



Privacy, Data Sharing, & Consent in Disaster Virtual Care

HIPAA Guidelines in Disasters

HIPAA remains in effect during disasters. A **Centers for Medicare & Medicaid Services (CMS) Section 1135 waiver** may be issued under a federal emergency declaration, but it applies only to **hospitals in an active emergency area for 72 hours after the hospital activates its disaster protocol**^{1-3,19-23}. The waiver temporarily relaxes five Privacy Rule elements: (1) speaking with family, (2) facility directory opt-out, (3) distributing the Notice of Privacy Practices (NPP), (4) honoring requested restrictions, and (5) honoring requests for confidential communications, but all other HIPAA and Security Rule requirements remain enforceable^{1, 4,19-23}. The **Office for Civil Rights (OCR)** issues “emergency bulletins” to clarify existing HIPAA flexibilities; these notices provide guidance but **do not create new exceptions**¹. The COVID-19 “good faith virtual care” enforcement discretion ended in 2023, and all virtual care must now meet standard HIPAA requirements unless a hospital-specific CMS 1135 waiver is active⁵. Assume HIPAA applies in full unless operating under a documented CMS 1135 waiver.

State Law, Cross-State Care & Conflicts

Federal emergency declarations **do not override state virtual care or privacy laws**. Under HIPAA’s preemption rule, **the stricter standard governs**^{6,7}. Providers must follow the law offering patients the highest privacy protection-which is most important when practicing across state lines.

- **Florida:** Requires documented consent for all virtual care visits, including during disasters⁸.
- **North Carolina:** Allows verbal consent which may be documented in the patient record; an audio recording is not required⁹.
- **Tennessee:** Maintains consent and privacy requirements even during emergencies¹⁰.

For privacy, licensure, and liability, the patient’s physical location determines governing law unless the provider is deployed **under Emergency**

Disclaimer: This material is for **informational purposes only** to support disaster virtual care planning and operations. It **does not constitute legal advice** and should not be relied upon as a substitute for consultation with qualified counsel. Laws, waivers, and declarations **change rapidly**; clinicians and organizations should verify current requirements with their state authorities, payors, and legal advisors. Providers should verify current requirements with their **state licensing boards, activating entities, and legal counsel** before providing care.

Management Assistance Compact (EMAC) or federal **National Disaster Medical System (NDMS)** status¹¹. Confirm governing state rules before deployment; **HIPAA compliance alone is insufficient**.

Platforms, Security & BAAs

Since the end of the COVID enforcement discretion, only HIPAA-compliant systems with encryption, authentication, and audit trails can be used unless covered by a short-term 1135 CMS waiver^{5,12}. All virtual care vendors, including any cloud storage, documentation, call centers, or interpreters, are considered Business Associates and require Business Associate Agreements (BAAs) before exchanging Protected Health Information (PHI)^{12,13}. OCR, to date, has never issued a blanket BAA waiver^{1,5}. As an example, Georgia’s 2024 virtual care rule mandates “reasonable privacy safeguards” aligned with HIPAA^{14,30}. Vendors must execute a BAA before handling PHI; this requirement is not waived during emergencies.

Consent & Special Populations

HIPAA does not mandate consent for treatment, but virtual care consent is a state-controlled requirement⁶. Written or documented consent is considered a strong guideline for all encounters^{8,9}. HIPAA still requires notice of privacy practices, right of access, and minimum necessary compliance even under waivers^{1,2}. Providers caring for minors or behavioral-health patients may trigger additional state-level consent obligations^{9,15}. Document how and when consent was obtained whether written, verbal, or recorded.

Data Sharing & Breach Responsibilities

The **HIPAA Privacy Rule (§164.512)** allows limited disclosures of PHI without patient authorization when necessary for treatment, public health purposes, or



disaster response coordination. This provision enables information sharing with MOCCs, EMAC partners, and EMS while maintaining compliance with the Minimum Necessary Standard unless an active 1135 CMS waiver applies^{1,3,16}. Additionally, breach notification requirements remain fully in effect during disasters. The designated record custodian, such as the state ESF-8 authority, hospital, or individual provider, must notify affected patients and regulators¹⁰⁻¹⁸. Federal HIPAA rules allow 60 days for notification, but many states impose stricter timelines. For example, North Carolina and Tennessee require notice within 45 days, while Florida allows only 30 days²⁶⁻³⁰. Identify the data custodian in writing before deployment.

Record Retention & End-of-Emergency Transitions

HIPAA requires six-year retention of privacy documentation, while medical record retention is determined by state law^{22,24-30}. For example, Georgia requires records to be kept for ten years, and most neighboring states such as Alabama, Tennessee, and South Carolina follow similar timelines²⁴⁻³⁰. Custodianship depends on deployment type:

- **State ESF-8 or EMAC:** Records are state property¹⁶.
- **Hospital-based:** Hospital retains ownership²⁴.
- **Independent volunteers:** Provider becomes custodian and assumes breach liability¹⁸.

When waivers expire, temporary platforms or devices must be secured or destroyed per HIPAA and state law^{5,22}. Confirm custodianship, storage, and data transfer plans before emergency termination.

References

1. HHS/OCR – HIPAA Emergency Preparedness & Response <https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/index.html>
2. HHS/ASPR – Section 1135 Waivers Overview <https://aspr.hhs.gov/legal/1135-Waivers/pages/1135-waivers.aspx>
3. CMS – “1135 Waiver at a Glance” (PDF) <https://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/SurveyCertEmergPrep/Downloads/1135-Waivers-At-A-Glance.pdf>
4. HHS/OCR – HIPAA Bulletin Example (Hurricane Milton, 2024) <https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/2024-hipaa-bulletin-fl-hurricane-milton/index.html>
5. HHS/OCR – HIPAA & Telehealth (COVID discretion ended Aug 9 2023) <https://www.hhs.gov/hipaa/for-professionals/special-topics/telehealth/index.html>
6. HIPAA Preemption Rule – 45 CFR § 160.203 <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-160/subpart-B/section-160.203>
7. HIPAA Privacy Rule – Uses & Disclosures for Public Health (§ 164.512) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-E/section-164.512>
8. HIPAA Security Rule – Device & Media Controls (§ 164.310) <https://www.ecfr.gov/current/title-45/section-164.310>
9. HIPAA Documentation Retention (§ 164.530(j)) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-E/section-164.530>
10. HIPAA Breach Notification Rule (§ 164.400–414) <https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-D>
11. HHS/OCR – Breach Notification Guidance <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html>
12. HHS – Minimum Necessary Standard Guidance <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/minimum-necessary-requirement/index.html>
13. Telehealth.HHS.gov – Obtaining Informed Consent <https://telehealth.hhs.gov/providers/preparing-patients-for-telehealth/obtaining-informed-consent>
14. HHS Cybersecurity Best Practices (405(d) Program) <https://405d.hhs.gov/cornerstone/hicp>
15. NIST SP 800-53 Rev5 – Security & Privacy Controls <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>
16. Emergency Management Assistance Compact (EMAC) – Overview <https://www.emacweb.org/index.php/how-emac-works>
17. FSMB – State Emergency Declarations & Licensure Requirements <https://www.fsmb.org/siteassets/advocacy/pdf/state-emergency-declarations-licensures-requirements-covid-19.pdf>
18. Uniform Emergency Volunteer Health Practitioners Act (UEVHPA) – Model Law <https://asprtracie.hhs.gov/technical-resources/resource/1766/uniform-emny-volunteer-health-practitioners-act-uevhp>
19. ASPR TRACIE – HIPAA & Disasters Fact Sheet <https://files.asprtracie.hhs.gov/documents/aspr-tracie-hipaa-emergency-fact-sheet.pdf>
20. ASPR TRACIE – Legal & Regulatory Issues in Virtual Care <https://asprtracie.hhs.gov/technical-resources/resource/9602/legal-and-regulatory-issues-in-telehealth>
21. ASTHO – Emergency Authority & Immunity Toolkit <https://www.astho.org/advocacy/state-health-policy/legal-preparedness-series/emergency-authority-immunity-toolkit/>
22. ASTHO – Scope of Practice Toolkit <https://www.astho.org/advocacy/state-health-policy/legal-preparedness-series/scope-of-practice-toolkit/>
23. ASTHO – Public Health Authority Toolkit <https://www.astho.org/globalassets/toolkit/public-health-authority-toolkit.pdf>
24. CCHP – State Telehealth Consent & Privacy Requirements <https://www.cchpca.org/topic/consent-requirements-medicaid-medicare/>
25. CCHP – Cross-State Licensing & Telehealth Policies <https://www.cchpca.org/topic/cross-state-licensing-professional-requirements/>
26. Florida Telehealth Statute § 456.47 https://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&URL=0400-0499/0456/Sections/0456.47.html
27. Florida Information Protection Act (FIPA) – § 501.171 (30-day breach rule) https://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&URL=0500-0599/0501/Sections/0501.171.html
28. North Carolina Medical Board – Telemedicine Policy (Consent Requirement) <https://www.ncmedboard.org/resources-information/professional-resources/laws-rules-position-statements/position-statements/telemedicine>
29. North Carolina Identity Theft Protection Act – § 75-65 (45-day breach rule) https://www.ncleg.gov/EnactedLegislation/Statutes/PDF/BySection/Chapter_75/G_S_75-65.pdf
30. Georgia Composite Medical Board – Record Retention Rule § 360-3-.02 <https://rules.sos.ga.gov/gac/360-3-.02>

Disclaimer: This material is for **informational purposes only** to support disaster virtual care planning and operations. It **does not constitute legal advice** and should not be relied upon as a substitute for consultation with qualified counsel. Laws, waivers, and declarations **change rapidly**; clinicians and organizations should verify current requirements with their state authorities, payors, and legal advisors. Providers should verify current requirements with their **state licensing boards, activating entities, and legal counsel** before providing care.