GARDNER SKELTON
ATTORNEYS AT LAW

LEGAL NEWS FOR YOUR BUSINESS

January 2023

General Business Alert

NEW REQUIREMENTS FOR USING AN ASSUMED BUSINESS NAME IN NC

December 1, 2022, was the deadline for complying with North Carolina's revised laws regarding assumed business names, as the 2017 Assumed Business Name Act went fully into effect. The revised set of laws established a public, searchable online database for all assumed business names across the state. Additionally, businesses can designate multiple counties in which they conduct business, rather than filing individually with each county. Finally, the notarization requirement has been removed, simplifying the process of filing an assumed business name and completion of certificates.

What is an assumed business name?

An assumed business name is often referred to as a "DBA" – a "doing business as" name. A DBA is any name a business uses other than its legal name registered with the North Carolina Secretary of State ("NCSoS"). The factors that determine whether a name qualifies as a DBA differ by type of entity. For corporations or limited liability companies, a DBA is any name other than the entity's official registered name. For partnerships or sole proprietorships, a DBA is any name other than the name of the individual(s).

What does a DBA look like?

DBAs can differ across entities and personal preferences. For example, an LLC might have a registered name of Hypothetical Holdings, LLC, but do business as Restaurant Café. Alternatively, Doe's Cupcakes might be a DBA for a bakery owned by sole proprietor John Doe.

What are the new requirements?

For businesses that filed an Assumed Business Name Certificate on or after December 1, 2017, there are no new requirements. Businesses with Certificates filed before December 1, 2017, must now renew their DBA to keep it active, as all DBAs not included in the database have expired as of December 1, 2022. To renew or register a new DBA, businesses must file an Assumed Business Name Certificate, which includes the assumed

business name, the real name of the business or person (corporations, LLCs, and limited partnerships must also provide their SOSID number), the nature and address of the business, and the NC counties in which the assumed business name will be used. The Certificate can be filed with your county's register of deeds.

If you have questions about your business' DBA or the new requirements, please reach out to any member of Gardner Skelton's tax or business law team.

General Business Alert

HHS RELEASES BULLETIN ON TRACKING TECHNOLOGIES AND HIPAA

On December 1, 2022, the U.S. Department of Health and Human Services ("HHS") issued a bulletin regarding electronic tracking technologies and their interaction with the HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules"). The bulletin defines tracking technologies, acceptable and unacceptable uses, and outlines actions covered entities should take to ensure compliance.

Tracking technologies collect information about users and their activities on a website. These technologies include cookies, web beacons or tracking pixels, session replay scripts, and fingerprinting scripts. As technology continues developing in general, cookies and other tracking technologies have exploded, with an estimated 85% of the top 10,000 using at least one version of a tracking technology. Tracking technologies are used for a variety of purposes, from targeted advertising to remembering and auto-filling a site's login information. HHS' bulletin specifically focuses on situations in which covered entities use tracking technologies developed by third parties.

To serve their purpose, tracking technologies collect information, including individually identifiable health information ("IIHI") from website users, including their IP address, geographic location, home or email address, and medical appointment dates. HHS generally considers that when an individual visits an entity's website or mobile app, they are indicating that they have received or plan to receive medical services from that entity, and therefore either have a current patient-provider relationship or plan to have a future one. Therefore, HHS considers all IIHI collected on a regulated entity's website or mobile app to be Protected Health Information ("PHI"), and therefore subject to the HIPAA Rules.

Covered entities may use tracking technologies on different types of webpages and platforms. Unauthenticated webpages do not require a user to log in and may include general information about an entity and their services, policies, or procedures. Typically, tracking technologies used on unauthenticated webpages do not have access to PHI; however, there are a few notable exceptions. First, login pages for an entity's patient portal

are usually unauthenticated but may contain PHI such as credentials or registration information.

Additionally, unauthenticated webpages that contain information about specific symptoms or health conditions or allow individuals to search for a provider or schedule an appointment may also contain PHI. HHS specifically emphasizes webpages that contain information about pregnancy or miscarriage-related care as containing PHI. If a tracking technology vendor collects information from these users, the covered entity is considered to be disclosing PHI.

User-authenticated webpages require users to log in before they can fully access the webpage. Unlike unauthenticated webpages, user-authenticated webpages almost always contain PHI, which is disclosed to the tracking technology vendor. Additionally, covered entities may offer mobile apps to individuals. These apps may also collect PHI, such as fingerprints, billing information, geolocation, and device IDs. PHI collected by tracking technologies may only be disclosed for permissible purposes, or there must be prior authorization from the individual. Banners that ask users to opt-in or -out of tracking technologies and notices of privacy policies or terms and conditions are not considered a valid HIPAA authorization.

Any vendor that provides tracking technology on a user-authenticated webpage, app, or an unauthenticated webpage that contains PHI is considered a business associate under the HIPAA Privacy Rule, and a Business Associate Agreement ("BAA") must be in place. Additionally, if a covered entity uses an app that discloses PHI to the app's vendor or any other third party, or if the tracking technology vendor stores the protected information, the entity must comply with the HIPAA Rules and protect information appropriately.

Covered entities should take careful steps to make sure their tracking technology practices comply with the HIPAA Rules, including:

- Ensuring that all disclosures of PHI to tracking technology vendors are specifically permitted;
- Using a tracking technology vendor that meets the definition of "business associate" and using an appropriate BAA;
- In cases of impermissible disclosures, providing breach notifications to the affected individuals and HHS.

As technology continues to develop, so will the rules regarding its acceptable uses. By staying up to date on HHS guidance and reviewing practices related to collecting, storing, and transferring PHI, providers can stay in compliance and stay focused on providing the best healthcare possible.

If you have questions or concerns about tracking technologies or your obligations under HIPAA, please reach out to any member of Gardner Skelton's healthcare team.

DESIRAE HUTCHINSON
(704) 390-7056 direct
desirae@gardnerskelton.com

FRED PARKER
(704) 335-0350 phone
fred@gardnerskelton.com

JACKIE KINNI
(704) 390-7044 direct
jackie@gardnerskelton.com

LITIGATION. EMPLOYMENT. HEALTHCARE. TAX

contactus@gardnerskelton.com | www.gardnerskelton.com
505 East Boulevard Charlotte, NC 28203

MENT. HEALTHCARE. TAX. LITIGATION. EMPLO