digicert®

DigiCert® UltraDNS

Healthcare provider readiness checklist

Is your DNS infrastructure ready to support critical healthcare experiences? Use this checklist to identify gaps in availability, performance, security, and scalability.

1. High availability and traffic management setup

- [ ] **Deploy a redundant secondary network:** Implement an independent, secondary Anycast network (such as UltraDNS²) alongside your primary carrier to distribute traffic.
- [ ] **Configure intelligent failover:** Set up automated traffic rerouting so that if a primary carrier experiences an outage, traffic shifts in milliseconds to keep emergency portals and electronic health records online.
- [ ] **Enable geolocation-based routing:** Configure user data to route automatically to the closest cloud node across a global network. This minimizes latency for virtual visits and ensures critical biometric data transmits instantly for remote care.
- [ ] **Optimize advanced load balancing:** Balance your network traffic to optimize website performance and prevent application lag during sudden surges in telemedicine usage or unexpected traffic spikes.

2. Automated security and administrative configurations

- [ ] **Automate Domain Control Validation (DCV):** Integrate your DNS platform with DigiCert® ONE to handle DCV automatically. This eliminates manual setup risks, misconfigured records, and administrative delays as your clinical network grows.
- [ ] **Automate DNS TXT record renewals:** Ensure DNS TXT records are configured to automatically renew and validate in seconds. This eliminates expired certificate warnings and disruptive security alerts that confuse patients and discourage portal usage.
- [ ] **Enforce granular access management:** Set up easy-to-use administration tools with granular access permissions to control who can alter DNS settings.
- [ ] **Enable real-time alerts:** Turn on real-time notifications for any modifications made to your DNS to immediately flag and prevent malicious or accidental administrative errors.

3. Patient security and trust implementation

- [ ] **Activate one-click DNSSEC:** Deploy Domain Name System Security Extensions (DNSSEC) to secure the chain of trust and instantly halt cache poisoning attacks, protecting sensitive patient health information.
- [ ] **Integrate DMARC email authentication:** Implement DMARC capabilities to continuously monitor your domains, stopping threat actors from spoofing healthcare domains and conducting phishing fraud against patients.
- [ ] **Establish DDoS and ransomware defenses:** Ensure your underlying DNS infrastructure is backed by robust, globally distributed scrubbing capacity to withstand sustained DDoS attacks, mitigate ransomware threats, and protect sensitive personal data.

4. Verification and operational continuity checklist

Before opening services fully to patients, verify that your IT infrastructure aligns with the following metrics:

- [ ] **Verify 100% uptime Service Level Agreements (SLA):** Ensure your DNS provider guarantees a 100% uptime SLA backed by a highly resilient global architecture to eliminate network-driven care disruptions.
- [ ] **Confirm regulatory compliance:** Double-check that your built-in secure configurations adhere to strict geographical restrictions and absolute patient data privacy regulations.
- [ ] **Establish 24/7/365 expert support:** Confirm that you have a direct line of contact to a dedicated Security Operations Center staffed by technical experts who understand the urgency of healthcare applications.
- [ ] **Test the end-to-end patient experience:** Perform a simulated run-through to ensure patients experience zero connection friction, low-latency interactions, and immediate access during digital check-ins, telemedicine portals, and inventory management workflows.

Are you ready for peak demand?

If you can't confidently check every box on this list, your DNS infrastructure may be putting availability, performance, and patient trust at risk.

DigiCert UltraDNS is designed to help healthcare providers meet these requirements with global scale, built-in security, and high-performance DNS resolution. Get the solution sheet to see how.

About DigiCert

DigiCert is a global leader in intelligent trust. We protect the digital world by ensuring the security, privacy, and authenticity of every interaction. Our AI-powered DigiCert ONE platform unifies PKI, DNS, and certificate lifecycle management to secure infrastructure, software, devices, messages, and AI content, agents, and models. Learn why more than 125,000 organizations, including 90% of the Fortune 500, choose DigiCert to stop today's threats and prepare for a quantum-safe future at www.digicert.com