Telehealth HIPAA Compliance Checklist

NORTHEAST TELEHEALTH RESOURCE CENTER NETRC.org

A Practical Guide for Healthcare Organizations and Providers

This checklist outlines key actions healthcare organizations and providers can take to help ensure telehealth services comply with the HIPAA Privacy, Security, and Breach Notification Rules.

The checklist reflects guidance from the Center for Connected Health Policy (CCHP), Regional Telehealth Resource Centers (including the Northeast Telehealth Resource Center), and federal HIPAA standards applicable nationwide.

HIPAA compliance in telehealth requires intentional planning, secure technology, trained staff, and ongoing monitoring. By following this checklist and using trusted national and regional resources, healthcare organizations and providers can help ensure telehealth services protect patient privacy, meet federal requirements, and align with Northeast regional expectations.

1 | Governance and Administrative Safeguards

	Designate HIPAA leadership Assign a Privacy Officer and Security Officer responsible for HIPAA compliance, including oversight of telehealth technologies and workflows.
	Conduct a HIPAA risk analysis Perform and document a risk assessment that explicitly includes: • Telehealth platforms and video tools • Remote access systems • Remote patient monitoring devices • Home-based provider workflows
	Update policies and procedures Ensure HIPAA privacy and security policies explicitly address telehealth services, including virtual visits, messaging, and remote documentation.
	Maintain documentation Retain records of risk assessments, policies, training, vendor agreements, and corrective actions, consistent with HIPAA retention requirements.

2 | Technology and Vendor Management

	Use HIPAA-compliant telehealth platforms Select telehealth technologies that support: • Encryption of ePHI (in transit and at rest) • Unique user authentication • Role-based access controls • Audit logs
	Execute Business Associate Agreements (BAAs) Ensure BAAs are in place with all vendors that create, receive, maintain, or transmit PHI, including: • Telehealth platform vendors • Cloud hosting services • Remote monitoring vendors
	Configure systems securely Confirm security settings are enabled and aligned with organizational policies (e.g., disabling session recording unless necessary, using waiting rooms, limiting access privileges).
	Monitor and update systems Regularly review software updates, security patches, and configuration changes that may affect HIPAA compliance.

3 | Privacy Protections and Patient Rights

	Apply the "minimum necessary" standard Limit access to PHI during telehealth encounters to staff and information necessary for care delivery and operations.
	Provide Notice of Privacy Practices (NPP) Ensure patients receive and acknowledge the organization's NPP, including how PHI is used during telehealth services.
	Verify patient identity Use consistent identity verification practices at the start of telehealth encounters (e.g., name, date of birth, or other identifiers).
	Obtain and document consent where required. Follow state and organizational requirements for telehealth consent and document consent appropriately in the medical record.

4 | Workforce Training and Awareness

	Train staff on HIPAA and telehealth workflows Provide initial and periodic training covering: • Secure telehealth practices • Privacy considerations during virtual visits • Appropriate environments for telehealth delivery
	Address remote work risks Educate staff on securing home offices, avoiding public Wi-Fi, locking screens, and preventing unauthorized viewing or listening during telehealth sessions.
	Reinforce incident reporting Ensure staff know how and when to report suspected privacy or security incidents involving telehealth systems.

5 | Physical and Environmental Safeguards

	Secure provider environments Ensure telehealth visits are conducted in private settings where conversations cannot be overheard.
	Protect devices Implement safeguards for laptops, tablets, and mobile devices used in telehealth, including: • Password protection • Automatic log-off • Device encryption
	Control physical access Limit access to areas where telehealth systems and servers are located, even in hybrid or remote environments.

6 | Breach Response and Incident Management

	Maintain an incident response plan Ensure policies include steps for identifying, mitigating, documenting, and responding to telehealth-related privacy or security incidents.
	Assess potential breaches promptly Evaluate whether incidents involving telehealth systems constitute breaches of unsecured PHI under HIPAA.
	Follow breach notification requirements Notify affected individuals, HHS, and others as required by the HIPAA Breach Notification Rule and applicable state laws.

7 | Northeast- specific Considerations

	Account for state privacy laws Northeast states (Connecticut, Maine, Massachusetts, New Hampshire, New York, Rhode Island, and Vermont) may have **additional privacy or data security laws** that supplement HIPAA, including: • Broader definitions of personal data • State-specific breach notification timelines
	Use regional technical assistance Leverage resources from the Northeast Telehealth Resource Center (NETRC) for education, toolkits, and implementation guidance tailored to providers in the region.
	Monitor evolving telehealth policy Stay informed about state telehealth regulations and Medicaid policies that may affect documentation, technology use, or privacy expectations.

Key Reference Resources

Center for Connected Health Policy (CCHP) - cchpca.org
Telehealth policy and state law resources

Telehealth Resource Centers - telehealthresourcecenter.org
Practical telehealth implementation guidance, HRSA-supported

Northeast Telehealth Resource Center (NETRC) - netrc.org
Regional assistance for Northeast providers and organizations

HIPAA & Telehealth Guidance (HHS) - telehealth.hhs.gov
Federal standards for telehealth privacy and security

Note: This content is for informational purposes only and does not constitute legal advice or interpretation. NETRC encourages you to consult the appropriate state agency, internal colleagues, or an attorney for guidance.

The Northeast Telehealth Resource Center has been made possible by award number U1U42523 from the Office for the Advancement of Telehealth: HRSA / DHHS.