Confidentiality and Privacy in the time of COVID-19

Melissa Cranford, Partner
Robin Cross, Senior Attorney / Tessa Meredith, Associate
Messer, Fort & McDonald, PLLC
6371 Preston Rd., Suite 200
Frisco, Texas 78701
972.668.6400
www.txmunicipallaw.com

Introduction: Confidentiality and COVID-19

A constant struggle exists between privacy, information flow, and employer monitoring in the modern-day workforce. Employers in the past have battled to balance privacy rights and employee health, as shown through the development of policies and accommodations through existing legislation. The COVID-19 pandemic has only magnified the complexities of these competing workplace interests. Public health and government officials have had to adjust current legislation to ensure the public wellbeing during the pandemic, similarly to employers and their employees. The multitude of relevant federal and state statutes builds upon the pre-existing employer confusion, which is further stressed by a global pandemic. Employees have their own anxieties when entering back into the "in person" workplace. For example, potential coworker exposure, varying vaccination status among staff, and privacy of one's own health information are paramount employee concerns. With privacy laws in this country often hanging in the balance, governmental bodies, employers, and employees must adapt and stay aware of the changes happening around them.

I: Common Questions and Best Practice Answers

Can employers disclose an employee's COVID-19 Diagnosis'?

Employers may create standard communications to notify employees of close contact exposure but should refrain from directly identifying the contagious or potentially contagious employee. Employees are free to identify themselves to co-workers or to ask non-subordinate co-workers if they are symptomatic, vaccinated or COVID-19 positive. Likewise, co-workers may respond to co-worker questions or decline to answer.

May an employer - require proof of COVID-19 vaccination proof?

For most public employees in Texas, employers may inquire as to vaccination status, but may not require proof in order to allow an employee to work. Moreover, Governor Abbott's *Executive Order GA-40*, prohibits public employers from requiring any individual to get a COVID-19 vaccine. GA-40 does not include any restrictions on required testing for COVID-19. GA-40 is limited to the COVID-19 vaccine and employers may seek additional information regarding an employee's vaccination status for other vaccines when it is relevant, job-related, and consistent with business necessity.

Federal law differs and in the case of CMS covered workers, likely supersedes GA-40. For EMT/paramedics or first responders working in departments which bill the Center for Medicare and Medicaid Services ("CMS"), workers are subject to the CMS vaccination requirement.

May employers interview employees to determine signs or symptoms of COVID-19 or other communicable diseases?

Guidance issued by the Equal Employment Opportunity Commission ("EEOC") provides that employers are permitted to seek information from all employees who will be physically entering the workplace if they have been recently diagnosed, exposed to, or are experiencing symptoms associated with COVID-19. Employers are further permitted to take the temperature of employees

and members of the public entering a publicly operated building or workplace. Additional health related inquiries must be made consistent with the requirement expressed under the American with Disabilities Act ("ADA") that mandatory medical test of employees be "job related and consistent with business necessity".[1] This would include fitness for duty inquiries or exams for employees experiencing the symptoms of long-COVID-19. Under the framework of the Family Medical Leave Act ("FMLA"), employers remain limited in the information they can seek from employees who utilize leave under the FMLA to determine whether the employee or a dependent is experiencing a qualifying serious health condition.

Quarantine Requirements

The Families First Coronavirus Response Act ("FFCRA") required employers to offer paid leave to employees impacted by COVID-19. But with the FFCRA expiring on December 31st, 2020, employers are left to formulate internal quarantine policies.

In June 2021, TX Local Gov't Code § 180.008 was enacted, creating a model policy for Paid Quarantine Leave for Fire Fighters, Peace Officers, Detention Officers, and Emergency Medical Technicians. This enactment mandates governmental bodies to develop and implement paid quarantine leave for essential workers for workers with possible or known exposure to a communicable disease while on duty.[2]

II: Relevant Statutes and References

The Constitution and Privacy Rights

The United States Constitution and its amendments does not list an individual right to privacy as an enumerated right. Rather, an intrinsic right to privacy has been determined, through case law, to exist within the Bill of Rights and additional amendments, but the scope and application of this right remains heavily litigated and debated. Privacy oriented case law relative to communication about communicable disease and vaccination requirements is no exception. *Jacobson v. Commonwealth of Massachusetts* is an outlining precedent of what to expect from case law following the COVID-19 pandemic. The Court opined that "the board of health of a city or town, if, in its opinion, it is necessary for public health or safety, shall require and enforce the vaccination and revaccination of all inhabitant thereof, and shall provide them with the means of a free vaccination."[3] The Court sided against the defendant's 14th amendment claim, stating that "the authority of the state to enact this statue is to be referred to…the police power-a power which the state did not surrender when becoming a member of the union under the Constitution."[4] Additionally, "the Court has refrained from any attempt to define the limits of that power, yet it has distinctly recognized the authority of a state to enact quarantine laws and 'health laws of every description.'"[5] Even further, "according to settled principals the police power of a state must be held to embrace at least, such reasonable regulations established directly by

[1] 29 C.F.R. § 1630.14.
[2] Tex. Loc. Gov't Code 180.008(b).
[3] *Jacobson v. Commonwealth of Massachusetts*, 197 U.S. 11 (1905).
[4] *Id*. at 14.
[5] *Id*.

legislative enactive as will protect the public health and public safety."[6] The court in *Katz v. United States* held "virtually every governmental action interferes with personal privacy to some degree. The question in each case is whether that interference violates a command of the United States Constitution."[7] This emphasizes the argument that the Constitution does not explicitly provide a right to privacy overall, but rather rights of privacy are read into the amendments by the courts. For example, the First Amendment provides freedom of association along with privacy to that association, the Fourth amendment provides individuals a general privacy to unreasonable searches and seizures, and the Fourteenth amendment provides privacy from the government.[8] The Supreme Court upheld this notion in *United States v. Jones*, holding that the Fourteenth Amendment provides "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."[9] The notion that privacy rights do not exist within the Constitution, allows for federal and state laws to fill in the gaps while also create conflicting policies.

HIPAA

The Health Insurance Portability and Accountability Act ("HIPAA") has expanded patient privacy since 1996. The Privacy Rule under HIPAA protects the personal health information and medical records of individuals, with limits and conditions on the various uses and disclosures that can and cannot be made *without patient authorization.*[10] This privacy rule also gives every patient the right to inspect and obtain a copy of their records and request corrections to their file. Section 160.103 defines "protected health information" (PHI) as individually identifiable health information that is transmitted or maintained in electronic media or any other form or medium.[11] Additionally the Act identifies "individually identifiable health information" as information that is a subset of health information, including demographic information collected from an individual, and information that:

> (1) Is created or received by a health care provider, *health plan, employer*, or health care clearinghouse; and
>
> (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
>
> *(i) That identifies the individual; or*
>
> *(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.*[12]

The HIPAA privacy rule is not suspended during a public health crisis per se, but certain provisions and the related penalties can be waived.[13] For the Secretary of the Department of Health and

[6] *Id*.
[7] *Katz v. United States*, 389 U.S. 367, 350 (1967).
[8] *See generally Katz v. United States*, 389 U.S. 347, (1967).
[9] *United States v. Jones*, 565 U.S. 400, 404, 132 S. Ct. 945, 949, 181 L. Ed. 2d 911 (2012).
[10] 45 C.F.R. § 160.103 (emphasis added).
[11] *Id*.
[12] *Id*. (emphasis added).
[13] 42 U.S. Code § 1320b–5.

Human Services ("HHS") to waive the Privacy Rule, two conditions must be met: the President declares an emergency or disaster; and the Secretary of HHS declares a public health emergency.[14] Xavier Becerra, Secretary of Health and Human Services, on April 16, 2022, renewed the previous determination that a public health emergency exists currently nationwide.[15] Covered entities may, if directed by a Public Health Authority, disclose PHI for the purpose of preventing and controlling disease, injury or disability.[16] Authorized measures include: reporting of disease or injury, reporting vital events (death tolls), and conducting investigations and interventions.

Does the Privacy Rule protect employment records?

Generally, HIPAA does not apply to employee health information maintained by their employers. HIPAA does not cover all employee benefit information, including life insurance information, disability, wellness programs, and workers' compensation information. HIPAA's privacy rule applies only to "covered entities," which are defined as: (1) health plans; (2) healthcare clearinghouses; and (3) healthcare providers that electronically transmit certain health information (and certain "business associates" of covered entities).[17] Employers who send or receive health information to a health care plan may be a "covered entity."[18] Employers who do not fall into one of those categories are not "covered entities" and therefore not subject to the privacy restrictions under HIPAA. Even where employers are considered a "covered entity," HIPAA does *not* apply to health care information contained "in employment records held by a covered entity."[19] However, an employer may subject itself or incur the privacy rule's requirement when seeking or storing employee health information, by requesting PHI from a covered entity. For example, while a pre-hire drug test is not considered a medical exam subject to the protections of HIPPA, the results of the test do contain PHI and should be managed as a confidential health record.

HIPAA's Security Rule defines and regulates the standards, methods and procedures related to the protection of electronic PHI on storage, accessibility, and transmission.[20] Within this rule exists three safeguard levels of security. The administrative safeguards deal with the assignment of a HIPAA security compliance team. Technical safeguards deal with the encryption and authentication methods used to have control over data access. Physical safeguards access the protection of any electronic system, data or equipment within your facility and organization. The risk analysis and risk management protocols for hardware, software and transmission fall under this rule.

American with Disabilities Act

The Americans with Disabilities Act requires persons with disabilities, in certain circumstances, to disclose private health information. This requirement can place the person with a disability in a vulnerable position, as they risk negative employment and/or social consequences from the

[14] 42 U.S.C.A. § 247d.
[15] Xavier Becerra, *Renewal of Determination That A Public Health Emergency Exists (2022)*, https://aspr.hhs.gov/legal/PHE/Pages/COVID19-12Apr2022.aspx (last visited Jun 9, 2022).
[16] *See* 45 CFR 164.512(b)(1)(i).
[17] 45 C.F.R. § 160.103.
[18] *Id*.
[19] *Id*. (emphasis added).
[20] 45 C.F.R. § 164.306.

potential exposure of this private information. To address this risk, the ADA includes a confidentiality provision to limit the disclosure of health information once it has been obtained. Title I of The American with Disabilities Act requires employers to collect all information obtained regarding an applicant or employee's medical condition or history on separate forms, maintain the information in separate medical files and treat such information as confidential medical records[21] This protection covers all applicants or employees, regardless of whether they are a qualified individual with a disability under the ADA.[22] Under the ADA, this confidentiality protection includes medical diagnoses, prescribed treatments, and information concerning whether the employees have requested or are receiving reasonable accommodations. However, the ADA does carve out three exceptions from this general confidentiality mandate: (i) supervisors and managers may be informed regarding necessary restrictions on the work or duties of the employee and necessary accommodations; (ii) first aid and safety personnel may be informed, when appropriate, if the disability might require emergency treatment; and (iii) government officials investigating compliance with this provision of the ADA shall be provided relevant information upon request..[23] Courts transposed this statutory framework into a three step inquiry for determining whether an employee can recover monetary damages from an employer for violating the Title I confidentiality requirements.[24] The first inquiry asks, as a threshold matter, whether the medical information was received because of an employer-initiated medical inquiry or exam. The second inquiry is whether the information was disclosed by the employer or otherwise not kept confidential (or whether an exception applies). The final inquiry is whether the employee suffered a tangible injury as a result of the disclosure.

A. Employment-Related Medical Inquiry or Exam

The threshold inquiry for any ADA confidentiality case is whether the health information at issue is actually confidential within the meaning of the ADA. Health information is only confidential under the ADA if it was provided to the employer in response to a medical inquiry or exam concerning the applicant or employee.[25] This means the information provided to employers either voluntarily or as the result of a non-medical inquiry is not confidential under the ADA.[26] Disclosure is not considered "voluntary" if the employer solicited the information by making a medical inquiry or exam for the purposes of determining fitness for duty or assessing an accommodation request.

General inquiries are not medical inquiries unless the employer has pre-existing knowledge of a medical condition.[27] For example, general questions such as "is everything okay?" or "how are you doing?" would not typically be considered a medical inquiry unless in context the employer is seeking specific information about a known condition. *E.E.O.C. v. Thrivent Financial* provides further guidance. In *E.E.O.C. v. Thrivent Financial for Lutherans,* the employer sent an email to the employee that stated "we need to know what is going on" because the employee had failed to

---

[21] Americans with Disabilities Act, 42 U.S.C. § 12112(d)(3)(B); §12112(d)(4)(C).
[22] *McPherson v. O'Reilly Automotive, Inc*., 491 F.3d 726 (8th Cir. 2007).
[23] Americans with Disabilities Act, 42 U.S.C. § 12112(d)(3)(B)(i)-(iii).
[24] *See, e.g., Shoun v. Best Formed Plastics, Inc.*, 28 F.Supp.3d 786, 788-89 (N.D. Ind. 2014) (citing *Franklin v. City of Slidell*, 936 F.Supp.2d 691, 710-11 (E.D. La. 2013).
[25] 42 U.S.C.A. § 12112.
[26] *Id*.
[27] *Id*.

report for work.[28] The employee responded by explaining that he had a severe migraine. The Court found that the employer's email was not a medical inquiry. In reaching this conclusion, the Court held that for an employer's inquiry to constitute a medical inquiry for purposes of the ADA confidentiality provision, the employer must have had preexisting knowledge that the employee was ill. Since Thrivent had no such knowledge, its inquiry was not medical and the plaintiff's response that he had a migraine condition was not confidential. The preexisting knowledge rule has been applied in other cases involving general statements of concern.[29] However, *Thrivent* leaves open the possibility that such a statement *could* be considered a medical inquiry if the employer already had knowledge that the employee had a medical condition (for example, by knowing that the employee is in the hospital).[30]

B. Improper Disclosures

Once ADA's confidentiality protections for health information are established, the next question becomes whether the employer disclosed the information or otherwise failed to keep it confidential (or whether there is any exception that justifies disclosure). Clear cut examples where courts have found that the employer violated the ADA's confidentiality provision include an employer who shared the results of an employee's medical exam with a colleague who had no supervisory authority over the employee,[31] an employer who impermissibly commingled or merged employees' medical records with personnel files upon termination,[32] an employer who left a doctor's letter concerning plaintiff's reasonable accommodation request uncovered on a desk where other employees could see it,[33] and an employer who leaked an employee's drug screen results to the news media.[34]

May an ADA confidentiality violation be inferred based on the former employee's inability to obtain a new job?

In *Loschen v. Trinity United*, the employee presented evidence that after leaving her employer, Trinity, she applied for jobs at ten employers, all of whom failed to hire her.[35] She testified that by her second or third interview, the prospective employers seemed to know of her situation with Trinity and that she had a medical issue. Based on this evidence, the Court found in favor of the plaintiff, holding that there was a question of material fact about whether Trinity disclosed confidential medical information to the prospective employers. The Court's holding, however, may have been influenced by the employer Trinity's failure to maintain the former employee plaintiff's medical information as confidential, since they notated details about her condition on a logbook viewable by other employees.[36]

---

[28] *E.E.O.C. v. Thrivent Financial for Lutherans*, 700 F.3d 1044 (7th Cir. 2012).
[29] *See*, e.g., *Perez v. Denver Fire Department*, 243 F.Supp.3d 1186 (D. Colo. 2017).
[30] *See*, e.g., Fleming v. State Univ. of New York, 502 F.Supp.2d 324 (E.D.N.Y. 2007) (emphasis added).
[31] *See*, e.g., *Henderson v. Borough of Baldwin*, 2016 WL 5106945 (W.D. Pa. Sept. 20, 2016). See also, *Gascard v. Franklin Pierce University*, 2015 WL 1097485 (D. N.H. Mar. 11, 2015).
[32] *Equal Employment Opportunity Commission v. Valley Life*, 2017 WL 227878 (D. Ariz. Jan. 19, 2017).
[33] *Cripe v. Mineta*, 2006 WL 1805728 (D.D.C. June 29, 2006).
[34] *Giaccio v. City of New York*, 502 F.Supp.2d 380 (S.D.N.Y. 2007).
[35] *Loschen v. Trinity United Methodist Church of Lincoln*, 2009 WL 2902956 (D. Neb. Sept. 9, 2009).
[36] *Id*.

Confidentiality of medical records under Titles II and III present fewer confidentiality issues for municipalities. Title II of the ADA, which applies to State and Local Governments, and Title III of the ADA, which applies to private businesses and other places of public accommodation, do not contain specific confidentiality provisions. This is likely because the covered entities under Titles II and III generally do not have the same right as employers to solicit health information. There is no need, for example, to bring a doctor's note before utilizing the service animal relief area in an airport, or to request descriptive captioning for a live-streamed city council meeting.

Genetic Information Nondiscrimination Act

Title II of the Genetic Information Nondiscrimination Act ("GINA") prohibits employers from gathering or relying upon genetic information to make employment decisions. Genetic Information includes the employee's genetic tests, tests of the employee's family members and family medical history information.[37] GINA covers employers with 15 or more employees, including state and local governments.[38] Further, Title II of the Act prohibits employers to request, require, or purchase genetic information of an applicant or employee, with six exceptions: inadvertent acquisitions of information, acquiring information as part of health service (including wellness programs) offered by the employer, family medical history may be acquired as part of the certification process for FMLA leave, acquired through commercially and publicly available documents absent of the employers intent to find the information, acquired through a genetic monitoring program that screens for toxic substances in the workplace (under specific circumstances, and acquisition of information by employers who engage in DNA testing for law enforcement purposes.[39] Additionally, an employer is prohibited from releasing genetic information about applicants, employees, or members of the entity.[40]

Electronic Communication Privacy Act and Stored Communications Act

In addition to the federal acts establishing privacy protections for employee health and genetic information, the Electronic Communication Privacy Act ("ECPA") protects wire, oral and electronic communications while those communications are being made, are in transit, and when they are stored on computers. Additionally, the ECPA applies to email, telephone conversations, and electronically- stored data. The statute bars wiretapping and electronic eavesdropping, possession of wiretapping or electronic eavesdropping equipment, and the use or disclosure of information unlawfully obtained through wiretapping or electronic eavesdropping.[41] Under this Act, public employers should use extreme caution in utilizing video recording of employees, taking care to not record in common privacy zones such as locker rooms or restrooms. Public employers are generally prohibited from operating audio surveillance or conducting ongoing recording of employees. However, employers may use telephone extensions to record ordinary business

[37] 29 C.F.R. § 1635.1.
[38] 29 C.F.R. § 1635.2(d).
[39] EEOC, *Genetic information discrimination US EEOC*, https://www.eeoc.gov/genetic-information-discrimination (last visited Jun 9, 2022).
[40] *Id*.
[41] 18 U.S.C.A. § 2511.

communication -- but should advise both employees and callers that calls made on monitored lines are recorded.

Title II of the ECPA, the Stored Communications Act ("SCA"), controls how governmental entities can access stored account information from private entities including: internet service providers, social media companies, hosted email services, and communications stored on a cloud device. The SCA provides criminal penalties for anyone who intentionally accesses *without authorization* a facility through which an electronic communication service is provided or intentionally exceeds an authorization to access that facility and thereby obtains, alters, *or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system.*[42] Internet service providers may provide contents of a communication to an individuals employed or authorized or whose facilities are used to forward such communication to its destination and to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure immediately of communications relating to the emergency.[43] Non-public social media posts do not fall within this production scheme, but are protected by the SCA, unless the posts are obtained through the original poster's contacts.[44]

What can an employer do to help avoid any issues under the ECPA and SCA?

The SCA authorizes disclosure with the consent of the user, customer, or subscriber. If practicable, obtain *user consent* before requesting data. But note, an employer may not be able to consent to the release of its employees' data. One way of obtaining consent is through the onboarding process and hiring paperwork of new employees. Second, employers can request data (e.g., social media information) directly from an authorized user, rather than the internet provider. Lastly, the employer can request non-content information. This may assist the employer in identifying other parties to the communications at issue who may be willing to consent to its release.

Texas Medical Records Privacy Act

The Texas Medical Records Privacy Act ("TMRPA") expands on HIPAA's definition of "covered entities", instead covering any person who engages in the practice of assembling, collecting, analyzing, using, evaluating, storing, or transmitting PHI.[45] TMRPA embraces HIPAA's standards relating to uses and disclosures, including requirements relating to consent, unless it falls under a few exceptions. The standards are not adopted for financial institutions for processing of payment transactions, non-profit agencies, worker's compensation insurance, employee benefit plans, and offenders with mental impairments.[46] Notably, the Texas Medical Records Privacy Act is more limiting of marketing to employees or utilizing PHI for marketing purposes than HIPAA. The Act prohibits the release of PHI for marketing purposes without consent or authorization from the individual.[47] Additionally, an individual *may not be re-identified* from de-identified health information without obtaining the individual's consent. For example, screening records from a

[42] 18 U.S.C.A. § 2522 (emphasis added).
[43] 18 U.S.C.A. § 2518.
[44] *Ehling v. Monmouth-Ocean Hospital Service Corp.*, No. 2:11-cv-03305 (WJM) (D.N.J. Aug 20, 2013).
[45] Tex. Health & Safety Code Ann. §181.001(b)(2)(A)-(D).
[46] Tex. Health & Safety Code Ann. §181.052-181.057.
[47] Tex. Health & Safety Code Ann. §181.152(a),(b),&(c).

wellness program or assembled records of COVID-19 compiled for reporting requirements may not be used to re-identify employees. TMRPA follows both HIPAA regulations, applying to workplace wellness programs executed by employers. Further, the Act has an embedded training requirement for individuals charged with handling PHI, which must be completed within 90 days of the individual's state date.

Health and Safety Code

Texas' Health and Safety Code allows the release of information regarding cases or suspected cases of diseases of health conditions "to the extent necessary during a public health disaster, including an outbreak of a communicable disease, to law enforcement personnel and first responders solely for the purpose of protecting the health or life of a first responder or the person identified in the report, record, or information."[48] Section 81.46 only allows the released of the minimum necessary information, to be determined by the health authority, local health department, or the department handling the situation.[49] Additionally, information supplied to the commissioner or the commissioner's designee of the Texas Commission on Environmental Quality that relates to an epidemiologic or toxicologic investigation of human illnesses or conditions and of environmental exposures that are harmful or believed to be harmful to the public health are not public information under Chapter 552, Government Code, and are subject to the same confidentiality requirements as described by Section 81.046.[50] Further, for a covered entity that is a governmental unit, an individual's protected health information includes any information that reflects the individual received health care from the covered entity; and is not public information and is not subject to disclosure under Chapter 552, Government Code.[51]

Texas Public Information Act

Medical information is generally not considered public information under the Texas Public Information Act. Under Section 552.002(d), public information excludes protected health information as defined by Section 181.006 of the Health and Safety Code. The Public Information Act does follow the doctrine of Common Law Privacy.[52] The Act excepts from public disclosure "information considered to be confidential by … judicial decision."[53] This section encompasses the doctrine of common-law privacy, protecting information if it (1) contains highly intimate or embarrassing facts, the publication of which would be highly objectionable to a reasonable person, and (2) is not of legitimate concern to the public.[54]. To establish whether common-law privacy is applicable, both prongs of this test must be met.[55] The type of information considered highly intimate or embarrassing by the Texas Supreme Court in *Industrial Foundation* included information relating to sexual assault, pregnancy, mental or physical abuse in the workplace, illegitimate children, psychiatric treatment of mental disorders, attempted suicide, and injuries to sexual organs. The Office of the Attorney General has previously ruled that any information

[48] Tex. Health & Safety Code Ann. § 81.046.
[49] Id.
[50] Tex. Health & Safety Code Ann. § 161.0213.
[51] Tex. Health & Safety Code Ann. § 181.006.
[52] Gov't Code §552.101.
[53] *Id*.
[54] *Indus. Found. v. Tex. Indus. Accident Bd.*, 540 S.W.2d 668, 685 (Tex. 1976).
[55] *Id*. at 681-82.

acquired or created during an investigation under Chapter 81 of the Health and Safety is confidential and may not be released unless an exception in the statute applies.[56] The Attorney General has also previously ruled information that collected under the ADA from an applicant or employee concerning that individual's medical condition and medical history is confidential under section 552.101, in conjunction with the ADA.[57]

Other Law

The additional statutes below also contain privacy limitations that may impact an employer's management of COVID-19 related data and the privacy of their employees.

A. Texas Data Breach Notification Law

Texas Data Breach Notification Law ("TDBNL"), also known as the Identity Theft Enforcement and Protection Act, requires the Texas Attorney General's office to provide a public listing of data breaches. Further, it requires businesses that experience a breach of security to notify affected consumers and the Office of the Attorney General.[58] Under the Texas law, businesses must implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect sensitive personal information from unlawful use or disclosure. This Texas data breach notification law component is Texas' equivalent of a HIPAA Security Rule standard. TDBNL protects "sensitive personal information," which includes information related to the physical or mental health or condition of the individual, the provision of health care to the individual and payment for the provision of health care.[59] An entity must disclose any breach of system security within 60 days of determining a breach if this information has occurred.[60] Entities required to provide notification of a data breach of at least 250 Texas residents must also notify the Texas Attorney General with specific details about the breach, including how many people were affected and what measures the entity has taken regarding the breach. [61]

B. Fair Credit Reporting Act

The Fair Credit Reporting Act ("FCRA") prohibits the unauthorized release of "medical information" in a consumer report. FCRA requires consumer reporting agencies to adopt reasonable procedures to accommodate "the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization" of the information.[62] The FCRA enables employers to use consumer reports for employment purposes, except when a third party is used for internal investigations.[63] Medical-related information excluded from consumer reports include: medical information, an individualized list or description based on payment transactions for medical products or services, or an aggregate list of identified consumers based

[56] Open Records Decision No. 577 (1990).
[57] Open Records Decision No. 641 (1996).
[58] Attorney General of Texas, *Data Breach Reporting* | Office of the Attorney General (2021), https://www.texasattorneygeneral.gov/consumer-protection/data-breach-reporting (last visited Jun 9, 2022).
[59] Tex. Bus. & Com. Code Ann. § 521.002(2).
[60] Tex. Bus. & Com. Code Ann. § 521.053.
[61] *Id*.
[62] 15 U.S.C.A. § 1681.
[63] 15 U.S.C.A. § 1681a(d)(1)(B).

on payment transactions for medical products or services.[64] The FCRA requires employers to disclose the use of consumer reports when making employment assessments and obtain consent of the individual who is the subject of the report.

Conclusion

Employers, public health, and governmental officials continue to find a balance between privacy rights and employee health, shown through the COVID-19 pandemic. Employees' "return to work" has both magnified and accelerated the need for updated legislation and employee accommodations. In the context of the pandemic, uncertainty exists whenever the employer seeks to balance employee privacy and wellbeing against business operations. With varying standards on internal, local, state, and federal levels, employers must act and adapt to ensure employee wellbeing – including their rights to privacy.

[64] 15 U.S.C.A. § 1681a(d)(3)(A)-(C).