

White Paper

HIPAA Issues You May Have to Confront



Brief Background

“HIPAA” refers to the Health Insurance Portability and Accountability Act of 1996, brought to ensure confidentiality of private health information. Since the Act was passed, the “Privacy Rule” was issued by the U.S. Department of Health and Human Services (“HHS”) as a means to implement the requirements stipulated by the act.

This document covers the Security and Privacy Amendment (Part 164) of the Privacy Rule for it has special importance regarding the security of information systems. If your organization is faced with HIPAA compliancy requirements, and your information systems reside on IBM iSeries / i5 hardware, this document offers clear answers to some difficult issues.

As laid down in paragraph § 164.318, major health plans have been required to conform to the amendment since April 20, 2005, while small health plans have been bound to comply as of April 20 2006.

Security standards

Paragraph § 164.306 defines some general rules:

- Ensure confidentiality of electronic protected health information you create, receive, maintain or transmit.
- Protect against any threats or hazards to the security or integrity of sensitive information in your system.
- Protect against any unauthorized use or disclosure of sensitive information in your system.
- Ensure compliance by your workforce.

In addressing these rules, you are required also to do the following:

- To ascertain whether your existing technical infrastructure provides a sufficient solution to these issues.
- To ascertain the probability and criticality of potential risks to sensitive information in your system.

The above requirements are easy to state, but far more complicated to implement. They require technical solutions to access control at the most granular level, auditing of many different kinds of activity, an extensive reporting capability, an automated method of assessment and a way to handle all this with simplicity and ease. The operating system of the iSeries or i5 provides only a partial solution and one that is not always easy to implement.

The following requirements are probably familiar to anyone involved in HIPAA compliance. For each we provide a quick and available solution to the issue.

§ 164.308 Administrative Safeguards.

You are required to implement policies to prevent and detect security violations.

Bsafe/Enterprise Security allows you to setup policies to both prevent and detect security violations. These can be defined for users, groups of users and for network nodes. The policies defined can be reviewed and updated at any time.

You are required to conduct a thorough assessment of potential risks and vulnerabilities to sensitive information in your system

The Bsafe/Security Assessment provides a means of checking system definitions, assessing their affectivity and recommending any changes, if necessary.

Additionally, it includes a unique penetration attack simulation and full report of all results, including graphs and summary.

You are required to implement measures that are sufficient to reduce these risks and vulnerabilities to a reasonable and appropriate level.

The more specific issues below will provide detailed answers to this general paragraph.

You are required to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

Bsafe/Enterprise Security has sophisticated auditing tools build in. These include, dozens of pre-shipped reports for all different kinds of system activity and network access, means of monitoring data changes, read-record access at the field level and SQL statement logging. The system allows scheduling for automatic, periodic running and for previewing and saving reports for viewing in a spreadsheet application.

You are required to implement policies and procedures to ensure that all members of the 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.

Bsafe/Enterprise Security provides a granular mechanism of allowing access to those who are authorized, while denying access to those who are not. Various forms of group permissions keep maintenance to a minimum.

You are required to implement procedures for the authorization and/or supervision of work with electronic protected health information by location (where it might be accessed).

Location restriction is handled in Bsafe/Enterprise Security through permissions at the level of IP address ranges with or without a secondary level of granularity of user, user group, application server.

You are required to implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required.

That's easy with Bsafe/Enterprise Security. User access to system resources, application servers can be granted and revoked quickly and simply through the product's intuitive GUI.

© Copyright 2006 Bsafe Information Systems, Ltd. All rights reserved. This document is the property of Bsafe Information Systems, Ltd. It cannot be reproduced or duplicated without the permission of Bsafe Information Systems. www.bsafesolutions.com

Tel: +1-201-5030021 +972-9-9610400 (all regions).



Updated 28 June 2006

You are required to 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.

Bsafe/Enterprise Security excels in granting access at many different levels. These include user, group profile, custom user group, generic name – even IP address within or outside of your local network. Further examples of this granular level are access to remote command which can be permitted for each user or group down to specific commands and called programs and database access down to the type of operation and specific files and libraries.

You are required to 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.

Policy may be reviewed and modified in Bsafe/Enterprise Security at every level from the general system level down to specific user level. Changes to policy can be monitored and later reported, if required.

You are required to implement a security awareness and training program for all members of your workforce, including management.

Firstly, the easy-to-use GUI has been designed for administrators who are not skilled experts in iSeries security. It provides an intuitive integrated environment through which many of the product's users learn much about managing the security of their i5 / iSeries machines. To this you can add the full, context-sensitive, on-line help, a large selection of free, downloadable tutorials and presentations and free product training sessions from Bsafe Information Systems.

You are required to have procedures for guarding against, detecting, and reporting malicious software.

The issue of malicious software is somewhat different on the iSeries platform than other platforms, like the PC. First of all, if the malicious software tries to update the IFS, then Bsafe/Enterprise Security can protect against changes in IFS folders. If, on the other hand, the malicious software is a custom script or program produced by someone within the organization, then the locking down of 'unusual' means of accessing the system, like remote command and SQL scripting, is probably the most effective means of protection. All of these are standard modules of the product.

You are required to have procedures for monitoring log-in attempts and reporting discrepancies.

All network log-in attempts, native signons and signoffs can be monitored. Failed attempts through invalid user, invalid password or lack of

authorization are monitored, logged, reported and instantly alerted if you so choose, with Bsafe/Enterprise Security.

You are required to be able to identify and respond to suspected or known security incidents;

Identify security incidents through a host of reports, a sophisticated multi-faceted graphic analyzer, instant alerts and on-line inquiries with full filtering capability.

You are required to perform a periodic technical and non-technical evaluation, based initially upon the standards implemented and subsequently, in response to changes affecting the security of electronic protected health information

Bsafe/Security Assessment provides a means of checking system definitions, assessing their affectivity and recommending any changes necessary. Additionally, it includes a unique penetration attack simulation and full report of all results, including graphs and summary.

§ 164.312 Technical Safeguards.

You must implement technical policies and procedures for information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights.

Bsafe/Security Assessment provides a uniquely rich and granular system of protection that controls access at user, user group and IP address levels to application servers, functions and objects.

You are required to implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

This feature is built into Bsafe/Enterprise Security

You are required to implement a mechanism to encrypt and decrypt electronic protected health information whenever deemed appropriate.

The Field Masking module of Bsafe/Enterprise Security allows you to mask specified fields in database files from the mainstream of users while allowing authorized users to view them. Among the masking options, is encryption.

You are required to implement audit controls - mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

Bsafe/Enterprise Security has sophisticated auditing tools built in. These include, dozens of pre-shipped reports for all different kinds of system

© Copyright 2006 Bsafe Information Systems, Ltd. All rights reserved. This document is the property of Bsafe Information Systems, Ltd. It cannot be reproduced or duplicated without the permission of Bsafe Information Systems. www.bsafesolutions.com

Tel: +1-201-5030021 +972-9-9610400 (all regions).



Updated 28 June 2006

activity and network access, monitoring of field changes, read-record access at the field level and SQL statement logging.

You are required to implement policies and procedures to ensure integrity - to protect electronic protected health information from improper alteration or destruction and to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

This requires the implementation of both protection and monitoring as information sometimes gets altered by authorized users, in an unauthorized way. Application Access Control, File Audit and a GUI-based Object Authority management facility all combine to ensure this integrity.

You are required to ensure transmission security, by implementing technical security measures to guard against unauthorized access to electronic protected health information transmitted over a communications network. Integrity must be ensured so that electronically transmitted electronic protected health information is not improperly modified without detection.

The connection between the PC-based GUI and the server protecting software is secured by SSL. The locking down of various Application Servers ensures that network transactions like FTP and ODBC are strictly controlled.

§ 164.314 Organizational requirements.

You are required to ensure that the measures detailed above apply also to business associates and wherever possible, to implement administrative, physical, and technical safeguards to protect the confidentiality, integrity and availability of the electronic protected health information.

The issue here can be split into two. 1-the information residing on the business associate's systems and 2-allowing access of the business associate to information on your system. The first of these can be facilitated by implementing security and auditing software like Bsafe/Enterprise Security also on the associate's computers. The second is handled no differently to your internal users, as detailed in the above paragraphs. You have the same latitude of control and auditing wherever users are located.

§ 164.316 Policies and procedures and documentation requirements.

You are required to document your policies and procedures and changes made in them

The product includes features that can document and save to history, any changes in policy for network access permissions, system values, authority changes and system auditing policy changes.

See more about Bsafe Information Systems products: www.bsafesolutions.com

© Copyright 2006 Bsafe Information Systems, Ltd. All rights reserved. This document is the property of Bsafe Information Systems, Ltd. It cannot be reproduced or duplicated without the permission of Bsafe Information Systems. www.bsafesolutions.com

Tel: +1-201-5030021 +972-9-9610400 (all regions).



Updated 28 June 2006