FEDERAL TRADE COMMISSION AND ENFORCEMENT OF PRIVACY LAW

As we have mentioned previously, there is no overarching federal data privacy law in the United States. By contrast, the European Union's General Data Protection Regulation (GDPR) regulates data privacy, including consumer data, in all sectors. Although there is no overarching federal data privacy law in the United States, there are a few sector-specific laws. In health care, for example, the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) govern many aspects of privacy. Also, the Telecommunications Act and the Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM) touch on privacy issues in marketing. Still, there is no federal law specifically regulating the use of consumer data.

Despite the lack of consumer privacy statutes in the United States, the Federal Trade Commission (FTC) has been active for years in protecting American consumers against certain unfair and deceptive practices involving data privacy. The Federal Trade Commission Act (FTC Act) includes an extremely brief section that serves as perhaps the most important provision in U.S. privacy law. Section 5 of the FTC Act states simply: "unfair or deceptive acts or practices in or affecting commerce . . . are . . . declared unlawful." This single line, which does not specifically mention privacy, has been used by the FTC and Congress to make the FTC the de facto privacy enforcement agency of the federal government.

The FTC defines "Unfair Trade Practices" as any practice that results in a substantial injury, that lacks offsetting benefits, and cannot be easily avoided by consumers. In the privacy context, the FTC often looks at practices that unreasonably leave consumers' data vulnerable to hacking or theft. Should a company collect the personal data of an individual in connection with a product or services and make inadequate efforts to protect that data, the FTC may seek enforcement for violation of Section 5 of the FTC Act. Conversely, "Deceptive Trade Practices" involve material statements or omissions that are likely to mislead consumers who are otherwise acting reasonably. Deceptive practices can include false representations or false promises. Importantly, the FTC has taken the position that failure to adhere to the steps, standards, and promises contained in a privacy notice is a deceptive trade practice. Thus, for example, should a company state in its privacy notice that it will not transfer a consumer's data to a third party, any subsequent transfer of data to third parties is likely to be considered a deceptive trade practice.

The financial penalties for unfair or deceptive trade practices can be enormous. These financial penalties can be imposed through a consent decree or through fines imposed by the FTC and approved by the courts. In many instances, the FTC will seek a consent decree with the company through which the company agrees, without admitting guilt, to pay certain

fines, stop the alleged practices, or implement new or improved privacy policies and practices. Alternatively, if the company refuses to enter a consent decree, the FTC can seek judgment through an administrative law judge. Should the company refuse to adhere to the FTC ruling, it may be fined up to $43,280 per violation and be liable for any damages caused by the alleged acts. Importantly, each instance of the alleged privacy violation constitutes a unique violation for the purposes of such penalties, leading to potentially substantial fines.

Over the past several years, the FTC has been increasingly active in enforcing unfair and deceptive trade practices that concern consumer data privacy. In 2019 alone, the FTC brought 130 spyware and spam cases as well as 80 general privacy lawsuits. The biggest privacy case of 2019 was *In the Matter of Facebook*, in which the FTC and the social media giant agreed to a consent decree requiring Facebook to pay a five billion dollar fine and institute a broad and privacy-related corporate restructuring. This year, the FTC has commenced 102 actions related to privacy, including cases against Zoom Video Communications, Inc., Williams Sonoma, Inc., and the Western Union Company.

The ability of the FTC to impose substantial penalties on companies who willingly or unwillingly deviate from the practices described in their privacy notices makes it extremely important to routinely review and update your company's privacy notice to ensure that it accurately depicts your company's privacy practices.

HEALTH CARE LAW ADVISOR ALERT: VACCINE INJURY CLAIMS AND THE FEDERAL VACCINE COURT

As the development of a potential COVID-19 vaccine continues, so too do questions about the types of vaccines being developed and how they will be administered. Vaccines offer overwhelming public health benefits, but a small number of individuals who receive vaccines are harmed by them. Most claims alleging health problems caused by vaccines must be brought in the "Vaccine Court" of the United States Court of Federal Claims under the National Childhood Vaccine Injury Act of 1986, 42 U.S.C. § 300aa-1, *et seq*.

The Act creates the National Vaccine Injury Compensation Program to handle vaccine-related claims. The program is administered by a secretary who may compensate a party who has suffered a vaccine-related injury or death. The Act largely preempts traditional tort claims against vaccine administrators or manufacturers for vaccine-related injuries and it limits claimants to only those sustaining injury or their legal representatives.

The Act creates a Vaccine Injury Table listing various vaccines and medical conditions that may result from them. Claimants must show, by a preponderance of evidence, that they suffered an injury listed in the Table or that a vaccine caused or significantly aggravated their injury within the time periods set forth in the Table. *Terran ex rel. Terran v. Sec'y of Health and Human Servs.,* 195 F.3d 1302, 1307 (Fed. Cir. 1999), *cert. denied,* 531 U.S. 812 (2000). If claimants do so for an injury listed in the Table within the time period stated in the Table, they are presumed to be entitled to compensation. *Knutson by Knutson v. Sec'y of Health and Human Servs.*, 35 F.3d 543, 547 (Fed. Cir. 1994). For claims not falling within the Table, claimants must prove the vaccine at issue caused their injury by a preponderance of evidence. *Golub v. Sec'y of Health and Human Servs.*, No. 99-5161, 2000 WL 1471643, at *2 (Fed. Cir. Oct. 3, 2000). Claimants are limited to a recovery of $250,000 for pain and suffering, but may recover additional damages for actual and projected un-reimbursable expenses, actual and anticipated lost earnings, and reasonable attorneys' fees and costs.

Claims made to the Vaccine Court are sent to the office of the Chief Special Master, who then assigns the claim to a special master to review and issue a decision to be entered as a judgment by the Federal Court of Claims. Either party can request that the Federal Court of Claims review this decision, and also can seek further review in the United States Court of Appeals for the Federal Circuit. Judicial review of the special masters' decision is limited; the decision can be set aside only if either court determines it is arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law. If claimants choose to reject a judgment by the Vaccine Court, they then may pursue a tort action in state or federal court. However, the Act offers certain defenses and presumptions to defendants facing such claims.

For more information about the Vaccine Court, or other legal issues relating to the COVID-19 pandemic, contact Grant Killoran of O'Neil Cannon at 414-276-5000 or grant.killoran@wilaw.com.

TAX AND WEALTH ADVISOR ALERT: A BRIEF OVERVIEW OF WISCONSIN'S MARITAL PROPERTY SYSTEM

In general, states are considered either "common law property" or "community property" states. Wisconsin, along with a few other states, is a community property state (community property is referred to as "marital property" in Wisconsin). It is important to understand the difference between these two systems for purposes of wealth management planning, estate planning, and divorce.

Under the common law property system, assets and debts earned or acquired by one spouse during the marriage belong only to that spouse. With this type of system, only assets and debts that are titled under the name of both spouses are owned by both spouses. Under Wisconsin's marital property system, all assets and debts acquired or earned during a marriage belong to both spouses, regardless of whose name the assets and debts are titled under. It is important to emphasize that this general rule applies only to assets or debts acquired *during* the marriage—assets and debts acquired before the marriage remain the individual property of whichever spouse brought the assets or debts to the marriage. There are, however, some exceptions to this general rule, such as assets acquired as a gift or through inheritance. Also, non-marital property that is comingled with marital property may be unintentionally reclassified as marital property. Income and appreciation incurred on a non-marital asset may also be deemed marital property.

Spouses living in Wisconsin may wish to enter into a marital property agreement to define and clarify ownership of their assets and debts. Because classifying and defining assets and debts may be difficult, as the above-paragraph outlines, some spouses may wish to enter into a marital property agreement "opting into" Wisconsin's marital property system. By doing so, the spouses can be certain that their property will be classified as marital property, which may have certain tax and estate planning advantages. On the other hand, some spouses may want their property to be subject to a common law property system to protect assets for their children from a prior marriage or shield assets in a potential divorce. These spouses should consider entering into an agreement "opting out" of Wisconsin's marital property system.

Overall, understanding the distinction between common law property systems and community property systems is important for wealth management planning, estate planning, and divorce. Whether it makes sense for spouses living in Wisconsin to opt out of or opt into Wisconsin's marital property system depends on a variety of factors that you should discuss with your estate planning attorney.

If you would like to learn more about Wisconsin's marital property laws and how they affect your estate plan, please contact attorney Kelly M. Spott.

EMPLOYMENT LAWSCENE ALERT: THE ELECTION IS ALMOST HERE—VOTING LEAVE IN WISCONSIN

Tuesday, November 3, 2020 is Election Day. Although early voting is underway and many

individuals have already returned their absentee ballots, many people will want to vote in-person on Election Day. All Wisconsin employers are required to provide employees who are eligible to vote up to three consecutive hours of unpaid leave to vote while the polls are open (from 7 AM until 8 PM), and employees must request the time off prior to the election. Voting leave cannot be denied on the basis that employees would have time outside of their scheduled work hours to vote while the polls are open, but employers can specify which three hours an employee is permitted to utilize. Employers may not penalize employees for using voting leave. Although voting leave is unpaid, employers should remember that, under the FLSA, they may not deduct from an exempt employee's salary for partial day absences.

Additionally, all Wisconsin employers are also required to grant an employee who is appointed to serve as an election official 24 hours of unpaid leave for the election day in which the employee serves in his or her official capacity. Employers may not penalize employees for using election official leave. Employees must provide their employers with at least seven days' notice of their need for this leave.

Finally, Wisconsin employers are not permitted to make threats that are intended to influence the political opinions or actions of their employees. Specifically, employers cannot distribute printed materials to employees that threaten to shut down the business, in whole or in part, or reduce the salaries or wages of employees if a certain party or candidate is elected or if any referendum is adopted or rejected.

As always, O'Neil, Cannon, Hollman, DeJong and Laing is here for you. We encourage you to reach out with any questions, concerns, or legal issues you may have.

THE WILAW QUARTERLY NEWSLETTER

Newsletter Article Highlights:

- Don't Be Caught Off Guard by the Tax and Legal Consequences of Your New Quarantine Hobby
- Overview of Data Protection Laws in Wisconsin
- Strike While the Giving is Good—Historically High Estate and Gift Tax Exemptions May Be Reduced or Eliminated as Early as January 1, 2021
- DOL Updates FFCRA Leave Regulations
- Videoconferencing Considerations for Health Care Litigators

Firm News:

- John Gehringer Named "Lawyer of the Year"

- Attorney Joseph Gumina Featured in *Merit Shop Contractor*
- 20 OCHDL Lawyers Selected as 2021 Best Lawyers®; Another 5 Named Best Lawyers: Ones to Watch

Click the image below to read more.



HEALTH CARE LAW ADVISOR ALERT: TELEHEALTH IN WISCONSIN (PART 2 OF 2)

Medical Malpractice Risk and Telemedicine Policies

This article is the second of a two-part series on telehealth in Wisconsin. The first article of this series, available here, highlighted basic standards for regulatory compliance in the design of internal telehealth policies. This second article addresses the practitioner's obligation to minimize patient harm (and thus practitioner liability) with attention to the medical standard of care when assessing when and how telehealth is appropriate for each patient.

A. Maintaining Medical Standard of Care in Telemedicine

Wisconsin medical providers must critically evaluate whether their use of a telemedicine platform would permit their evaluation and treatment of each patient in compliance with "the standard of minimally competent medical practice."[i] Standards of practice and conduct required for in-person visits, including standards relating to patient confidentiality and recordkeeping, must be observed in the telehealth context.[ii]

In view of these standards articulated by the Wisconsin medical examining board, internal telemedicine policies and procedures must preserve the same degree of quality and safety achieved during in person appointments. Clinical leadership must assess whether quality of patient care can be maintained via telehealth, an evaluation which is dependent upon the provider's area of specialty, the patient's condition, and other factors. For example, the use of telemedicine is not suitable for conditions where physical examinations are necessary, because of extreme symptoms, forceful interventions, or in the case of medical procedures for which certain protocols need to be followed.[iii]

Clinical guidelines specific to telemedicine can serve as important indicators as to whether your practice should incorporate telemedicine for specific patient encounters or diagnostic evaluations.[iv] However, guideline compliance does not guarantee accurate diagnosis or safe and effective medical care meeting the standard of care. Local circumstances must be considered, and the practitioner is ultimately responsible for all decisions regarding the appropriateness of a specific course of action.[v] Published guidelines for every clinical scenario and application simply do not exist and so by necessity may need to be developed in-house.[vi] The policies of each medical practice should delineate between circumstances in which various telehealth platforms can, and cannot, preserve the quality of care for patients. Providing treatment recommendations, including issuing a prescription, based only on a static electronic questionnaire does not meet the standard of minimally competent medical practice.[vii]

Sometimes the proper standard of care is reflected in government reimbursement decisions. For example, the Wisconsin Department of Health Services' ("DHS") expansion of telehealth coverage will exclude comprehensive assessment and care planning for children with complexities, since this requires an in-person assessment. However, case management for children with complex medical needs will be covered. Certain, but not all, dental evaluations will be covered. Certain therapy services will be covered.[viii]

Where clinical leadership determines that telehealth is appropriate, workflow must be re-evaluated in the telehealth context to maintain the standard of care. For example, staff responsibilities may require adjustment for telehealth encounters to ensure that updates to the medical record, physician orders and the "after visit summary" are properly recorded in connection with each telehealth encounter. Providers may consider requiring immediate scheduling of patients who express symptoms that require in-person evaluation during a telemedicine visit to promote patient safety and minimize liability. Providers might also consider whether patient/family coaching regarding medication administration is properly handled in the telehealth context.

B. Telephone and Texting: Risk Mitigation

While the use of synchronous audio and video visits has exploded in the wake of the

COVID-19 pandemic, physicians have provided routine medical advice by phone for decades, responding to patient calls reporting a change in condition and advising medication changes by phone communications. Surveys of patients since the COVID-19 pandemic indicates that texting is a preferred method of communication over phone calls.[ix] In addition to health care privacy and security issues (outside of the scope of this article), what are some of the legal considerations for such telephone and texting encounters?

First, practitioners must observe the criteria for government and private insurer reimbursement of telehealth, unless their practice is limited to self-pay. In the case of Medicaid reimbursement, the Wisconsin Medical Assistance Program generally covers consultations through "interactive telehealth" and certain asynchronous telehealth services and remote patient monitoring.[x] The Wisconsin Statutes delegate authority to DHS to determine whether to include telephone encounters within the definition of "telehealth."[xi] DHS is temporarily providing coverage for certain telephone visits during COVID-19 pandemic, and the agency may ultimately decide to continue coverage of certain telephone communications as part of its permanent policy.[xii] Audio-only telephone communications must be delivered with the functional equivalency of a face-to-face encounter in order to be covered by Wisconsin Medicaid during the COVID-19 pandemic.[xiii]

If the patient will be located out-of-state, the provider must assess whether the applicable state's criteria for Medicaid telehealth reimbursement differs from the requirements imposed by Wisconsin Medicaid.[xiv] If federal Medicare will instead serve as payor, the Centers for Medicare and Medicaid Services ("CMS") will reimburse certain audio-only phone visits during the COVID-19 public health emergency. For reimbursement purposes, CMS distinguishes "telephone visits" from "services that "would normally occur in person." Telephone visits are "not paid as though the service occurred in person," and reimbursement may be bundled into a pre- or post-service if the phone encounter falls within the previous seven days of a prior visit or leads to a subsequent evaluation/management service.[xv]

Because audio-only telephone and texting encounters are inherently more limited with respect to patient evaluation capabilities, providers should exercise caution when using these modes of telehealth in circumstances that would usually *or could* warrant a physical evaluation of the patient based upon medical history or the symptoms described when scheduling an appointment. In addition to introducing risk of medical malpractice claims, providers risk non-compliance with criteria for reimbursement, such the standard of "functional equivalency to the face-to-face service" required by state Medicaid for reimbursement. The "functional equivalency standard" applicable to state government reimbursement is higher than the "the standard of minimally competent medical practice" generally applicable to the practice of telemedicine in the state.[xvi]

C. Updates to Telehealth Policies and Procedures

Irrespective of whether government reimbursement is in play, your medical practice policies and procedures should be updated to mitigate risk to patient care and safety in the telehealth context. Your internal policies and procedures should delineate between when telemedicine is (and is not) appropriate based upon a critical assessment of each of the several evaluative and diagnostic services provided by your practice. Staff, including schedulers and nurses, should be trained as to when scheduling a telemedicine appointment poses risk to your patients and your practice. Your policies should incorporate customized procedures designed to preserve the standard of care and the medical recordkeeping requirements imposed by the Wisconsin medical examining board for the practice of telemedicine. In addition, physicians practicing telemedicine should confirm that their medical malpractice insurance coverage applies outside of the traditional health care facility settings.

OCHDL's health care practice group will continue to monitor telehealth regulations and related guidance as the standard of care for telemedicine evolves. For more information on this topic, contact Marguerite Hammes at 414-276-5000 or marguerite.hammes@wilaw.com.

---

[i] ***See*** **WIS. ADMIN. CODE § MED 24.06.**

[ii] ***See*** **WIS. ADMIN. CODE § MED 24.05. (requiring the same standard of practice and conduct regardless of whether health care services are provided in person or by telemedicine). The standard of care that is required of all Wisconsin health care providers is defined as the degree of skill, care, and judgment which reasonable health care providers who practice the same specialty would exercise in the same or similar circumstances, having due regard for the state of medical science at the time.** ***Nowatske v. Osterloh*****, 198 Wis.2d 419, 543 N.W.2d 25 (1996),** ***abrogated on other ground by Nommensen v. American Continental Ins. Co.*****, 246 Wis.2nd 132, 629 N.W.2d 132 (2001); Wis. J.I. Civil No. 1023.**

[iii] Secure Medical, Best Telemedicine Clinical Guidelines (April 13, 2018), available at https://www.securemedical.com/telemedicine/best-telemedicine-clinical-guidelines/

[iv] ***E.g.,*** **American Telemedicine Association, Practice Guidelines Archives, available at https://www.americantelemed.org/resource_categories/practice-guidelines/ ; Pantanowitz, Liron et al. "American Telemedicine Association clinical guidelines for telepathology." Journal of pathology informatics vol. 5,1 39. 21 Oct. 2014, doi:10.4103/2153-3539.143329; Krupinski, Elizabeth A, and Jordana Bernard. "Standards and Guidelines in Telemedicine and Telehealth." Healthcare (Basel, Switzerland) vol. 2,1 74-93. 12 Feb. 2014, doi:10.3390/healthcare2010074.**

[v] Elizabeth A. Krupinski and Jordana Bernard, Standards and Guidelines in Telemedicine and Telehealth, Healthcare 2014, 2, 74-93; doi: 10.3390/healthcare2010074, at 81.

[vi] ***See*** **Standards and Guidelines in Telemedicine and Telehealth, Healthcare, supra note 5, at 81.**

[vii] ***See*** **WIS. ADMIN. CODE § MED 24.07 (2).**

[viii] ***See*** **Brook Anderson, Wisconsin DHS Benefits Policy Section Chief, Telehealth Expansion: Acute and Primary Services, available at https://www.dhs.wisconsin.gov/telehealth/telehealth-expansion-all-provider.pdf (revised July 30, 2020).**

[ix] SR Heath, Patient Communication Preferences: the COVID-19 Impact, July 30, 2020, available at https://mhealthintelligence.com/resources/white-papers/patient-communication-preferences-the-covid-19-impact eid=CXTEL000000554482&elqCampaignId=16139&utm_source=ded&utm_medium=email&utm_campaign=dedicated&elqTrackId=607a1670c3c349349ac195f03c60cba2&elq=362f09f490fe41169f2fc16dbcab5410&elqaid=16904&elqat=1&elqCampaignId=16139

[x] ***See*** **WIS. STAT. § 49.46(2)(b)(21)-(22).**

[xi] ***See*** **WIS. STAT. § 49.45(61)(a)(4); §49.46(2)(b)(23).**

[xii] ***See*** **ForwardHealth Update 2020-12, "Temporary Changes to Telehealth Policy and Clarifications for Behavioral Health and Targeted Case Management Providers" (revised May 8, 2020), available at https://www.forwardhealth.wi.gov/kw/pdf/2020-12.pdf**

[xiii] ***See id*****.**

[xiv] ***See*** **Center For Connected Health Policy, State Telehealth Laws and Reimbursement Policies (Fall 2020), available at https://www.cchpca.org/sites/default/files/2020-10/CCHP%2050%20STATE%20REPORT%20FALL%202020%20FINAL.pdf**

[xv] ***See, e.g.,*** **Centers for Medicare and Medicaid Services, COVID-19 Frequently Asked Questions (FAQs) on Medicare Fee-For-Service (FFS) Billing (revised October 20, 2020), at 63-79, available at https://www.cms.gov/files/document/03092020-covid-19-faqs-508.pdf**

[xvi] ***Compare*** **Wisconsin ForwardHealth Telehealth Expansion and Related Resources for Providers, available at https://www.forwardhealth.wi.gov/WIPortal/content/html/news/telehealth_resources.html.spage , *with* WIS. ADMIN. CODE § MED 24.06.**

IS YOUR HOTEL WEBSITE IN COMPLIANCE WITH THE ADA?

There has been a trend recently in the state of Wisconsin, and elsewhere, for attorneys to file lawsuits against hotel owners alleging that their websites are in violation of the Americans with Disabilities Act ("ADA") because they are not accessible to disabled individuals. Specifically, the complaints allege that the hotel websites are in violation of the ADA because they fail to identify accessibility features, do not allow for booking of accessible rooms, and do not provide sufficient information regarding accessible rooms and amenities at the hotel.

Frequently, the attorneys bringing the lawsuits against the hotel owners will represent the same disabled party (often referred to as a "tester"), use a stock, form set of allegations

against several hotel owners, and file more than one lawsuit at a time. Based on the sheer volume of these cases in recent weeks, it is unlikely these lawsuits will cease any time soon.

The parties filing the lawsuits typically assert that hotel owners must ensure that their website (and the third-party booking websites used to reserve their rooms) meet certain requirements. For example, the plaintiffs assert that hotel websites must:

- identify and describe accessible features in the hotels and guest rooms offered through their reservation service in enough detail to reasonably permit individuals with disabilities to assess independently whether a given hotel or guest room meets their accessibility needs;
- ensure that assessible guest rooms are held for use by individuals with disabilities until all other guest rooms of that type have been rented and the accessible room requested is the only remaining room of that type; and
- reserve, upon request, accessible guest rooms or specific types of guest rooms and ensure that the guest rooms requested are blocked and removed from all reservations systems.

If you or your business receives a demand letter threatening legal action or are served with a lawsuit, you should promptly contact an attorney to discuss your options.

TAX AND WEALTH ADVISOR ALERT: THE IMPORTANCE OF A POWER OF ATTORNEY FOR HEALTH CARE

A proper estate plan covers not only what should happen upon your death, but also what should happen if you lose your decision-making skills. While planning for incapacity may be as unpleasant as planning for death, it is an important step in the estate planning process. Planning for incapacity ensures that someone you specifically choose and trust can act on your behalf while you are unable to do so for yourself. In another article, we discussed the importance of a Durable Financial Power of Attorney. Here, we discuss why a Power of Attorney for Health Care is equally as important.

A Power of Attorney for Health Care is a document that allows you to appoint someone, your “health care agent,” to make medical decisions for you in the event you are unable to do so for yourself. This document allows your health care agent to communicate with your health care providers regarding what treatments you do and do not want.

You will still receive medical care if you do not execute a Power of Attorney for Health Care,

but you risk not having the right person speak for you on your behalf and not receiving the type of care or treatment you would want. For example, your physician may ask the court to appoint someone to act on your behalf, and your court-appointed agent could subject you to a medical treatment you did not want. Additionally, the appointment process can be expensive, public, and time consuming.

While a Power of Attorney for Health Care is an important part of your estate plan, it applies only to medical decision-making. For this reason, this document is often drafted as part of a larger estate plan.

The attorneys at O'Neil Cannon have experience in drafting various estate plans, both simple and complex, and would be happy to discuss the estate planning process with you. If you are interested in learning more about estate planning, please contact attorney Kelly M. Spott.

WISCONSIN BUSINESSES AND COMPLYING WITH CONSUMER DATA PROTECTION LAWS

As we have previously covered, Wisconsin businesses may be subject to the requirements of the European Union General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA). Additionally, many states, including Wisconsin, and the federal government are considering similar data protection bills that may impact Wisconsin businesses. With overlapping obligations, compliance with data protection laws is an increasingly tricky business for most companies. To ensure that your company doesn't inadvertently violate any current or future laws, consider the following six steps:

Step 1: Consider the Applicability of Data Privacy Laws

Companies should determine whether existing consumer data privacy laws apply to them. The GDPR applies to companies (1) established in the EU and conducting data processing in the context of that business's activities; or (2) either: (a) offering goods or services, for free or for a fee, to individuals in the EU or (b) monitoring the behavior of individuals within the EU.

Wisconsin companies with a physical presence in the EU will almost certainly be subject to the GDPR. Without a physical presence, a Wisconsin company will nonetheless likely fall within the GDPR's scope if it offers products or services to EU individuals or businesses or if it monitors the online behavior of EU individuals or businesses.

On the other hand, the CCPA will apply to your business if it is a **for-profit business that does business in the state of California and collects** California consumers' personal information (or such information is collected on its behalf) and determines the **purposes and means** of processing California consumers' personal information, AND if it meets *one* of the following criteria:

- It has at least **$25 million** in annual gross revenues;
- It buys, sells, shares, or receives the personal information of at least **50,000 California consumers, households, or devices** per year; *or*
- It derives at least **50 percent** of its annual revenue **from selling** California consumers' personal information.

Most companies should be able to determine whether they meet the above criteria. Some businesses may struggle to determine whether or not they buy, sell, share, or receive the personal information of at least **50,000 California consumers, households, or devices** per year. Still, companies with even a small or moderate online presence will likely meet this threshold due to the broad scope of the CCPA's definition of personally identifiable information (PII).

Once you have determined that the GDPR or CCPA applies, take affirmative steps to ensure that you are in compliance.

Step 2: Map Your Company's Data

Once you have determined that the GDPR or the CCPA applies to your company, you must map the data that your company collects. Mapping will include knowing the type of data you are collecting, its source, and what happens to the data after it has been collected. You should also identify where the data is kept, what encryption or other security your company uses to protect that data, who has access to the data, and whether there are any security risks.

This step is necessary and must be taken to understand what data your company collects and where and how it is stored so that you can take appropriate steps to ensure efficient compliance with applicable data protection rules.

Step 3: Clean Up Your Company's Data

Companies should be disciplined and strict about data collection. Determine what information is necessary and what information is superfluous. Moreover, think about why certain PII is retained, rather than deleted, in view of the company's data collection goals. You may find a greater financial gain in deleting troves of PII as opposed to investing in storage and encryption. Moreover, deleting unnecessary files can help reduce the risk of inadvertently committing data protection violations.

This step will not only help ensure compliance, but it will also allow you to develop an effective and potentially financially valuable strategy for data collection.

Step 4: Create Privacy Protection Procedures and Policy

To ensure that consumers may exercise the rights to their PII granted to them under the GDPR and the CCPA, your company must have efficient processes. In crafting a privacy protection policy, consider:

- how individuals can give consent for data collection and transfer;
- the process for a consumer to request data deletion or to opt-out of data collection;
- how the company can ensure complete, effective data deletion or tagging across all platforms;
- the process for responding to a hypothetical data breach; and
- how the company can ensure that minors give proper consent.

When creating privacy procedures and policies for your company, it is important to understand that the relevant consumer data privacy laws require transparency in matters concerning PII. Therefore, your company's privacy procedures and policies must be drafted carefully and with the complex obligations of the GDPR or the CCPA in mind.

Step 5: Update Your Company's Online Privacy Policy

Under the GDPR or the CCPA, your company must have an easily accessible and understandable privacy policy. To ensure that your company's privacy policies comply with the GDPR and the CCPA, you must ensure that it contains the following:

- A statement to residents of California or the EU that they have the right to opt-out of the sale of their data;
- An explanation that indicates how the company will inform consumers of future privacy policy updates; and
- A description of how the consumer's data will be used, including all possible uses that involve a transfer of that data.

Furthermore, you must update your company's privacy policy at least once every 12 months and notify consumers of each such update. As discussed, every privacy policy must be easily accessible and transparent. Even unintentionally complex policies may expose your company to liability.

Step 6: Update Your Company's Website

Finally, to comply with the GDPR and the CCPA, a company must include a link on its website that says "Do Not Sell My Personal Information." The link must use that specific phrasing and bring users to a page that allows them to opt-out of any sale of their data. This link must be

separate from the general privacy agreement and cannot require the consumer to create a profile or account to access the opt-out. The CCPA also requires companies to create a toll-free number for consumers wanting to opt-out of the sale of their data.

After a consumer opts out, a company has two options under the CCPA: (1) it can retain the consumer's PII but exclude that PII from any sale, or (2) it can delete the consumer's data entirely. However, the GDPR requires the company to delete the consumer's data entirely. Thus, it is very important to understand whether the CCPA or GDPR (or both) applies and to have specific procedures in place to respond to a consumer's request to opt out.

What to Expect in Wisconsin

Because the GDPR and the CCPA are intentionally extraterritorial, their obligations may easily reach Wisconsin businesses. Furthermore, because of the steep fines for violating these data protection laws, Wisconsin businesses must either confirm that they are not subject to these strict requirements or take proactive steps to ensure compliance.

Even if the GDPR and the CCPA currently do not apply to your company, it may not be long until Wisconsin or the federal government implements a consumer data protection law that does. Consequently, regardless of whether you do business in the European Union or in California, beginning to implement better data collection practices now may help your companies online reputation and reduce future risks.

O'Neil, Cannon, Hollman, DeJong and Laing remains open and ready to help you.

TAX AND WEALTH ADVISOR ALERT: NEW STREAMLINED FORGIVENESS FOR PPP LOANS UP TO $50,000

Late last week, the Department of Treasury and Small Business Administration (SBA) jointly released a new loan forgiveness application for Paycheck Protection Program loans of $50,000 or less. This new streamlined application removes calculations required on prior forms and simplifies documentation requirements, relieving both borrowers and lenders of the prior compliance burdens present in the older form.

Pursuant to an interim final rule, the simper one-page application form, SBA Form 3508S, does not require borrowers to reduce their forgiveness amount for any reductions in full-time equivalent (FTE) employees or in salaries or wages. Additionally, the new form does not

require borrowers to show calculations used to determine their loan forgiveness amount. With that said, the SBA could request additional information and documents as part of its loan review process.

While simpler overall, the application still requires the borrower to make certain certifications regarding the accuracy of the information reported. Further, the application requires the borrower to submit documentation supporting the fact that the use of the loan proceeds was for eligible costs. Borrowers who, together with their affiliates (as determined under SBA rules), received loans of $2 million or more are ineligible to use the new streamlined application. For example, if an entity has a loan of $50,000 and its parent corporation has a loan of $1.95 million, the former would not be able to use Form 3508S to apply for loan forgiveness.

Form 3508S and its accompanying instructions are posted on the SBA's website.

O'Neil, Cannon, Hollman, DeJong and Laing remains open and ready to help you. For questions or further information relating to the new streamlined application for PPP loans under $50,000, please contact the author of this article, Attorney Britany E. Morrison.