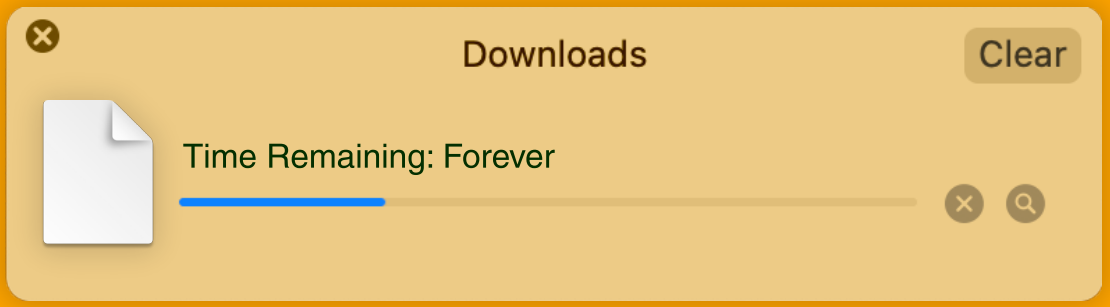
Optimizing Your Network for Eyefinity Cloud

eyefinity™

a vsp vision company

1. Right-sizing Your Bandwidth



When making a decision about your practice's bandwidth provision, the aim is to strike the ideal balance between the two undesirable extremes of overestimating and ending up paying for more bandwidth than you need, or underestimating and finding that your network can't cope with your practice's demands.

Number of Practice Users*	Minimum Bandwidth Speed	Recommended Bandwidth Speed
1–5	5 Mbps download 3.5 Mbps upload	10 Mbps download 5 Mbps upload
6–10	10 Mbps download 5 Mbps upload	20 Mbps download 10 Mbps upload
11–15	20 Mbps download 10 Mbps upload	30 Mbps download 15 Mbps upload
16–20	30 Mbps download 15 Mbps upload	50 Mbps download 20 Mbps upload
21+	50 Mbps download 20 Mbps upload	100 Mbps download 25 Mbps upload

* Number of users is based on the number of practice users (doctors, staff, and patients) simultaneously using Eyefinity cloud products (Eyefinity Practice Management, AcuityLogic, and Eyefinity EHR, including the patient kiosk) at the practice location.

Ensure you're getting what you paid for.

To verify your practice's actual bandwidth, go to www.speakeasy.net/speedtest and select the city closest to you. If your bandwidth does not meet the minimum requirements for your practice type, contact your internet service provider (ISP).

If your bandwidth is too slow or your software is struggling to perform, you may need to ask your ISP about other service options. Higher bandwidth levels may be more expensive, and it is best to shop around and consider multiple ISPs whenever possible. If telephone lines in your area are degraded, see if cable internet is available.

2. Managing Your Network Traffic

One of the biggest challenges a practice may have when managing internet bandwidth is making sure most of the bandwidth is directed and available to practice management and EHR business application software.

Internet-dependent technology has become more prevalent in the healthcare industry, whether it's a doctor using a tablet to access an electronic medical record or a patient taking advantage of a guest network while waiting. The challenge is the competition for network resources and the impact to a particular group's activities.

Prioritize clinical applications on your network.

Give your critical applications like Eyefinity Practice Management and Eyefinity EHR priority over less important traffic. Create a policy to guarantee the necessary amount of bandwidth for these applications to ensure healthcare teams can quickly access, download and share the clinical information they need from any facility at any time of day.

Restrict recreational activity.

Ensure video streaming and social media activity doesn't overwhelm your network and impede the performance of your critical apps, implement traffic policies. Allocate the right amount of resources to this recreational traffic so patients can still access these applications, but not at the expense of mission-critical services like EHR, and practice management software.

- Have a sensible guest network policy. Limit the number of devices that can connect to the guest network.
- Limit the number of personal nonbusiness devices that can access the network.
- Limit video streaming.
- Limit music and radio station streaming.

3. Choosing the Right Connections

In the not-so-distant past, networks had to be wired with computers and devices connected by cables. Today, wireless networks are more commonly used, allowing doctors and staff to access the network from anywhere the wireless signal reaches. As a result, flexibility across the office is enabled by the ability to connect to the network via mobile devices.

However, wired (or Ethernet) networks have some advantages, including greater security, better reliability, and faster speeds. Wireless networks are prone to dropping out if too many devices use the network at once. Even weather can affect connectivity. Many practices incorporate both wired and wireless access into the network.

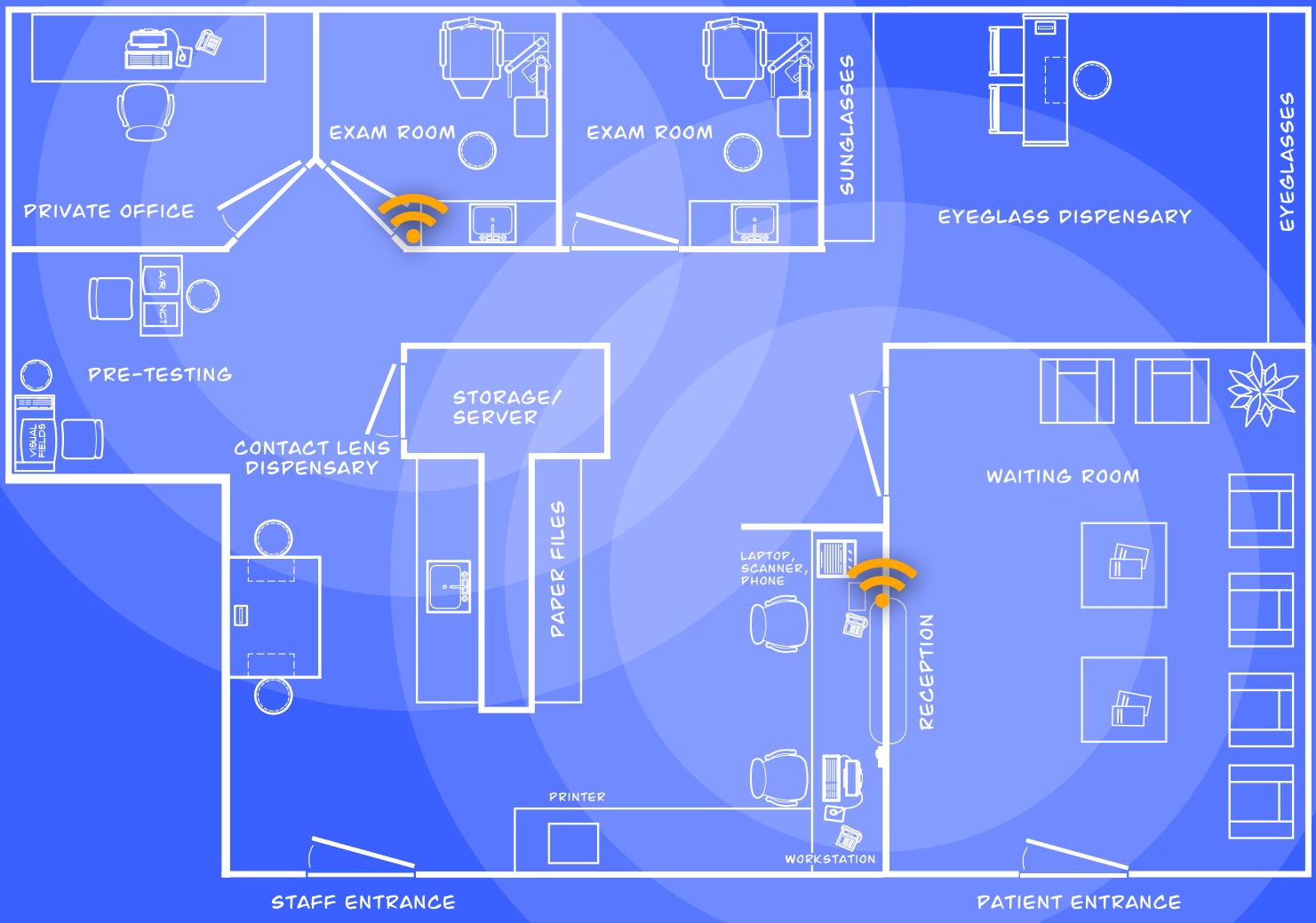
Use wired (or Ethernet) connections whenever possible.

If you're adding more Ethernet connections to your practice or building your new practice from the ground up, be sure to request **Category 6** (Cat-6) Ethernet cables. Cat-6 offers superior speed and performance.

Choose the right wireless router.

You'll need a router to connect your devices to the internet wirelessly. Select a business-grade router and enable wireless security and encryption for HIPAA compliance.

4. Setting Up Wireless Access Points



1,000 SQ FT PRACTICE

In open space, Wi-Fi routers can reach up to 150 feet. However, that 150-foot range can be quickly cut down due to several factors:.

- **Physical obstructions.** walls, doors, and air-conditioning ducts
- **Electromagnatic interference.** diagnostic equipment, the microwave in the breakroom, x-ray imaging in the dentist's office next door
- **Radio interference.** other wireless devices, including Bluetooth headphones

Installing wireless access points throughout your practice will boost wireless signals and increase internet speeds.

Deploy the right number of access points.

You don't need to add a wireless access point to every room. Be strategic in where you place access points to blanket the office with even coverage and avoid interference. You'll know a wireless access point needs to be added to a building area whenever the wireless signal does not reach full bars.

When setting up a new wireless access point, install it in a location that will be unlikely to cause radio interference (e.g., away from diagnostic equipment and thick construction materials).

The image on the previous page illustrates a 1,000 sq. ft. office space that shows recommended placement for multiple wireless access points in the exam room area.

5. Securing Your Network

Protecting patient data is a critical responsability of your practice. Here are some suggestions to help you protect sensitive information.

Set up a guest network.

If you decide to allow staff or patients to connect to your wireless network with their personal devices, consider setting up a guest network. A guest network allows you share your internet bandwidth without sharing your network password or allowing imporpper access to confidential data on your network. See also **“2. Managing Your Network Traffic”**

Secure your network.

Here are some steps you can take to secure your network and protect your data:

- Change the default administrator password to one that is long and complex.
- Turn on the firewall.
- Turn on wireless encryption.
- Physically secure the router. Internal hackers can physically reset the router and return it to factory settings, opening it to illicit access. Keep your router in a secure place.
- Choose a wireless password that is reasonably complex and difficult for unauthorized people to guess. Pick a phrase with at least eight characters, take its initials and replace some of those letters with numbers and other characters and mix up the capitalization.

Allow access for practice and clinical software.

Open the following firewall ports to allow Eyefinity Practice Management and Eyefinity EHR to access your network:

- **Port 443** for HTTPS (browser and iPad)
- **Port 80** for HTTP (browser and iPad)
- **Port 8036** for iProfiler by Zeiss (Visual Equipment Interface)

6. Managing Your Mobile Devices

Get the right mobile devices.

When acquiring a new iPad, you should always purchase the latest model to ensure the longest useful life. Apple supports each model for about five to sixyears with iOS updates. Purchasing a cheaper, older model may cost you more money in the long run becasue you'll need to replace the device sooner.

To see a complete list of iPad models supported please visit www.eyefinity.com/electronic-health-records/eyefinity-ehr/sys-req.html.

Secure your mobile devices.

The tablet industry has seen explosive growth over the last decade. Integrating tablets into healthcare environments has created a need for smart, effective ways to mount and secure these devices. Many companies have designed products that secure the iPad without compromising its aesthetics or user experience.

A great selection of security devices can be found at www.tryten.com/ipad-products.

Get help if you need it.

These vendors specialize in practice networking and hardware and are familiar with Eyefinity software requirements.

- **Think Smart Inc.** 800.941.4913 or sales@thinksmartinc.com
- **North Shore Computing.** 631.234.1200 or omsupport@nscomputer.com

eyefinity™
a vsp vision company