



**HealthCare
Compliance**
Network

Regulatory Compliance: The New Paradigm under COVID-19

Presenter: Todd McDonagh, Principal & CEO

SHARE FACTS ABOUT COVID-19

FACT
1

Diseases can make anyone sick regardless of their race or ethnicity.

FACT
2

For most people, the immediate risk of becoming seriously ill from the virus that causes COVID-19 is thought to be low.

FACT
3

Someone who has completed quarantine or has been released from isolation does not pose a risk of infection to other people.

FACT
4

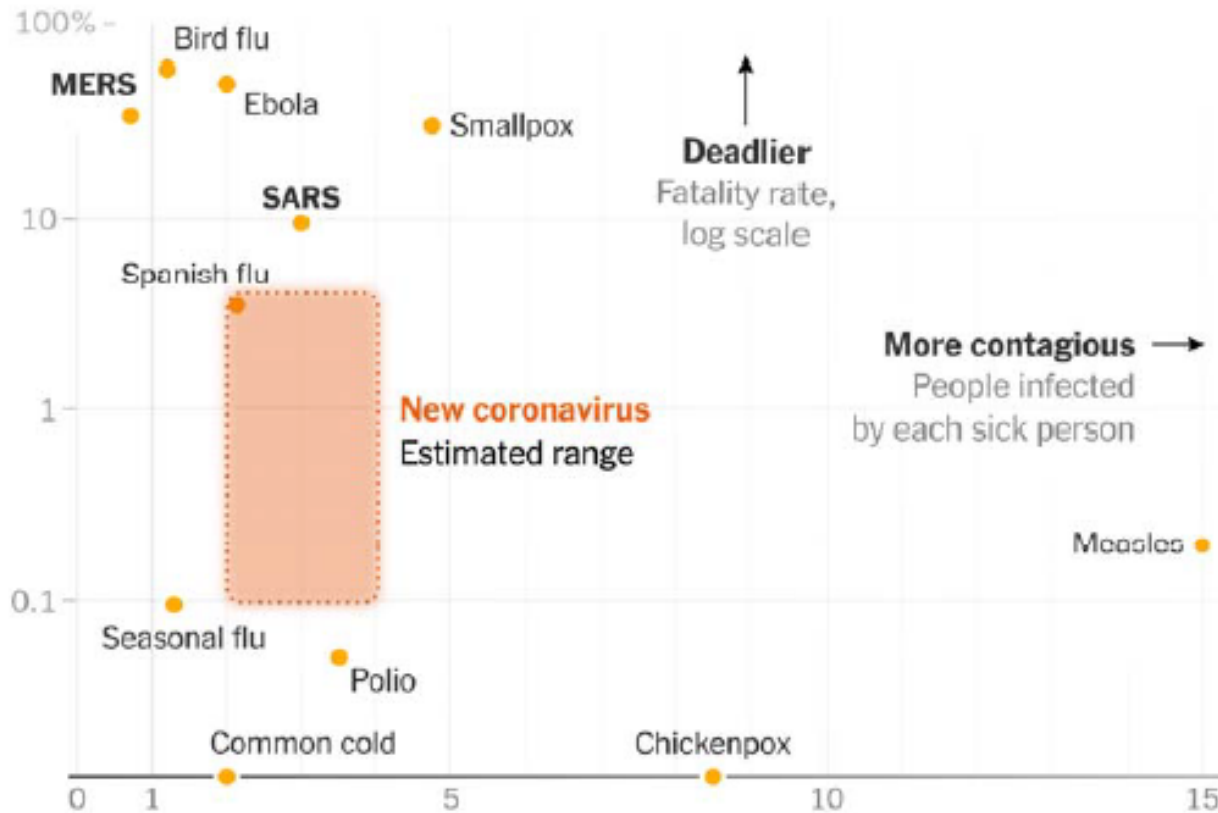
There are simple things you can do to help keep yourself and others healthy.

FACT
5

You can help stop COVID-19 by knowing the signs and symptoms:

Source: CDC website

Estimated severity of COVID-19



<https://www.nytimes.com/interactive/2020/world/asia/china-coronavirus-contain.html>

5

3

All Government Agencies Have Mobilized

- Department of Labor – OSHA
- Department of Health & Human Services – Office of Civil Rights
- Department of Health & Human Services – Office of Inspector General
- Center for Medicare & Medicaid Services
- Equal Employment Opportunity Commission



What Changed with HIPAA?

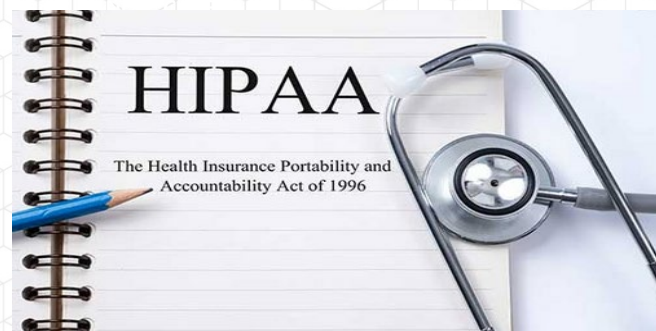
- Emergency Communication
- Notification of Enforcement Discretion for Telehealth
- Disclosures to law enforcement, paramedics, other first responders and public health authorities
- Other considerations: remote employees, cybersecurity, professional liability, documentation & storage



Limited Waiver of HIPAA Sanctions and Penalties During a Nationwide Public Health Emergency

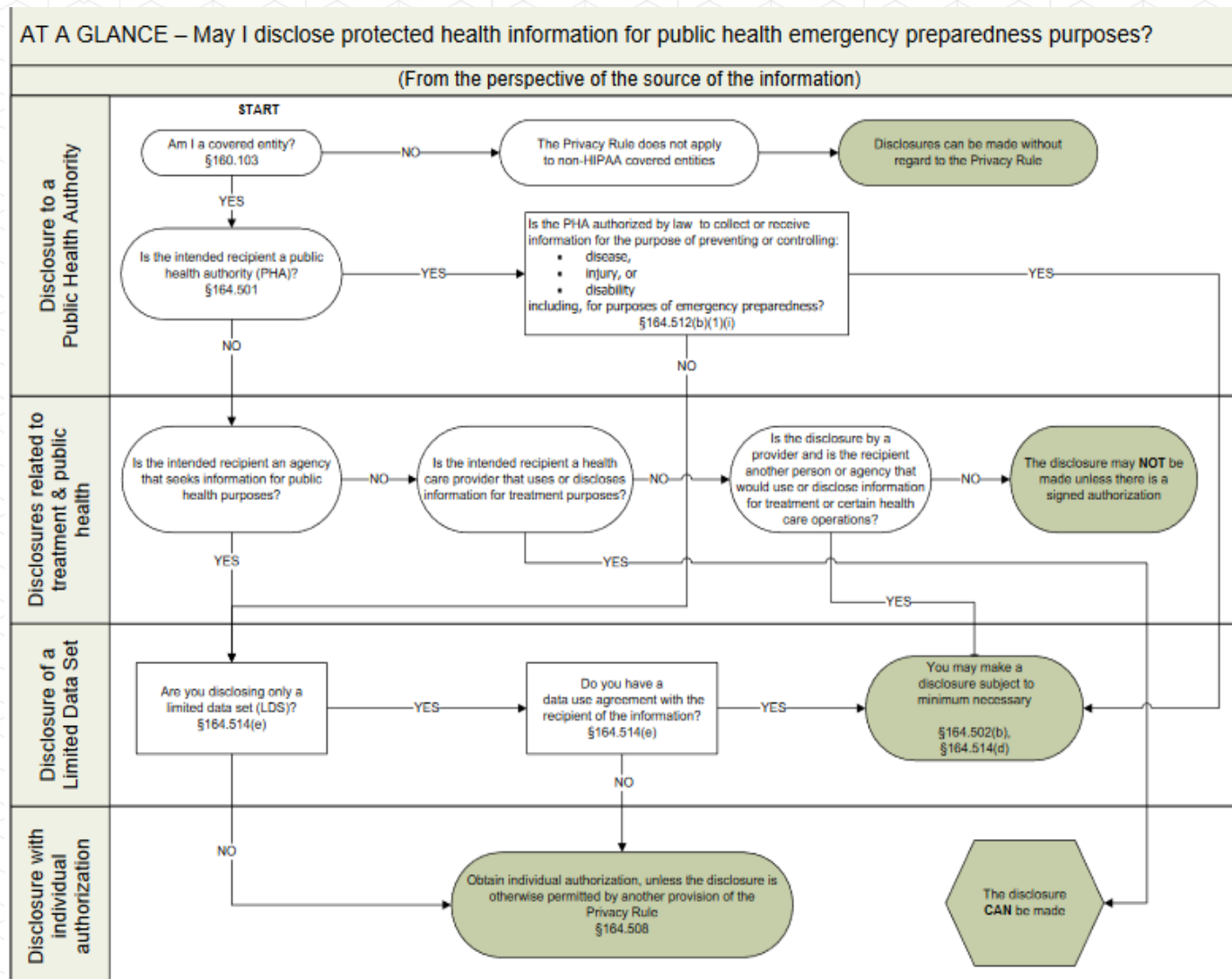
Key Elements: *Privacy Rules are not set aside during an emergency*

- Public Health Activities
- Disclosures to Family, Friends, and Others Involved in an Individual's Care and for Notification
- Disclosures to Prevent or Lessen a Serious and Imminent Threat
- Disclosures to the Media or Others Not Involved in the Care of the Patient/Notification



<https://www.hhs.gov/sites/default/files/hipaa-and-covid-19-limited-hipaa-waiver-bulletin-508.pdf>

Emergency Preparedness - A Decision Tool



Notification of Enforcement Discretion for Telehealth

On 3/17/20, 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 opens the door for popular apps like Apple FaceTime, Facebook Messenger, Google Hangout and Skype to be used for video chat.

Other HIPAA compliant video conferencing apps:

- Skype for Business
- Updox
- Vsee
- Zoom for Healthcare
- Doxy.me
- Google G Suite Hangouts Meet

<https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html>

[FAQs for telehealth](#)

Disclosures to law enforcement, paramedics, other first responders and public health authorities

Key Elements: *Privacy Rules are not set aside during an emergency*

- When the disclosure is needed to provide treatment.
- When such notification is required by law.
- To notify a public health authority in order to prevent or control spread of disease.
- When first responders may be at risk of infection.
- When the disclosure of PHI to first responders is necessary to prevent or lessen a serious and imminent threat to the health and safety of a person or the public.
- When responding to a request for PHI by a correctional institution or law enforcement official having lawful custody of an inmate or other individual.

<https://www.hhs.gov/sites/default/files/covid-19-hipaa-and-first-responders-508.pdf>

When Your Employees Go Remote

Whether you already have or are considering having some of your employees go remote, there are a number of things that you must put in place to keep your practice's PHI secure.

- Make a list of those remote employees.
- Indicate the level of information to which they will have access.
- Have your IT department or vendor configure personal devices before allowing them access to the network.
- Make sure that the employee's home wireless router is encrypted and that the password for the router follows your organization's password policy.
- All remote devices should use a VPN.
- All PHI must be encrypted before being transmitted. This can occur via email encryption or by utilizing a secure file sharing app, like ShareFile.
- If PHI needs to be stored on the employee's personal device, the hard drive needs to be encrypted.

When Your Employees Go Remote

- While the employee is working remotely, their PC should not be used by any other person.
- Employees must disconnect from the network, when not engaged in work activities. Preferably, IT configures a timeout.
- If PHI needs to be printed or maintained in a hard copy, it needs to be stored in a lockable file at home.
- Once hard copy PHI isn't needed, it should be shredded. If shredding is going to occur at the practice, hard copy PHI needs to be transported via a lock box.
- Keep logs of remote access activity.
- Make sure that the employee has signed the organization's Confidentiality Agreement and that they are aware of organization's policies on Password, Sanctions and Workstation Use.

When Your Employees Go Remote

Employees who telework face challenges to maintaining engagement and connection with their organizations. This can be especially true in situations, like the coronavirus COVID-19 pandemic, when employees may be required to work from home suddenly for an extended period.

Challenges include:

- **Isolation** - It is easier for an employee to feel connected and part of a team when they are in the office and can share ideas quickly and easily every day. Individuals working remotely have fewer interactions with coworkers and must plan more in order to connect and collaborate.
- **Distractions** - The home environment provides ample opportunities for distraction, from television to pets to unlimited snacks in the refrigerator. If family members also are home (e.g., the children are out of school), that can add an additional layer of potential disruption to work.
- **Work/life balance** - It is very easy for individuals working from home to tie themselves to their desks, continually check email or work on projects at all hours of the day, blurring the lines between work and home life.
- **Visibility** - "Out of sight, out of mind" is a maxim that encapsulates a fear of those teleworking. Employees may perceive a lack of support from their organization or their supervisor, and may fear the loss of opportunities to work on key projects or to be considered for a special assignment or promotion.

12

Other Considerations: HIPAA/Telehealth

- Cybercriminals Smell Blood in the Water
- Professional Liability/ Cyber Liability
- Documentation
- Consents
- [National Consortium of Telehealth Resource Centers](#)



What Changed with OSHA?

- Misinformation about OSHA 300 log
- Standard Precautions – Shared Environments
- PPE - 29 CFR 1910 Subpart I
- Bloodborne Pathogens standard (29 CFR 1910.1030)
- Emergency Preparedness

Resources:

<https://www.cdc.gov/coronavirus/2019-ncov/hcp/respirator-use-faq.html>

<https://www.cdc.gov/coronavirus/2019-ncov/release-stockpiled-N95.html>

<https://www.cdc.gov/coronavirus/2019-ncov/hcp/healthcare-supply-ppe-index.html>

Additional Changes for Other Agencies

- Dept. of Health & Human Services – Office of Inspector General

<https://oig.hhs.gov/fraud/docs/alertsandbulletins/2020/policy-telehealth-2020.pdf>

- Equal Employment Opportunity Commission

https://www.eeoc.gov/eeoc/newsroom/wysk/wysk_ada_rehabilitaion_act_coronavirus.cfm

- Drug Enforcement Agency

<https://www.dea.gov/press-releases/2020/03/20/deas-response-covid-19>

- Center for Medicare & Medicaid Services

1135 Waiver Authority / Coronavirus Preparedness and Response Supplemental Appropriations Act

- Historically, Medicare coverage for telemedicine has been restricted to those patients who live in medically underserved areas.
- Effective for services starting 3/6/20 and for the duration of the COVID-19 Public Health Emergency, Medicare will provide coverage for telehealth services furnished to patients in broader circumstances by allowing payment for professional services furnished to beneficiaries in all areas of the country in all settings.
- This includes services provided in any healthcare facility or in their home.
- These visits are considered the same as in-person visits and are paid at the same rate as regular, in-person visits.

TYPE OF SERVICE	WHAT IS THE SERVICE?	HCPCS/CPT CODE	Patient Relationship with Provider
MEDICARE TELEHEALTH VISITS	A visit with a provider that uses telecommunication systems between a provider and a patient.	<p>Common telehealth services include:</p> <ul style="list-style-type: none"> • 99201-99215 (Office or other outpatient visits) • G0425-G0427 (Telehealth consultations, emergency department or initial inpatient) • G0406-G0408 (Follow-up inpatient telehealth consultations furnished to beneficiaries in hospitals or SNFs) <p>For a complete list: https://www.cms.gov/Medicare/Medicare-General-Information/Telehealth/Telehealth-Codes</p>	<p>For new* or established patients.</p> <p>*To the extent the 1135 waiver requires an established relationship, HHS will not conduct audits to ensure that such a prior relationship existed for claims submitted during this public health emergency</p>
VIRTUAL CHECK-IN	A brief (5-10 minutes) check in with your practitioner via telephone or other telecommunications device to decide whether an office visit or other service is needed. A remote evaluation of recorded video and/or images submitted by an established patient.	<ul style="list-style-type: none"> • HCPCS code G2012 • HCPCS code G2010 	For established patients.
E-VISITS	A communication between a patient and their provider through an online patient portal.	<ul style="list-style-type: none"> • 99421 • 99422 • 99423 • G2061 • G2062 • G2063 	For established patients.

HCN Fact Sheet



If you like more information on any of these subjects, please email me at tmcdonagh@hcompliance.com or text me at 978 886-1054.