TECHNICAL FAQ

Overview

NPAR™ is a secure, web-based database service. Its easy-to-use screens allow authorized users to quickly locate and retrieve a patient's antibody records and transfusion history from any participating blood bank or transfusion service. NPAR features a fully automated data entry process, so it is scalable to institutions of all sizes.

1. What software will we receive?

NPAR is a Software-as-a-Service ("SaaS") offering. You only need to install one program called the Upload Manager. It interfaces to your hospital's blood bank computer system and uploads patient history to the NPAR Server.

After the installation is completed and verified, the application requires no regular maintenance or administration.

2. What computer does the Upload Manager run on?

The NPAR Upload Manager runs a customer-supplied Windows platform, Vista or later, with a minimum of 2 GHz CPU, 2GB of RAM, and 500 MB of free disk space. This platform must have LAN access to the hospital blood bank computer system, and Internet access for daily uploads to the NPAR Server.

3. How does the Upload Manager import patient data from our blood bank software?

The data export method varies by software vendor, relying on published interface methods wherever possible. We can also import from formatted database output.

4. How often does NPAR update its data?

The NPAR Upload Manager uploads patient data once a day.

5. What are the license fees for the Upload Manager?

The Upload Manager is included with the NPAR service at no extra charge.

6. How will I know if the upload process is working?

If the NPAR Server does not receive a successful upload on schedule, both the hospital's NPAR administrator and the NPAR tech support team are notified, and corrective action is initiated. The NPAR Server also provides an upload history report.

7. How much network bandwidth will each upload use?

An upload file of 100,000 patient records is about 7.4MB.

8. How long does the Upload Manager installation take?

Installing and configuring the NPAR Upload Manager takes about 15 minutes. You will need to open dedicated ports on your Internet firewall to allow the Upload Manager to communicate with the NPAR Server.

9. What hardware will our end users need?

The NPAR user interface is completely web-based, and supports Microsoft Internet Explorer® 7 or later, Google Chrome™, and Mozilla Firefox®. Any platform running one of these browsers is acceptable. Desktop virtualization products such as Citrix and VMware View may also be used.

10. How is authentication handled?

All access requires a valid user ID and password. User accounts are managed by the hospital's designated NPAR site administrator. Standard security practices apply, including password strength, password aging, and locking out users after excessive login attempts.

11. How does NPAR ensure data privacy?

All communications with the NPAR Server use the TLS (formerly SSL) protocol with 256-bit keys. Electronic Protected Health Information (ePHI) is encrypted when stored on persistent media.

SSNs, if provided, are hash-encrypted by the Upload Manager prior to transmission, using the SHA1 algorithm with an added "salt" value. Patient SSNs are never transmitted to or stored on the NPAR Server, and therefore are not vulnerable to loss.

12. Where are the servers housed?

The NPAR Servers reside at a top-tier hosting firm, with highly secure facilities that include 24x7 staffing, redundant power and networking, fire suppression, and biometric access controls.

13. Have any independent parties reviewed NPAR security?

NPAR engaged a recognized Internet security firm to perform a security audit, and has implemented all recommendations. In addition, several top healthcare chains have reviewed and approved our security practices.

14. What about technical support?

Users can obtain support via our trouble ticket system (support.npar.com), context-sensitive help screens, and a 24x7 telephone hotline.

15. How can I learn more about how NPAR works in the blood bank?

Please read the accompanying Clinical FAQ.

16. Our legal department / risk manager / privacy officer will have additional questions. What information can I give them?

Please read the accompanying Privacy FAQ.