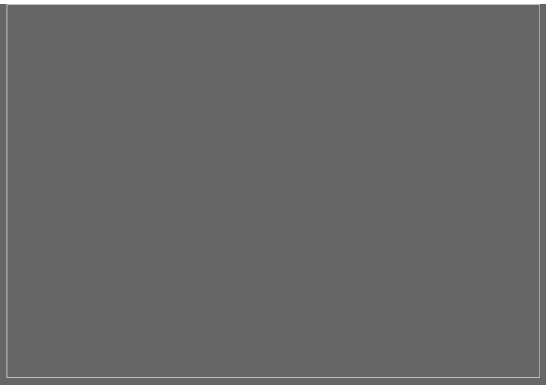
- DATA BREACH RESPONSE. Cyber attacks are increasing, seeking to capitalize on the sense of urgency attached to COVID-19. We can help with data breach response, which should be triggered by any unauthorized access or use of personal data such as ransomware, phishing, inappropriate media disclosures, and employees viewing records outside the scope of their employment (i.e., snooping). In many states, and for HIPAA covered parties, health information is subject to data breach notification if it is disclosed inappropriately, even by mistake with no malicious intent.

- TRACKING EMPLOYEES AND PATIENTS. We can help clients identify compliance and risk management considerations when implementing tracking apps or voluntary surveys. Remember that if these initiatives are launched on behalf of your group health plan, such as by your plan's TPA, they may be HIPAA covered. If they are not HIPAA covered, they may be subject to FTC and state law requirements.

- DATA SECURITY STANDARDS. Clients may find it necessary to modify security standards for employees and vendors now working remotely. We can help clients determine how to do that without violating applicable data security laws, and how to expeditiously update any required compliance documents or contracts to reflect these changes.

- SECURITY RISK ANALYSIS. Businesses should update their security risk analyses, or conduct a COVID-19 situational risk analysis to supplement their compliance documentation. We can help clients ensure their risk evaluation process remains compliant and meets regulatory expectations. That step is important to defend practices in the event a data breach arises and a business needs to justify its acceptance of risks that contributed to the breach.

- CONSUMER OUTREACH AND TELEHEALTH. DHHS OCR has issued a number of advisories, some confirming how HIPAA applies in specific, relevant cases such as disclosures to public health authorities and emergency responders. Notably, OCR is deferring HIPAA enforcement for telehealth (permitting good faith use of non-public facing communication methods to deliver care remotely, including Security Rule deferral). However, it is important to layer that discretion into other relevant agencies' guidance, such as the FCC's more limited allowance for emergency texting under TCPA and SAMHSA's confirmation that Part 2 has a narrow "medical emergency" exception for disclosure of substance use disorder records.



OFFICE

The Summit
4101 Lake Boone Trail, Suite 300
Raleigh, NC 27607.7506

Phone: **919.781.4000**
Fax: **919.781.4865**

SITEMAP

Practices

People

Careers

News & Insights

Our Firm

Contact Us

Remote Access

Search the site...