VAREQUE

Strictly Confidential Document

Vareque HIPAA White Paper

At Vareque, We are committed to complying with all federal and state regulations for privacy and security. If you feel that there is something we should address, please feel free to contact us at **contact@vareque.com** for further clarification or questions or visit us at **http://www.vareque.com**.

We understand the concern of our clients and their providers and business partners. To this end we have built the V-DoX™ platform with "Privacy and Security" as our top design constraint. Each contact with the V-DoX is documented by a IP stamp and date and time. We display the IP stamps and Unique ID's on our "monitors" at all times. These monitors can be viewed or can transform into 'protected' PDF printable reports which document the transactions between our server and a password protected user.
Our endeavor is to the spirit of the regulations aimed at achieving the following:

- Ensure the internal protection of individual health information and implement physical and administrative safeguards;
- Limit the use and disclosure of patient information to meet the "minimum necessary" standard;
- Accounting and auditing of all disclosures;
- Allow only registered individuals to amend their health information;
- Ensure the confidentiality, integrity, and availability of all electronic data created, received, maintained, or transmitted by Vareque
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required

At Vareque we have implemented systems and procedures for HIPAA compliance which fall into the following three categories:
1. Administrative Procedures
2. Physical Safeguards and
3. Technical Data Security.

1. Administrative Procedures:

We have established a HIPAA Compliance Management Committee consisting of the CEO and other managers. The HIPAA Compliance Committee performs internal assessments and audits, performs gap analyses, conducts training, sets policies for security and access to components, and monitors the HIPAA implementation rules on an ongoing basis and assigns activities and responsibilities to ensure compliance.
All users and associates who are given access to customer data or customer records are required to sign a confidentiality agreement before they can start work. All business partners with access to protected information must enter into a business associate agreement that requires full compliance with all HIPAA requirements and safeguards.

2. Physical Safeguards:

Our servers are housed in a state-of-the-art data center. The servers

☑ Run on fault-tolerant systems!

☑ Utilize smart-routing to ensure "speed of light" loading time!

☑ Provide utmost redundancy at any time!

☑ The data center is physically secured and requires the use of special electronic access codes to enter.

☑ Logs of all entry and exit from the facility are automatically maintained.

☑ The data center facilities are equipped with climate control systems, fire detection and suppression systems, and backup UPS and generator.

3. Technical Data Security:

This category includes systems and procedures used to protect, control, and monitor information access and include processes used to prevent unauthorized access to data transmitted over a communications network. Security is addressed at all layers: physical, network, database, application, and user.

☑ **Network Security**

All our servers and databases are located on a secured internal network that is protected by Firewall (hardware firewall) that employs IPSEC encryption built-in.

☑ **Database Security**

We use the MySQL databases and implements the SQL Server Security Model whose guidelines are at http://dev.mysql.com/doc/mysql/en/Security_guidelines.html. In summary, this model addresses security at multiple layers including securing access to the server, securing access to the database, securing access to database objects, and securing access through application roles.

☑ **Application Security**

The proprietary V-DoX applies 128-bit encryption to all files prior to any file transmission via the public Internet. This uses the standard SSL (secure socket layer) with 128-bit encryption strength. Attempts to
(More information about SSL is at http://www.rsasecurity.com/standards/ssl/basics.html)

☑ **User Security & Audit Trail**

Access to the V-DoX is limited to registered users only. Users must provide their username and password (which are shadow encrypted) to gain entry. A complete audit trail is maintained including user session information. All database transactions are logged with IP stamps. A sample of the report is show below.

V-DoX Activity Log - Microsoft Internet Explorer

File   Edit   View   Favorites   Tools   Help

Back | Search   Favorites   Media

Address https://www.vareque.com/jobs/comlog.php   Go   Links

ACTIVITY MONITOR
Date : 2004-07-06 | Time: **11:02:13**. Last 30 days | Last 7 days

>>>> West Valley Medical Partners Activity log for the last 20 days<<<<

Show only

Select | Showing job list from 2004-06-16 | 20 | days | Range

No.	Activity	Job ID	Details	Ref ID	Name	Date	Time	IP
Activity Monitor for John Anderson MD since 2004-06-16	Print Version							
1	Print	14420		56423	Kathy Crowe	2004-06-18	09:31:25	208.36.167.27
2	Email	14420	bbisceglia@axiominternet.com	56423	Kathy Crowe	2004-06-18	11:13:21	208.36.167.27
3	Email	14420	bbisceglia@axiominternet.com	56423	Kathy Crowe	2004-06-18	11:14:01	208.36.167.27
4	Email	14420	bbisceglia@axiominternet.com	56423	Kathy Crowe	2004-06-18	11:14:56	208.36.167.27
5	Email	14420	bbisceglia@axiominternet.com	56423	Kathy Crowe	2004-06-29	14:40:12	208.36.167.27
6	Print	14423		5478	Elise Jameson	2004-06-18	09:34:36	208.36.167.27
7	FAX	14425	18053838028	0	Jeffrey Hessman	2004-06-29	15:28:50	68.233.156.20

2004©Vareque