

BlueOrange Alert:

HIPAA Enforcement Discretion Under COVID-19 Regulation Waivers

The Department of Health and Human Services (HHS) and the Office for Civil Rights (OCR) issued a “limited waiver” related to HIPAA during the COVID-19 pandemic. The HIPAA Privacy Rule allows patient information to be shared to assist in nationwide public health emergencies, and to assist patients in receiving the care they need.

First and foremost – **the HIPAA regulations and its protections to PHI are still in effect**– the “waiver” does NOT mean that you can lift all of your HIPAA safeguards, policies & procedures!

What has changed?

- Under the waiver, hospitals **will not be penalized for failing to comply with the following HIPAA requirements:**
 - To obtain a patient’s agreement to speak with family members or friends involved in the patient’s care
 - The requirement to honor a request to opt out of the facility directory
 - The requirement to distribute a Notice of Privacy Practices
 - The patient’s right to request privacy restrictions
 - The patient’s right to request confidential communications

NOTE: this waiver **only applies to:**

- Providers located in the emergency area identified in the public health emergency declaration.
- Providers who implemented disaster protocols, and up to 72 hours from the time a hospital makes that declaration.

After that 72 hours or when HHS terminates this waiver, all HIPAA requirements, sanctions and penalties go back into effect.

What has not changed?

- In addition to the waiver, remember that HIPAA already allows you to share patient information:
 - for treatment purposes – the minimum necessary rule does NOT apply to treatment;
 - for public health activities (including to public health authorities such as the CDC and local health department); and
 - to prevent or lessen serious and imminent threats to the patient or community.
- You must still make reasonable efforts to limit the PHI disclosed to the ‘minimum necessary’ to accomplish the purpose for everything other than treatment purposes.
- You should still use your role-based access policies to limit access to PHI to only those workforce members who need it to carry out their duties.

The following restrictions still apply:

- You may NOT share PHI with the media (without a patient’s consent)
- You may NOT disclose PHI to others not involved with the patient’s care (without a patient’s consent)
- Other impermissible uses and disclosures (such as marketing, sale of PHI, research, or other restrictions in the HIPAA rule)

About BlueOrange Compliance:

BlueOrange Compliance specializes in assisting healthcare organizations navigate HIPAA and HITECH privacy and security requirements. Complex, ever-changing healthcare regulations and increasing risks make it difficult for organizations to stay in front of emerging cyber threats. As a single source, we equip every client with affordable, practical, comprehensive privacy and security solutions, including multiple sources of information to help manage risk. Our clients have peace of mind knowing they are compliant and prepared for potential breaches and adverse audits. BlueOrange Compliance provides this alert for educational purposes only without warranty and specialized advice should be sought about your specific circumstances.