so on.
- At the same time, movements among the members of the workforce (turnover, reassignment, mergers, etc.) imply regular, constant updating.

This creates operational risks, for example:

- Rights allocation is often delegated to the systems engineers, who consider this to be a secondary task. This manual step is thus sometimes delayed or contains operator errors. This is a source of process-related risks.
- When an employee leaves the Covered Entity, his or her rights are often not cancelled, the problem being that it is hard to make a complete inventory of all the authorizations granted to the user during the course of his or her career. He or she will, therefore, still have access to systems even though he/she is no longer employed. This is a source of external fraud.
- Finally, too many passwords means that they are often lost or forgotten, generating calls to the help-desk team. Faced with the volume of these calls (up to 30% according to the Gartner Group), a large number of people have to be given the power to change a password. This can be a source of internal fraud.

How to reduce these risks?

These risks can be significantly reduced by using a "provisioning" solution with identity management. Allocation (and cancellation) of access rights is easily done from a Web Portal, without any manual intervention on the resources themselves.

This allocation of rights is done on the basis of organizational criteria by trustworthy persons and with no technical know-how required. The solution permits to therefore delegate administration rights to role holders. For example, a department manager, who has the service administrator role, owns administration rights limited to the employees and applications of this service.

Coherent Identity and Access Management

Introduction

The HIPAA Security Rule requirements make it mandatory for Covered Entities to design and enforce effective procedures to “ensure the confidentiality, integrity, and availability of all electronic protected health information”. However

- **Designing** procedures is especially difficult if the procedure has to go into technical details. This means that technicians and security specialists must collaborate to establish it, and that the resulting rule will be obsolete once technology evolves.
- **Enforcing** procedures is impractical if they require too many manual operations, or frequent transmission of information between many people.
- For these reasons, it is definitely better to **manage** security procedures from a central location. If a HIPAA-mandated rule can be defined centrally and applied automatically in a matter of seconds, health information can be best protected. Of course, central administrators can choose to delegate the management of some areas to local administrators.

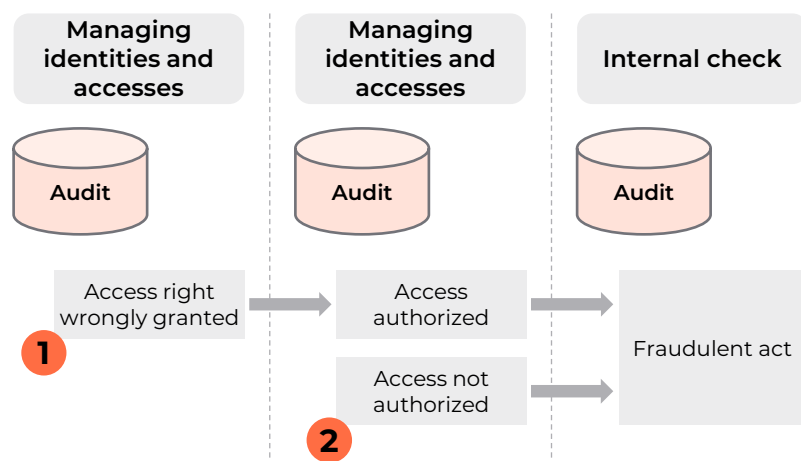
The Separation of Roles in the Access Rights Allocation Process

In order to be easily auditable, the access rights allocation process must be clearly defined and comprise as few manual operations as possible.

IGA solution relies on the user and organization definitions already in place in the Covered Entity. It in fact uses the company’s LDAP human resources directories automatically. The roles are thus clearly defined and the information auditable:

Role	Who?	Where to audit?
Definition of the organization, creation, modification and cancellation of the users.	Existing organization. Generally, the human resources department.	Central frLDAP user’s directory
Allocation of rights to users thus defined.	Management of user rights; centralized organization with possible delegation.	Policy Database
Definition of technical resources for which the access rights are to be managed	IT department	Policy Database
Generation of audit data on the accesses and administration operations	Done automatically by IAM suite	Central Audit Database

The rights allocation processes (request, qualification, approval, etc.) can thus be easily defined and audited, even if highly detailed and complex.



In this way, the information needed for the audit, such as an inquiry into the origin of an operational incident, is clearly localized.

In the diagram on the left side,, we can see that a fraudulent act can be the result either of an unauthorized access (password theft for example), or incorrect allocation of access rights (intentionally or otherwise).

The Identity and Access Management audit data must thus cover both aspects:

- 1. audit of rights allocations**
- and**
- 2. audit of accesses**

High Availability and Contingency Plan

The HIPAA Security Rule requires Covered Entities to put in place “policies and procedures for responding to an emergency (...) that damages systems that contain electronic PHI.”

Any IAM system must itself be included in that contingency plan. If systems containing PHI are back online but inaccessible (or worse, widely accessible) due to a failure of the IAM environment, this could lead to huge issues.

Evidian IAM includes valuable high-availability and disaster recovery features. With real-time data replication, changes to the data containing identity and access security information can be propagated automatically to a remote server that can be used in case of emergency. In case of failure, automatic failover is achieved and no manual intervention is necessary



Audit Data

Regulatory Requirements

- Audit controls must be put in place to “record and examine activity in information systems that contain or use electronic PHI.” **Security management** processes require security incidents tracking records to be regularly reviewed.
- **Information access management** policies and procedure must include log-in monitoring, including all log-in attempts.
- **Security incident procedures** include security response and reporting processes. Security incidents must be quickly identified and documented.
- Lastly, **audit controls** are specifically required; mechanisms must be implemented to record activity in “information systems that contain or use electronic PHI”

The audit data generated by an IAM tool should, therefore, satisfy the following requirements:


- **Data completeness:** this makes it possible to review incidents and accurately document them.
- **Information accessibility:** it should be possible to access data through easy-to-use interfaces in order to more easily review security incidents.
- **Information usability:** the audit data should be accessible in a standard format (database, structured file) or through well-documented APIs. In that case, it can be fed into complete data analysis tools.

Audit Data Content with IAM Suite

The audit data generated by IAM Suite is extremely detailed. It covers the following domains:

- **Access Certification:** gives you detailed information on current and completed access certification campaigns
- **Activity:** helps you to monitor the user activity
- **GDPR:** provides information about personal data handled by Evidian IGA
- **KPI – Quality:** gives you Key Performance Indicators (KPIs) and Quality information of the security policy
- **Policy Status:** gives you status on the policy objects
- **Statistics:** helps you monitor the usage of the policy
- **User Life Cycle:** gives you information about user arrivals and departures

The solution also provides standard dashboards in Analytics and Intelligence (A&I) such as:

 User authentications Number of user authentication for a given period	 User authentications risks Level of risk related to user authentication displayed by hour or minute	 Users Comprehensive view of users by organizations for a given period
 Applications accesses View of successful and failed user's access to applications and resources on the system	 Users with SoD violations Notification of user accounts with Segregation of Duties violations and possibility to investigate and act on them	 Users without entitlements Dashboard to track users without any permission or role and launch certification decisions
 Right assignment/ revocation requests Number of entitlements requests handled per month and in depth-view (decision, type of approval, rule, etc.)	 User lifecycle Number of users entering, leaving or evolving within the company per month	 Password changes Number of passwords changed, whether by the user or by an administrator and password changes that failed
 Provisioning failures Number of errors that occurred during the provisioning of target systems	 User-to-service registration/ un-registration Number of registration and un-registration for every application of the system and check for inconsistencies	

Evidian's IAM Modules

The Evidian IAM suite solution is designed in a modular way, making it possible to implement only the features you require for regulatory compliance. These modules are interoperable so your IAM solution may evolve over time.

Identity Governance & Administration



Govern, manage, control user identities, mass updates, self-registration, auto-activation, resources provisioning risk based access rights reconciliation and access certification

Web Access Management



Identity provider for web apps, web SSO, multifactor and contextual authentication, Identity Federation. APIs and mobile native apps protection

Enterprise Access Management

Authentication Manager



Provides Multifactor authentication on Windows & Thin Client, Kiosk & Cluster of PCs, Self-Service Password Reset, ...

Enterprise Single Sign-On



Secure access to web and non-web applications from PC Win and Mac, tablets, mobiles Android and iOS

Analytics & Intelligence



Data collection, risk analysis, advanced analytics for Identity & Access Management

The Evidian IAM suite solution can also help achieve **return on investment for operating costs** in terms of productivity gains. Three types of populations are concerned:

1. **Users:** they are quickly granted the access rights they require and save time by no longer having to enter multiple passwords,
2. **Help desk staff:** setting up an IAM solution considerably brings down lost password calls,
3. **System administrators:** deploying new internal applications is faster as the related security tasks (e.g. distributing passwords) are considerably reduced; account deactivation when a user leaves the organization is also totally automated.

An identity and access management solution can thus quickly pay for itself, even without taking into account the reduced risk of wrongful PHI access.

Conclusion: Towards a Zero Trust approach in healthcare

The digital transformation of the healthcare sector greatly expanded its network perimeter in the recent years. The hospital environment is no longer restrained to the doctor's office. Connected medical devices, transition to the Cloud and Bring your Own Devices (BYOD) practices raise complexity in the way to address security challenges.

To protect electronic health records, healthcare organizations must not only protect from external threats but also from insiders. The frontier between public domain and the healthcare own infrastructure also tends to blur. Employees move between the internal IT infrastructure of the hospital to then connect to their preferred website through their own device. This lack of visibility affects the security strategy efficiency.

That is where the Zero Trust principle applies: no actors or systems should be automatically trusted. Each user and access points must be authenticated and authorized when trying to connect and access data.

That is why authentication and access right governance are the cornerstone of Zero Trust strategies. These tools help CISOs continually assess access to corporate services regardless of whether they are on-premise, internet-facing, or Cloud-hosted. It is also a way to prevent lateral movement attacks which can prove to be very effective in flat IT organizations often found in healthcare. For example, connected devices are often exploited by hackers and compromised to exfiltrate sensitive information. With a Zero Trust approach, if a biotech device, usually collecting healthcare information, is not explicitly required to download information from a database, then its access will be denied by default.

Adopting a Zero Trust model can help achieve a stronger security posture to maintain compliance in the years to come, like with the HIPAA regulation. Healthcare organizations embracing this strategy and IAM solutions will be able to demonstrate to auditors that they have taken all appropriate steps to secure data even in the case of a data breach.

Glossary

Term	Description
CE	Covered Entity
EAM	Enterprise Access Management
GDPR	General Data Protection Regulation
IAM	Identity and Access Management
IGA	Identity Governance and Administration
HIPAA	Health Insurance Portability and Accountability Act of 1996
LDAP	Lightweight Directory Access Protocol
MFA	Multi-Factor Authentication
OTP	One-time password
PHI	Protected Health Information
PIV card	Personal identity verification card (United States Federal smart card)
RFID	Radio-frequency identification
SoD	Segregation of Duties
SSO	Single Sign-On
WAM	Web Access Manager

EVIDEN

About Eviden¹

Eviden is a next-gen technology leader in data-driven, trusted and sustainable digital transformation with a strong portfolio of patented technologies. With worldwide leading positions in advanced computing, security, AI, cloud and digital platforms, it provides deep expertise for all industries in more than 53 countries. Bringing together 57,000 world-class talents, Eviden expands the possibilities of data and technology across the digital continuum, now and for generations to come. Eviden is an Atos Group company with an annual revenue of c. € 5 billion.

¹ Eviden business is operated through the following brands: Alia Consulting, AppCentrica, ATHEA, Atos Syntel, Bull, Cloudamize, Cloudreach, Cryptovision, DataSantics, digital.security, Eagle Creek, EcoAct, Edifixio, Energy4U, Engage ESM, Forensik, IDEAL GRP, IDnomic, In Fidem, Ipsotek, Maven Wave, Miner & Kasch, Motiv, Nimbix, Processia, Profit4SF, science+computing, SEC Consult, Visual BI, Worldgrid, X-Perion, zData

About Atos

Atos is a global leader in digital transformation with 112,000 employees and annual revenue of c. € 11 billion. European number one in cybersecurity, cloud and high performance computing, the Group provides tailored end-to-end solutions for all industries in 71 countries. A pioneer in decarbonization services and products, Atos is committed to a secure and decarbonized digital for its clients. Atos is a SE (Societas Europaea) and listed on Euronext Paris.

The [purpose of Atos](#) is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Learn more at: atos.net

Connect with us



eviden.com