HIPAA during the COVID-19 national Emergency

On February 2020 the Office for Civil Rights (OCR), U.S. Department of Health and Human Services released the "HIPAA Privacy and Novel Coronavirus" bulletin https://www.hhs.gov/sites/default/files/february-2020-hipaa-and-novel-coronavirus.pdf

Key takeaways from the bulleting:

What information can be shared between covered entities?
Under the Privacy Rule, covered entities may disclose, without a patient's authorization, protected health information about the patient as necessary to treat the patient or to treat a different patient.

What power is given to Public Health Authorities under the Privacy rule?
The HIPAA Privacy Rule recognizes the legitimate need for public health authorities and others responsible for ensuring public health and safety to have access to protected health information that is necessary to carry out their public health mission. Therefore, the Privacy Rule permits covered entities to disclose needed protected health information without individual authorization to:

- A public health authority
- At the direction of a public health authority, to a foreign government agency
- Persons at risk

What is a public health authority?
A "public health authority" is an agency or authority of the United States government, a State, a territory, a political subdivision of a State or territory, or Indian tribe that is responsible for public health matters as part of its official mandate, as well as a person or entity acting under a grant of authority from, or under a contract with, a public health agency

What are some examples of health authorities?
The CDC, State or local health department, that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury or disability

What are some examples of information that should be made available to Public Health Authorities?

Reporting of disease or injury; reporting vital events, such as births or deaths; and conducting public health surveillance, investigations, or interventions

Who is a person a risk?
Is a person at risk of contracting or spreading a disease or condition if other law, such as state law, authorizes the covered entity to notify such persons as necessary to prevent or control the spread of the disease or otherwise to carry out public health interventions or investigations

Can I share information with Family, Friends, and Others Involved in an Individual's Care and for Notification?
A covered entity may share protected health information with a patient's family members, relatives, friends, or other persons identified by the patient as involved in the patient's care. A covered entity also may share information about a patient as necessary to identify, locate, and notify family members, guardians, or anyone else responsible for the patient's care, of the patient's location, general condition, or death. This may include, where necessary to notify family members and others, the police, the press, or the public at large. See 45 CFR 164.510(b)

Can providers disclose information to Prevent a Serious and Imminent Threat?
Yes. Health care providers may share patient information with anyone as necessary to prevent or lessen a serious and imminent threat to the health and safety of a person or the public – consistent with applicable law (such as state statutes, regulations, or case law) and the provider's standards of ethical conduct.

Can providers disclose information to the Media or Others Not Involved in the Care of the Patient/Notification?
In general, except in the limited circumstances described in the OCR and HHS bulletin, affirmative reporting to the media or the public at large about an identifiable patient, or the disclosure to the public or media of specific information about treatment of an identifiable patient, such as specific tests, test results or details of a patient's illness, may not be done without the patient's written authorization (or the written authorization of a personal representative who is a person legally authorized to make health care 5 decisions for the patient)

What is the minimum necessary information that should be shared with covered entities?
A covered entity must make reasonable efforts to limit the information disclosed to that which is the "minimum necessary" to accomplish the purpose. (Minimum necessary requirements do not apply to disclosures to health care providers for treatment purposes.)

What is an example of minimum necessary information sharing with Public health authorities?
A covered entity may rely on representations from the CDC that the protected health information requested by the CDC about all patients exposed to or suspected or confirmed to have Novel Coronavirus (2019-nCoV) is the minimum necessary for the public health purpose

What safeguards do I need to implement during an emergency?
In an emergency situation, covered entities must continue to implement reasonable safeguards to protect patient information against intentional or unintentional impermissible uses and disclosures.

Working from Home and HIPAA during the COVID-19 public health emergency

As stated by the Department of Health and Human Services, some HIPAA enforcement provision have been relaxed to allow healthcare providers to communicate and continue providing healthcare services to patients in need during the COVID-19 national public health emergency. For more information go to: https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html

What is new?
Covered health care providers subject to the HIPAA Rules may seek to communicate with patients, and provide telehealth services, through remote communications technologies. Some of these technologies, and the manner in which they are used by HIPAA covered health care providers, may not fully comply with the requirements of the HIPAA Rules.

What flexibility is allowed during this emergency?
OCR is exercising its enforcement discretion to not impose penalties for noncompliance with the HIPAA Rules in connection with the good faith provision of telehealth using such non-public facing audio or video communication products during the COVID-19 nationwide public health emergency. This exercise of discretion applies to telehealth provided for any reason, regardless of whether the telehealth service is related to the diagnosis and treatment of health conditions related to COVID-19.

What are providers allowed to do for Telehealth?
A covered health care provider that wants to use audio or video communication technology to provide telehealth to patients during the COVID-19 nationwide public health emergency can use any non-public facing remote communication product that is available to communicate with patients.

Is this provision only available to COVID-19 patients?

No. A covered health care provider may provide telehealth services in the exercise of their professional judgment to assess or treat any medical condition, even if not related to COVID-19, such as a sprained ankle, dental consultation or psychological evaluation, or other conditions.

Sample guidelines to allow healthcare workers to work from home and comply with HIPAA

These are some recommended guidelines to follow when providing Telehealth or any other service covered under HIPAA:

- Develop policies and procedure for at home office space
    - Home office should be secured and not easily accessible to other people
    - Recommend or require a door that can be locked
    - Space cannot be shared with other people
    - Hardware cannot be used by other people
- Provide your own hardware and software when possible
    - Extend computer and equipment policies to include at home usage
- If employee is using it's own hardware:
    - Develop policies to require limitation on media and downloads
    - Develop policies and procedures prohibiting employees from allowing friends and family from using devices that contain PHI.
    - Create a Bring Your Own Device (BYOD) Agreement, with clear usage rules.
- Provide a secure encrypted connection to the EHR and any other system with PHI
- Secure or provide lockable file cabinets or safes for employees who store hard copy PHI in their home offices.
- Provide HIPAA-compliant shredders for remote workers so these workers can destroy paper PHI at their work location once the PHI is no longer needed.
- Ensure employees disconnect from the company network when their work is complete. This can be done by applying measures such as IT configuring timeouts.
- Maintain and periodically review logs of remote access activity.

Ensuring mobile device security (laptots, phones, etc..):

- Encrypt home wireless router traffic.
- Change default passwords for wireless routers from the existing passwords.
- Encrypt, and password-protect, personal devices employees may use to access PHI.
    - Personal devices should be configured before allowing those devices can access the network. Covered entities can also specify what brands and versions of personal devices are permitted to access company data.

- Ensure all devices that access your network are properly configured (i.e., are encrypted, with password, firewall, and antivirus protection).
- Encrypt all PHI before it is transmitted.
- Require employee use of a VPN when employees remotely access the company Intranet.

These are links to HIPAA guidelines for remote work

45 CFR § 164
45 CFR § 164.308(a)(5)(ii)(B) Protection from Malicious Software
45 CFR § 164.312(d) Standard: Person or entity authentication
45 CFR § 164.312(e)(1) Standard: Transmission Security & (2) Implementation specifications