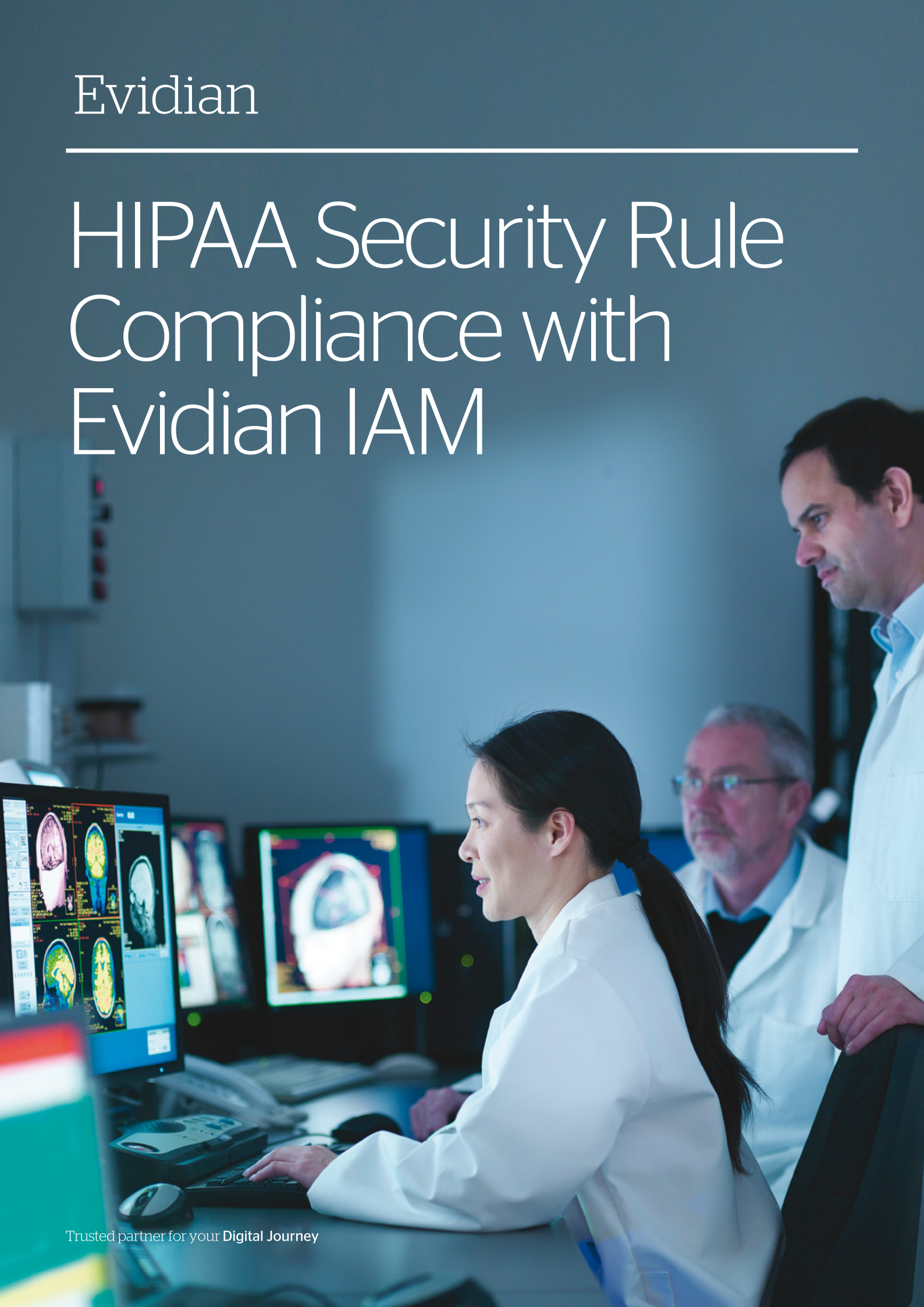
Evidian

HIPAA Security Rule Compliance with Evidian IAM



Trusted partner for your **Digital Journey**

Evidian Identity and Access Management Suite can help a Covered Entity[1] achieve compliance with the implementation specifications contained in the HIPAA Security Rule.

As explained in Paragraph 164.306.d, some implementation specifications are **"required"**, which means that they must be implemented as specified. Some implementation specifications are **"addressable"**, which means that the Covered Entity must determine how best to implement them, taking into account its own environment and risk estimates.

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.

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

45 CFR Paragraphs	Definitions/ Requirements	Required/ Addressable	IAM Suite feature
164.308.a.1.i	 **Standard: Security management process.** Implement policies and procedures to prevent, detect, contain, and correct security violations.		
164.308.a.1.ii.B	**Risk management.** Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Sec. 164.306(a).	Required	See § 164.306.a.3.
164.308.a.1.ii.D	**Information system activity review.** Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	Required	IAM Suite stores and makes available a quantity of audit data regarding security-related activity, for instance: User-related data such as access to individual applications, successful or failed access, security incidents etc. ◄◄Administrator-related data such as granting of rights, creation and deletion of user and resources, groups etc. ◄ Centralized data on consultation history for all protected web resources. ◄ Access certification is an audit and governance process aimed to ensure that user's access rights are compliant with security policies.
164.308.a.3.i	 **Standard: Workforce security.** Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information (…) and to prevent those workforce members who do not have access (…) from obtaining access to electronic protected health information.		
164.308.a.3.ii.A	**Authorization and/or supervision.** Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	Addressable	Access to the features of the administration user interface is itself restricted according to roles. This means that the range of administration actions that administrators may perform is entirely configurable, and the authorization procedures can be implemented with ease. The Web Portal Home page is generated dynamically depending on your rights. It only displays the list of actions (requests and/or information consultation) that you can execute by yourself. As well, the responsibility of user access granting can be delegated to administrators in remote locations
164.308.a.3.ii.B	**Workforce clearance procedure.** Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	Addressable	Using IGA provisioning, each workforce member can be assigned the appropriate access rights to resources (on-premise or cloud) where PHI is located. This is the case not only for workforce members, but for all other types of users as well – internal or external.
164.308.a.3.ii.C	**Termination procedures.** Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.	Addressable	IGA solution makes access termination easy and quick. Once a user's employment ends, the user is simply removed from the list of active users; IGA handles automatically all access rights deactivation/removals to individual resources. Employee termination can concern remote entities such as affiliates of the CE. In that case, termination can be handled locally by a delegated administrator whose administrative rights are tailored according to the CE's internal procedures.

45 CFR Paragraphs	Definitions/ Requirements	Required/ Addressable	IAM Suite feature
164.308.a.4.i	**Standard: Information access management.** Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.		
164.308.a.4.ii.A	**Isolating healthcare clearinghouse functions.** If a healthcare clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.	Required	To determine user access rights, IGA can base itself on the CE's own user directory and the organizations users belong to, as defined in that directory. The IGA model takes into account the specificities of each role within each organization (in the broadest definition of this term; see next paragraph). This is the extended RBAC model, which takes into account the position of a user within an organization, just like his roles or businesses. This model takes into account the characterizations made by the various organizations and applies them to their user roles (businesses). This means that a user belonging to the larger organization will not be granted access rights that are specific to the smaller organization. Moreover, a user leaving the smaller organization to another job in the larger organization will automatically lose his or her access rights to the smaller organization's clearinghouse. Upon the modification, if permissions and accounts are added or removed, the user of the portal can configure a transition period during which the coworker can keep all or part of his previous rights. In this case, the various constraints defined in the segregation of duty rules are automatically checked to make sure that the extension of some authorizations associated with the old assignment does not conflict with the security policy. At the end of the transition period, the extended rights are automatically removed.
164.308.a.4.ii.B	**Access authorization.** Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.	Addressable	IAM Suite enables organizations to grant access users access to a variety of resources, including workstations, applications (on-premise/cloud), web resource or other type of data. Such access can be granted, not just on a per-user basis, but also based on policies that refer to the CE's organization as defined in the corporate directory. Management is therefore easy, as can be based on rules such as "administrative users in hospital A can access general medical information".
164.308.a.4.ii.C	**Access establishment and modification.** Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	Addressable	The security information base of IGA can be accessed on an as-needed basis, using a graphical interface, to modify, document, verify, generate reports and launch certification campaigns to review access rights and ensure they are compliant with security policies.

45 CFR Paragraphs	Definitions/ Requirements	Required/ Addressable	IAM Suite feature
164.308.a.5.i	**Standard: Security awareness and training.** Implement a security awareness and training program for all members of its workforce (including management).		
164.308.a.5.ii.A	**Security reminders.** Periodic security updates.	Addressable	Security experts in R&D teams are constantly on the lookout for new proven or potential threats on these modules, on security notes issued and security bulletins from different sources (CERT, Microsoft, etc.), for example regarding vulnerabilities Apache or OpenSSL. Evidian also receives security information directly from its partners. Any security patches are systematically deployed in the products as soon as possible.
164.308.a.5.ii.B	**Protection from malicious software.** Procedures for guarding against, detecting, and reporting malicious software.	Addressable	The Web Access Manager module provides users access to protected web information using a secured portal. As this portal is the gateway to PHI, it can be used to publish security reminders. In addition, this module has undergone several audits to this effect, carried out by third parties. These audits have verified that the products meet the requirements of the OWASP standard. Conformity checks were carried out before production started, and minor non-conformities were corrected within a very short time. No major risk was identified during these audits. The same principles apply to technical vulnerabilities within the meaning of the CVSS standard (http://www.first.org/cvss).
164.308.a.5.ii.C	**Log-in monitoring.** Procedures for monitoring log-in attempts and reporting discrepancies.	Addressable	Evidian IAM Suite provides comprehensive auditable data on a large array of indicators available in reports and dashboards, which includes (but is not limited to): ◀ User activity including login attempts ◀ Detailed user activity on protected web sites: user authentications, user authentications risks, password changes ... ◀ The status of access rights, either individual or rule-based Administrative actions including user definition, access granting etc.
164.308.a.5.ii.D	**Password management.** Procedures for creating, changing, and safeguarding passwords.	Addressable	Sophisticated password management features are included in IAM Suite single sign-on (SSO) modules (E-SSO and WAM). Primary password policy can be tailored to any organization's requirements (alphanumeric characters, etc.). Using graphical administration interface, password policy can be defined and is implemented automatically. This includes password expiration dates. Primary and secondary passwords are stored in an encrypted format inside SSO security directories. As a safeguard measure, secondary passwords (i.e. individual passwords for the applications handling PHI) can be managed automatically. These passwords will be defined and changed without users having any knowledge of them; they can therefore be as non-intuitive as needed. This means that manual procedures need only cover users' primary passwords.

45 CFR Paragraphs	Definitions/ Requirements	Required/ Addressable	IAM Suite feature
164.308.a.6.i	**Standard: Security incident procedures.** Implement policies and procedures to address security incidents.		
164.308.a.6.ii	**Response and Reporting.** Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.	Required	In addition to its extensive reporting, IAM Suite has predefined dashboards to survey security incidents such as highlight the risk related to user authentication based on a risk aggregation formula. The user can display the lists of users and hosts that have generated failed authentication events for a given period. An overall level of risk is computed and displayed by hour or by minute.an alerting feature that can be configured to warn security administrators when a suspicious situation occurs. Such live warnings can therefore be incorporated in the CE's procedures. A Web console provides a centralized tool to quickly diagnose the security incident and fix the issue quickly.
164.308.a.7.i	**Standard: Contingency plan.** Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.		
164.308.a.7.ii.C	**Emergency mode operation plan.** Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.	Required	IAM Suite provides options for emergency mode operation. Access to PHI remains secured in case of emergency, regardless of whether a systems-damaging accident affects the network or the IAM Suite security infrastructure itself. ◄ In case of incident on the network, access security remains active even if the EAM servers are inaccessible. Local 'cache' copies of encrypted data can be configured, on the workstations. Moreover, users' authentications rely on the Active Directory high availability (and load balancing) procedures already implemented. ◄ IAM Suite can be installed in a fault-tolerant configuration so that in case of accident, operation is automatically transferred to other security servers. This concerns both authentication and administration. Refer to "High Availability and Contingency Plan" Chapter
164.310.c	**Standard: Workstation security.** Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.		Authentication Manager client software can be installed on the user workstation to prevent access without proper authentication. It is fully compatible with physical security measures such as smart cards, one-time password (OTP) devices, biometrics, etc. Such devices can substitute for ID/ passwords in the authentication procedure.

45 CFR Paragraphs	Definitions/ Requirements	Required/ Addressable	IAM Suite feature
164.312.a.1	**Standard: Access control .** Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in Sec. 164.308(a)(4).		
164.312.a.2.i	Unique user identification. Assign a unique name and/ or number for identifying and tracking user identity.	Required	IAM suite requires such unique user identification. IGA can assign that user identification itself when the user is created or can use one that has already been defined by the CE. IGA then uses it to manage users and assign access rights.
164.312.a.2.ii	Emergency access procedure. Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	Required	IAM Suite can be deployed in a fault-tolerant configuration so that PHI is available even if elements of the security chain are temporarily unavailable. This renders both user authentication and security administration fault tolerant.
164.312.a.2.iv	Encryption and decryption. Implement a mechanism to encrypt and decrypt electronic protected health information.	Addressable	All data are encrypted during transfer using HTTPS with TLS V.1.2 The solution uses the following encryption mechanisms: ◄ Asymmetrical for connection establishments to applications / Web API (HTTP / S). ◄ Symmetric session keys. ◄ SHA-256 hash functions. The solution also uses the RSA 1024/2048, AES 256 algorithms.
164.312.b	**Standard: Audit controls.** Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.		IAM Suite supplies an audit function allowing you to store the audit events generated by the different modules of the solution in a centralized database (SQL). The security policy data is stored in a central repository. The pieces of data may be viewed through the administration console, the web portal or a web service

About Evidian

Evidian is the Identity and Access Management (IAM) software suite of Eviden.

Evidian IAM is the European leader in identity and access management with a presence which is growing rapidly beyond Europe, particularly in Japan and the US.

More than 5,000,000 users in more than 900 organizations throughout the world connect to their companies every day and manage their access rights with Evidian identity and access management solutions.

For more information, please refer to our white paper "Maintaining HIPAA Compliance with Identity and Access Management solutions"

Contact us: https://www.evidian.com/company/contact-us/

For more information: https://www.evidian.com/

CT-200807-JR-EVIDIAN-LEAFLET-HIPAA SECURITY RULE COMPLIANCE