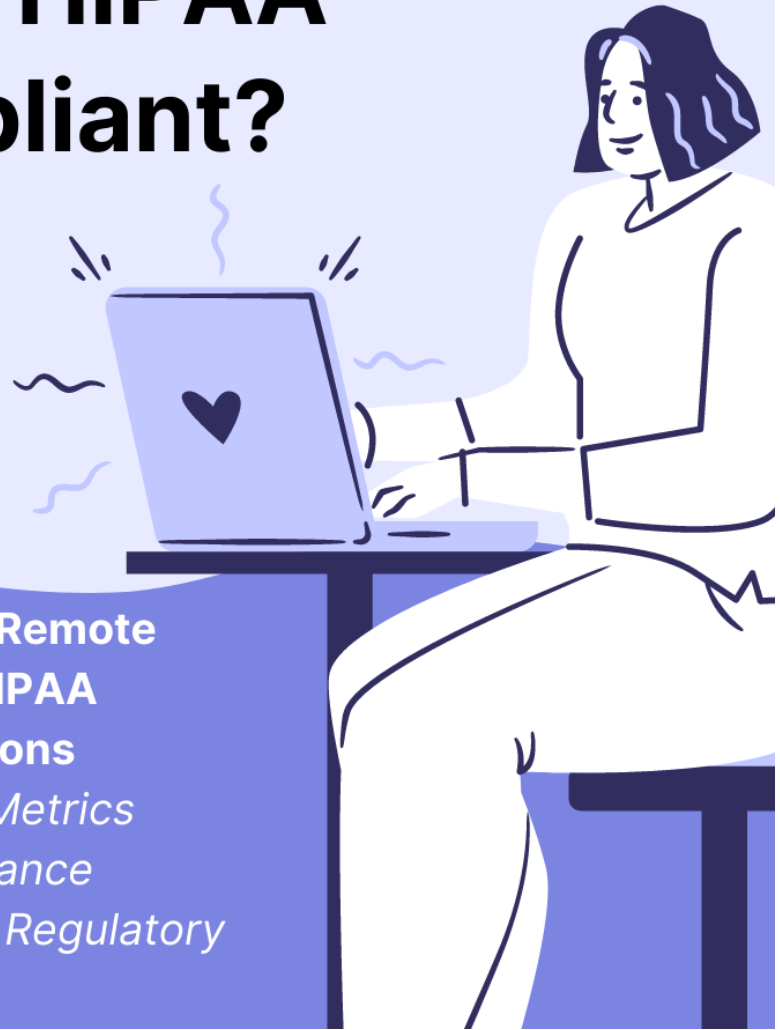**QMETRICS**

SPRING NEWSLETTER

It's Spring and most of us are still on orders to stay inside! We wanted to send a note to brighten your day - and quarantine! Below are links to articles included in our Newsletter.

- Is Your Remote Office HIPAA Compliant? Included is a HIPAA Checklist for you to review considerations and safeguards for your organization.
- Assess the Impact of Telehealth - Learn about services QMetrics provides.
- Read our article on "Deskercise" - That's right! You can work out and stretch while seated at your desk.

We hope you are well, and that you are staying safe and healthy. QMetrics is here for you as we weather the COVID storm, one day at a time from home.

Cheers, Suzan & the QMetrics team

Is Your Remote Office HIPAA Compliant?

QMETRICS

A Checklist for Remote Workers & HIPAA Considerations

Stacy Baker, QMetrics Chief Compliance Officer & Senior VP Regulatory Affairs

In response to the COVID-19 outbreak, many employers have been required to quickly transition their workforce to a remote work model with little time to prepare in response to government issued in-home orders. Employers have needed to focus on the many operational and logistical details to enable employees to work from home, but employers qualifying as HIPAA Covered Entities or Business Associates also need to consider their responsibility to maintain ongoing compliance with the HIPAA privacy and security requirements while employees are working from home.

Although HHS has issued guidance* providing HIPAA flexibilities and enforcement discretion during the COVID-19 emergency for providers offering telehealth services and in other clinical settings, the HIPAA rules still stand for other Covered Entities and Business Associates. Since suddenly expanding the number of employees working remotely comes with increased

cybersecurity and HIPAA compliance risks, the following are a few tips for employers to consider in consultation with its legal, information technology, and operational teams to ensure that employees working from home have physical, technical, and administrative safeguards in place to reduce the risk of a breach or running afoul of the HIPAA rules.

Checklist: General Considerations & Administrative Safeguards

- Remind employees to treat their home workspace like their on-site worksite and their responsibility to make sure they have the appropriate physical and technical safeguards in place to protect PHI.
- Provide employees with additional HIPAA training and remind them of best practices for safeguarding PHI every place. Employees should be reminded of their responsibility to immediately report potential breaches and the method to submit a potential breach report.
- Conduct a Risk Analysis with a focus on remote access to and use of electronic PHI (EPHI) and review HIPAA policies and training materials to determine if updates are needed to include added protections for the remote worker structure.
- Review vendor agreements to confirm whether you have a Business Associate Agreement in place for any vendors with access to PHI. If not, obtain one. Remind Business Associates of their responsibilities under HIPAA and the process to report potential breaches.
- Consider having employees sign a Remote Worker attestation form to confirm the employee has the physical and technical protections in place, understand the HIPAA responsibilities, and know the method and timeframes to report a potential breach.

Physical Safeguards

- Employees with access to PHI should have private workspace areas where PHI can be protected. This is especially important now because employees are likely home with other family members during this time which imposes an additional risk. Employers should consider providing privacy screen guards for employee laptops.
- Computers or other access to PHI should be physically secured and not left unsecured or unattended.
- Printed PHI should be stored in a locked or secured area that is accessible only to the employee.
- Discarded printed PHI should be shredded or carefully destroyed in a manner so as not to expose PHI.

Technical Safeguards

- Implement a two-factor authentication process and strong password requirements for granting remote access to systems that contain EPHI.
- Install firewall and anti-virus and intrusion detection software on any laptops and portable devices that store or access EPHI. Wireless networks must be WPA2 encrypted (WEP is no longer secure) and network devices must not use default device passwords.
- Implement encryption solutions for the transmission of EPHI and prohibit the transmission of EPHI over non-secure networks.

- Identify and maintain a tracking log of the types of hardware and electronic media being used and the authorized users in the case a device is lost or stolen.
- Ensure data from the remote system is automatically backed up to a secure protected location which is password protected and encrypted.

The considerations provided above is a non-exhaustive list. HHS has also developed some more detailed guidance to provide HIPAA covered entities with general information on the risks and possible mitigation strategies for remote use of and access to e-PHI. If you would like assistance with evaluating your Remote Worker policies or creating an employee Remote Worker Attestation Form, QMetrics can help. * For the most recent updates issued by the HHS Office for Civil Rights (OCR) regarding this topic refer to the HHS HIPAA, Civil Rights, and COVID-19 page here.

Contact SBaker@qmetrics.us to Schedule a Risk Assessment

Assess the Impact of Telehealth

COVID-19 has resulted in our governing entities relaxing rules around the provision of telehealth services, requiring health plans to reimburse providers for medical and behavioral health via telehealth.

QMetrics custom survey solutions can help health plans and provider groups assess the impact of COVID-19 and the resulting increase in telehealth services on enrollees and providers. Conducting a survey can provide critical feedback to inform leadership strategies to support your clients

during this critical time. Below are some survey topics for both providers and enrollees.

Providers:

- Knowledge, comfort level, satisfaction with telehealth appointments
- Plan/group services related to testing and treatment of COVID19

Enrollees:

- Enrollee satisfaction with telehealth appointments
- Enrollee satisfaction with COVID19 services and education
- Enrollee education through IVR messaging

Schedule Your FREE Consultation

Deskercise - Just What You Need

It's 2020 and we're pretty sure most of us didn't visualize we'd be working from home a lot more than before, or even, for the first time. We might not all have the same commodities as before with our ergonomic office furniture and it is important that we don't neglect our bodies.

This is why we'd like to remind you all about Deskercise—Exercises performed while seated at your workplace. Remember to take some stretching breaks, get up and walk around to relax the stress on your eyes.

Below are a few resources to provide you with inspiration:

- [5 Ways to Get Active & Stay Health from Home - CDC](#)
- [15 Simple Exercises You Can Do at Your Desk - DIYGenius](#)
- [Yoga at Your Desk - YouTube](#)
- [Desk Stretches - Mayo Clinic](#)