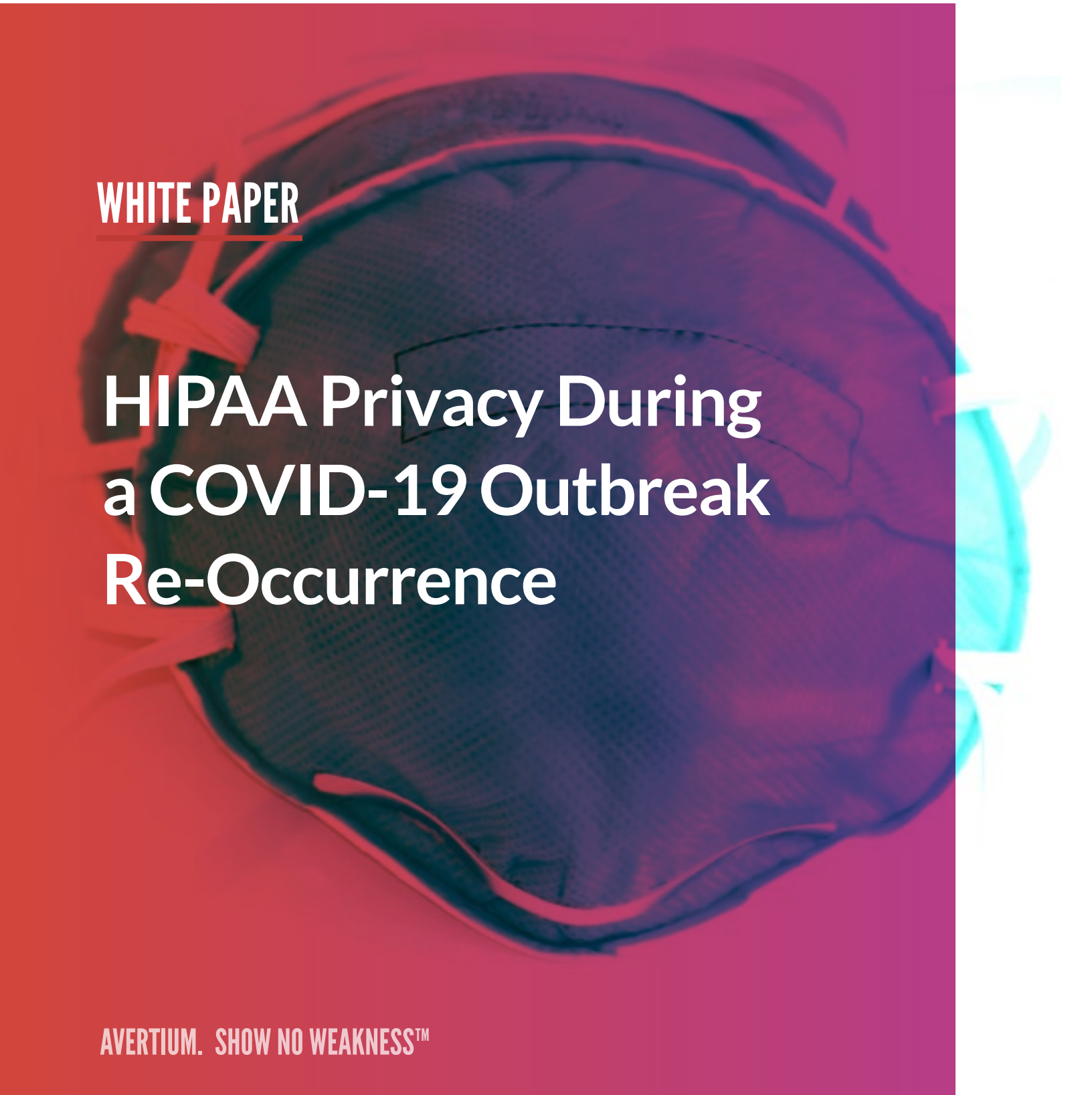
AVERTIUM



WHITE PAPER

HIPAA Privacy During a COVID-19 Outbreak Re-Occurrence

AVERTIUM. SHOW NO WEAKNESS™

The worst of the COVID-19 pandemic has passed, and your remote workers are returning to their office environments. Everything is back to normal. Or is it?

As the country re-opens for business, talk of possible future outbreaks raises questions about how a re-occurrence affects compliance with the Health Information Privacy and Accountability Act (HIPAA) Privacy Rule.

Even in these difficult times, the patient healthcare data privacy protections outlined under HIPAA remain in effect. Healthcare providers and business associates must continue to follow the requirements of the Privacy Rule to maintain HIPAA compliance.

The key is to be aware of the guidelines and prepared to be responsive in the case of an outbreak re-occurrence.

Health Data Sharing During COVID-19

Information sharing between healthcare professionals is vital in empowering them to learn from the initial COVID-19 outbreak to apply lessons learned and new practices to treatment in the case of another spike. Information regarding the efficacy of certain treatment plans or the infection and hospitalization rate of the virus can be vital for saving lives.

HIPAA's Privacy Rule includes special provisions for information sharing during an outbreak of an infectious disease or other disaster scenario. Here are instances in which sharing patient data without authorization is permissible under regulations set prior to the COVID-19 health crisis:

Enabling Treatment Payment, and Healthcare Operations (TPO)

The broadest category for the release of patient data is to enable treatment of the patient or other patients, to facilitate efficient payment and to offer access to quality healthcare.

Healthcare providers can share patients' medical records with other healthcare providers without patient consent according to the following TPO definitions contained in 45 CFR 164.501:

- Treatment: Generally includes the provision, coordination, or management of health care and related services among health care providers or by a health care provider with a third party, consultation between health care providers regarding a patient, or the referral of a patient from one health care provider to another.
- Payment: Encompasses the various activities of health care providers to obtain payment or be reimbursed for their services and of a health plan to obtain

premiums, to fulfill their coverage responsibilities and provide benefits under the plan, and to obtain or provide reimbursement for the provision of health care.

- Health care operations: Includes certain administrative, financial, legal, and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment.

Public Health Activities

Healthcare providers are also authorized to release patients' personal health data without authorization in order to protect public health and safety. The HIPAA Privacy Rule allows release of patient records without consent to:

- Public Health Authorities (PHAs): National, state-level, local, or tribal government agencies that have responsibility for matters pertaining to public health
- Individuals or Organizations: Entities or individuals can receive or collect this data if they are covered by a public health authority's contract or "grant of authority"
- Foreign Government Authority: A PHA can authorize release of healthcare data to a foreign government authority collaborating with that PHA
- Individuals at Risk: State and other laws may authorize the release of healthcare data to individuals at risk of contracting or spreading the disease

Family, Friends, and Caregivers

The HIPAA Privacy Rule acknowledges the need to share patients' care information with friends, family, and other caregivers. However, the intent is also to preserve the privacy of the patient. Sharing patient records with these parties is allowed in the following circumstances:

- **Verbal Consent:** A patient must give verbal consent for sharing their data or, at the least, no indication of an objection
- **Patient's Best Interest:** If a patient is incapable of giving verbal consent (unconscious or incapacitated), a healthcare provider may share relevant information if it is in the patient's best interest
- **Disaster Relief Organizations:** Healthcare providers can share health information with organizations such as the American Red Cross for the purposes of notifying family and other caregivers
    - Consent is not required if it would impede disaster response efforts

Beyond providing treatment and sharing information with friends and family, the release of patient records or other healthcare data is permitted in certain circumstances, such as:

- **Preventing a Serious and Imminent Threat:** Healthcare providers can share a patient's data with anyone who, in their professional opinion, can prevent or lessen a serious and imminent threat to the individual or the public
- **Media Releases**: Unless the patient has objected, a healthcare provider can confirm that a patient is in residence and their general condition without explicit consent. More detailed information requires written consent or is permitted if the patient is incapacitated and revealing the information is in the patient's best interest and is consistent with any previously expressed wishes of the patient

HIPAA applies to healthcare providers and business associates. Other organizations are not required to follow these rules but may, optionally, do so.

OCR Discretion Under COVID-19 Circumstances

Notification of Enforcement Discretion

HHS has made several announcements regarding its Notification of Enforcement Discretion during the COVID-19 pandemic. These stipulate the OCR will not impose penalties for noncompliance with the regulatory requirements under the HIPAA Privacy, Security, and Breach Notification Rules against covered health care providers or their business associates during the good faith participation of certain activities during the COVID-19 nationwide public health emergency.

To date, this includes the following exceptions:

Telehealth Remote Communications

On March 17, 2020 the OCR issued guidance on telehealth remote communications stating that, effective immediately, the agency would not impose penalties for HIPAA violations against healthcare providers in connection with their good faith provision of telehealth using communication technologies during the COVID-19 nationwide public health emergency.

This guidance applies to widely available communications applications when used in good faith for any telehealth treatment or diagnostic purpose, regardless of whether the telehealth service is directly related to COVID-19.

The OCR will provide further guidance explaining how covered health care providers can use remote video communication products and offer telehealth to patients responsibly.

"We are empowering medical providers to serve patients wherever they are during this national public health emergency," said OCR Director Roger Severino. "We are especially concerned about reaching those most at risk, including older persons and persons with disabilities," Severino added.

First Responders

On March 24, 2020 the OCR issued guidance to help ensure its regulations allow first responders and others to receive PHI about individuals exposed to COVID-19.

The guidance explains how covered entities may disclose PHI about an infected individual to law enforcement, paramedics, other first responders, and public health authorities in compliance with the HIPAA Privacy Rule so they can take extra precautions or use personal protective equipment.

The circumstances under which a covered entity may disclose PHI such as the name or other identifying information about individuals without their HIPAA authorization include:

- When needed to provide treatment
- When required by law
- When first responders may be at risk for an infection, and
- When disclosure is necessary to prevent or lessen a serious and imminent threat.

The guidance also includes a reminder that covered entities must make reasonable efforts to limit the PHI used or disclosed to that which is the "minimum necessary" to accomplish the purpose for the disclosure.

"Our nation needs our first responders like never before and we must do all we can to assure their safety while they assure the safety of others," said Roger Severino, OCR Director. "This guidance helps ensure first responders will have greater access to real time infection information to help keep them and the public safe," added Severino.

Community-Based Testing Sites

On April 9, 2020 the OCR announced it will include Community-Based Testing Sites (CBTSs) in its COVID-19 pandemic exceptions to support certain covered health care providers, including some large pharmacy chains, and their business associates that participate in the operation of mobile, drive-through or walk-up sites that only provide COVID-19 specimen collection or testing services to the public.

To protect the privacy and security of individuals' PHI, the OCR encourages covered health care providers to implement reasonable safeguards including the following:

- Using and disclosing only the minimum PHI necessary except when disclosing PHI for treatment.

- Setting up canopies or similar opaque barriers at a CBTS to provide some privacy to individuals during the collection of samples.
- Controlling foot and car traffic to create adequate distancing at the point of service to minimize the ability of persons to see or overhear screening interactions at a CBTS.

This exercise of enforcement discretion is retroactively effective from March 13, 2020.

Securing Patient Data During COVID-19

Healthcare providers and business associates should do their utmost to rigorously protect patient data during this crisis, and, even when authorized, should share the minimum possible amount of data required for a purpose with the exception of treatment.

About Avertium

Avertium, one of the largest cybersecurity services providers to the mid-to-enterprise market, is redefining the landscape with its distinctive show-no-weakness approach. Forged out of three award-winning cybersecurity services companies, each with a unique perspective on the security landscape, Avertium brings enterprise-level security to the many mid-sized and larger organizations that don't have access to comprehensive, specialized protection. More than 1,200 organizations in industries ranging from financial services and manufacturing, to technology and healthcare benefit from Avertium's managed security, consulting and compliance services delivered with more rigor, more relevance, and more responsiveness. The company's dual security operations centers are located in Arizona and Tennessee.

Avertium. Show No Weakness.™

AVERTIUM

+1 (877)-707-7997
hello@avertium.com
www.avertium.com