

Paylogix® HIPAA Compliance



Paylogix® is providing this statement concerning HIPAA (Health Insurance Portability and Accountability Act) to our customers in order to assist you in your planning and decision making efforts. Paylogix® understands the significance of this regulatory requirement and wishes to facilitate our customers' goals of HIPAA compliance.

Paylogix® services and products are built to address the four key areas of HIPAA. These areas include: Transaction and Code Set Standards, Privacy Standards, Security Standards and Uniform Identifier Standards. [HIPAA - 070504]

The table below lists the key HIPAA components that are addressed by the HIPAA compatible versions of Paylogix® systems. The items shaded in gray are not addressed in Paylogix® products as they are either not a requirement for our client base or are not yet approved HIPAA standards.

The Frequently Asked Questions section addresses specific questions that have been received from existing clients. Please refer to that section before submitting additional questions to Paylogix®. If this position statement does not answer your questions, please send them to us.

HIPAA At A Glance

HIPAA Components	Component Item	Compliance Date	Supported
Transaction Set Standards	ASC X12N 837 Professional, Institutional Claims and Coord. of Benefits		No
	ASC X12N 270-271 Professional, Institutional Eligibility and Benefit Inquiry		No
	ASC X12N 278 Referral Certification/Services Review		No
	ASC X12N 276-277 Claim Status		No
	ASC X12N 834/4010 Enrollment and Disenrollment		No
	ASC X12N 835/4010 Professional, Institutional Payment and Remittance Advice		No
	ASC X12N 820/4010 Premium Payments	10/2002	Yes
	NCPDP V5.1 Retail Drug Claims, Coord. of Benefits and Eligibility Inquiry		No
	ASC X12N 148/4010 First Report of Injury		No
	ASC X12N 275/4010 Health Claims Attachments		No
Code Set Standards	Diagnosis Codes - ICD9 International Classification of Diseases, 9th Edition, Vol. 1&2		No
	Procedure Codes - CPT-4 Current Procedural Terminology, 4th Edition		No
	Coding for Inpatient Services ICD9, Volume 3		No
	Other Procedure Codes HCPCS: Healthcare Procedure Coding System, Level 2		No
Privacy Standards	Authorization	10/2002	Yes
Security Standards	Administrative Procedures	10/2002	Yes
	Physical Safeguards	10/2002	Yes
	Technical Security Services	10/2002	Yes
	Technical Security Mechanisms	10/2002	Yes
	National Provider Identifier		No
Uniform Identifier Standards	Employer Identifier	10/2002	Yes
	Health Plan Identifier		No
	Unique Healthcare ID for Patients		No

Who is the Paylogix® contact for HIPAA?

The primary contact for HIPAA is Richard Pfadenhauer. He may be reached by any of the following:

Phone: 516-408-7800
Email: richardp@paylogix.com
Fax: 516-408-7100
Mail: 1025 Old Country Road
Suite #310
Westbury, New York 11590

Is there a cost involved with the implementation of a HIPAA compliant release of the Paylogix® system?

As always, product updates are provided free of charge. However, if a customer requires additional training, that will be billed at our regular rates.

Is there a web site for HIPAA updates?

No. As stated above, the Paylogix® web site will provide information about HIPAA as it relates to Paylogix® products. Updates will continue to be available when released.

Is Paylogix® customer data shared with any other organization?

No. Paylogix® use of shared data is restricted to the support and servicing needs of the client. This data is not shared with any other organization.

How does Paylogix® facilitate the compliance with HIPAA regulations for its Business Associates?

Paylogix® has taken the initiative to require the Acceptance of Terms prior to access to information contained within Paylogix®.

Does the application require individuals to logon before they can access data?

Yes.

Does the application include optional logon capabilities? (e.g. logon requirements can be "turned on" or "turned off" by an administrator?)

No. The application requires logon by the user. The administrator, the client or the user cannot turn off this feature.

Does the application include optional password capabilities? (e.g. password requirements can be "turned on" or "turned off" by an administrator?)

No. The password is required by the application. The administrator, the client or the user cannot

turn off this feature.

Are there any situations where a user can access data in the application without using a login and password?

Not through the use of the system. However, if the user has rights to the drive and access to a product that will allow them to access a SQL database, they could access the data external to the system (Helpdesk personnel from Paylogix® require this capability). Your company's network security would address this issue.

What are the requirements for passwords?

Minimum number of characters: Six (6).
Maximum number of characters: Fifteen (15).
Numbers allowed: Yes.
Numbers required: No.

Can password changes be made mandatory after a certain period of time?

Yes. This is an option and the administrator sets the period between changes.

Is the mandatory change requirement system or user controlled?

The administrator controls it. Once the parameters are set, the system will require changes per those parameters.

Does the application limit the maximum number of invalid attempts for access?

Yes. The maximum allowed number of incorrect attempts is three.

Does the system provide audit information about access to data?

Yes. The system logs user access to data and records the changes made to data by individual users.

How is security configured in the system?

The systems base security on both user roles and individual user access. Each user is established as a unique entity in the system. In addition, the access to system functions is controlled by the roles assigned to the user.

What are "Technical Security Mechanisms"?

This applies to the security of data that is transmitted over a network. These mechanisms guard data from interception while in transit through a network. They also guard against access to internal systems from external access points such as dial in lines or open IP addresses.

How does Paylogix® address these standards?

Paylogix® has adopted industry standard methods such as those offered by Verisign to create a unique key for each individual that can be authenticated by other parties.