



SUMMARY OF ICARDIOGRAM HIPAA COMFORMANCE PROCEDURES

Icardiogram achieves conformance to HIPAA guidelines through established procedures that protect healthcare information (PHI).

I. ADMINISTRATIVE PROCEDURES:

1. A Business Associate agreement is required between Icardiogram and all U.S. facilities and/or groups sending PHI to the Icardiogram server. In addition, Icardiogram allows physicians to access information only after their HIPAA compliance officer has certified them as trained in HIPAA guidelines, and after they have been provided an unique username and password. Icardiogram does not make use of group passwords that are in frequent use by other organizations.
2. Access to PHI is regulated through passwords which can only be awarded by limited personnel in the organization, and all access to PHI is subject to audit.
3. Clients are responsible for the physical and technical security of their EchoEncoder units, and other items purchased from Icardiogram. All computer systems that have PHI are password protected, and maintenance of that level of security is both the responsibility of the client and Icardiogram. Icardiogram maintains a record of all installations.
4. Procedures for the reporting of HIPAA violations are in place.
5. Icardiogram maintains a secondary server at its office site, and maintains an additional data repository off site. Routine virus checking is performed. Physical security is provided, as well as backup electrical generator power at the server site.

TECHNICAL SECURITY SERVICES TO PROTECT DATA:

1. Access control
 - a. Encryption.

All transfers to and from the Icardiogram server utilize SSL 128 bit encryption.

Cardiologists are expected, though their own HIPAA awareness program(s), to be aware that downloaded data in their possession is now the responsibility of the Cardiologist and no longer under the control of Icardiogram. Through the use of Quicktime Pro, it is possible for cardiologists to save the video as a file on a hard drive or other physical media,

but, once again, the data in that form is believed by Icardiogram to be the responsibility of the cardiologist that has downloaded the study.

b. Procedure of emergency access.

Emergency access to data from the Covered Entity or the interpreting cardiologist can be accomplished by personal telephone call from the entity requesting emergency information. Such request will be considered by an Officer of the Company, and will be recorded for auditing purposes.

c. User-based access.

Access to PHI from clients of Icardiogram is limited to individuals who are designated to view said information.

2. Audit controls.

Audit controls are in place.

3. Data Authentication.

Video data received by the IC server is authenticated to be genuine by the requirement for a password to access the IC server.

4. Entity Authentication.

a. Automatic logoff.

b. Password with unique user identification.

Each individual that sends or receives data from the Icardiogram server will not be allowed to do so without identification with a username and password. The initial identification of the individual, and permission to access the server, is arranged with the Covered Entity using a password access form (see below). In this way, Icardiogram knows the identity of all individuals that are permitted to interact with the server.

It is necessary for individuals to enter their username and password to access the echocardiograms on the server.

Icardiogram is familiar with situations where many users use the same password to log onto a server (for instance, the popular use of "Echoclinical" in the Phillips EnConcert system). Such collective use of password and username access is common and completely defeats the intention of the HIPAA safeguards. All users of the Icardiogram site have unique usernames and passwords, the security of which must be maintained by the user with auditing performed by Icardiogram.

TECHNICAL SECURITY MECHANISMS TO PROTECT DATA:

1. Communications/Network controls.

a. Access controls.

Icardiogram servers are protected by the need for password access, as well as physical access for some operations.

b. Audit trail.

All access to Icardiogram servers is monitored and recorded in a manner that can be readily accessed and reviewed by Icardiogram.

c. Encryption.

d. Entity authentication.

e. Event reporting.

All security events are recorded and responded to by Icardiogram, with reporting to the Covered Entity.

f. Integrity controls.

Icardiogram's HIPAA Compliance Officer routinely evaluates the quality of echocardiograms stored on the IC server.

g. Message authentication.

E-mail messages do not contain PHI, but contain a "link" to PHI on the Icardiogram site; access to that PHI requires use of a username and password.

MORE INFORMATION IS AVAILABLE UPON REQUEST.

Following are two sample password access forms used by Icardiogram to facilitate the above procedures:



REQUEST FOR ACCESS TO PROTECTED HEATHCARE INFORMATION RESIDING ON THE CARDIOGRAM SERVER.

To: David Reaugh
Data Security Officer
Icardiogram, Inc.

From: (Covered Entity)
HIPAA Compliance Officer

Date: _____

The following individuals are allowed to access protected healthcare information on the Icardiogram Server, and should be provided with all password access necessary to obtain such information. By making this request, we are informing you that all of these individuals are fully cognizant of and have been trained in HIPAA regulations regarding the confidentiality of the healthcare information that will be accessed.

	Name and Title (if applicable)	E-mail address	Access Authorization (e.g., all or part of information sent by our organization to the server)



REQUEST FOR REMOVAL OF ACCESS TO PROTECTED HEALTHCARE INFORMATION RESIDING ON THE ICARDIOGRAM SERVER.

To: David Reaugh
 Data Security Officer
 Icardiogram, Inc.

From: (Covered Entity)
 HIPAA Compliance Officer

Date: _____

The following individuals are no longer to be allowed access to protected healthcare information on the Icardiogram Server, and should no longer be provided with password access necessary to obtain such information. Please remove such access immediately.

	Name	Title	Access Authorization (e.g., all or part of information sent by our organization to the server)
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			