Bender's Labor & Employment Bulletin

November 2021
VOLUME 21 • ISSUE NO. 11

Inside This Issue

LexisNexis®
Matthew Bender®

The Employers Guide to Privacy and Requiring Proof of Employee Vaccination

By Karen Mandelbaum, RyAnn M. Hooper, and Susan Gross Sholinsky

The return to work race is well underway. While many employees grapple with their level of tolerance for a hybrid or full in-person workplace model, employers are seeking ways to entice employees back to the workplace safely. Some employers are electing a vaccination-only workforce, whether required by government mandates or not. Others are endeavoring to manage a mixed workforce of vaccinated and unvaccinated workers.

As noted above, one of the most common questions U.S. employers are pondering at the present time (beyond physical solutions for reducing the spread of COVID-19) is whether an employer can, should, or must implement a mandatory vaccine policy for returning employees. For the most part, mandatory vaccine policies are permissible and, many would argue, necessary to reduce the spread of COVID-19 in the workplace; however, implementation of a mandatory vaccine policy creates a myriad of considerations, including those around privacy and data security.

For example, once you ask an employee about their vaccination status, should (or must) the company then request proof of vaccination? Should the company request the same information from visitors, such as clients, customers, and vendors? If an employer collects vaccination records, what does the company do with the data collected? How does the company store the data? What safeguards does the company need to have in place to protect the data? Can the company share this data to make customers, visitors, and potential recruits to the business more comfortable about the safety of its work environment?

This article will explore the privacy concerns created when implementing a mandatory vaccine policy and collecting vaccination status information from employees and others.

A. Employment Law Considerations for Mandatory Vaccine Policies

1. EEOC Guidance and the Americans with Disabilities Act

Under the Americans with Disabilities Act, as amended by the Americans with Disabilities Amendments Act ("ADA"), covered employers may not make disability-related inquiries or require employees to get a medical examination unless the inquiry or examination is "job-related and consistent with business

 continued on page 287

CONTENTS:

ATTENTION READERS

Any reader interested in sharing information of interest to the labor and employment bar, including notices of upcoming seminars or newsworthy events, should direct this information to:

Laurie E. Leader
Law Offices of Laurie E. Leader, LLC
14047 W Petronella Dr., Suite 202B
Libertyville, IL 60048
E-mail: lleader51@gmail.com
or
Mary Anne Lenihan
Legal Editor
Bender's Labor & Employment Bulletin
LexisNexis Matthew Bender
230 Park Avenue, 7th Floor
New York, NY 10169
E-mail: maryanne.lenihan@lexisnexis.com

If you are interested in writing for the BULLETIN, please contact Laurie E. Leader via e-mail at lleader51@gmail.com or Mary Anne Lenihan via e-mail at maryanne.lenihan@lexisnexis.com.

A NOTE ON CITATION

The correct citation form for this publication is:
21 Bender's Lab. & Empl. Bull. 285 (November 2021)

ISBN 978-0-8205-5039-8, EBOOK ISBN 978-1-4224-8015-1

(Pub. 1239)

The Employers Guide to Privacy and Requiring Proof of Employee Vaccination
By Karen Mandelbaum, RyAnn M. Hooper, and Susan Gross Sholinsky

(text continued from page 285)

necessity."[1] On March 17, 2020, the Equal Employment Opportunity Commission ("EEOC") released "What you Should Know About COVID-19 and the ADA, the Rehabilitation Act and Other EEO Laws." (Last updated October 13, 2021).[2] This guidance addresses several topics, including return to the workplace and vaccinations, stating that federal EEO laws do not prevent an employer from requiring that all employees that physically enter the workplace be vaccinated against COVID-19.[3] The ADA, however, restricts when and how much medical information an employer may obtain from employees. Further, the guidance makes clear that simply requesting proof of vaccination from an employee is not a disability-related inquiry under the ADA.[4] Consequently, absent any state or local law providing otherwise, an employer may permissibly request or require production of documentation that validate employees' vaccination status.

As for non-employees who seek to enter an employer's premises, several legal obligations and restrictions could be implicated. First, with respect to individuals such as vendors, contractors, and consultants, certain of the employment-related protections discussed below may be applicable to such individuals, depending on the state or city in question. Further, some states have passed bans on businesses from requiring proof of vaccination (e.g., vaccine passport bans) which preclude businesses from denying access or services to customers who are not vaccinated. So, depending on the nature of an employer's business, while requesting proof of vaccination, in and of itself, may not violate employee privacy or disability-related laws, employers may be limited in their ability to maintain a vaccinated-only workplace or to take action based on the individual's vaccine status.

2. Privacy, Employee Overshare, and Asking One Question too Many

Any inquiry beyond a request for production of documents verifying vaccination status may run afoul of the ADA's rules about disability-related inquiries, turning a lawful request for proof of vaccination into a disability-related inquiry, which could, depending on when it is asked, be unlawful. For example, an inquiry into why an employee has not received a COVID-19 vaccine may elicit information about the employee's health or medical condition, and cannot be asked pre-offer of employment.

Likewise, employers may wish to limit the type of employee-provided documentation they will accept as proof of vaccination status. Documentation that the employer plans to rely on, keep, and potentially use, ideally should not contain any additional information that speaks to the employee's health or medical condition(s). Consequently, as we begin to consider the data privacy issues at play, the manner and form in which a company solicits this data becomes a central focus.

B. Considerations for Receipt and Storage of Proof of Vaccination Status

A company should be mindful of the type of information and the source from which it requests an employee provide documentation in support of their vaccination status. For example, requesting a copy of an employee's vaccination card may trigger a heightened data privacy and document retention requirement as a health related employment record. However, requesting lab results from a medical provider may trigger the requirement for a valid HIPAA authorization. In its guidance on vaccination, the EEOC takes the position that although a request for vaccination status is not a medical examination or disability-related inquiry under the ADA, any documents reflecting employee vaccination status are considered confidential medical records, and should be maintained separately from personnel records pursuant to the ADA.[5]

1. Method of Vaccine Record Collection

An employer may collect paper copies of vaccination records and store medical information related to COVID-19 in existing medical files (separate from the personnel file). Where an employer requests or receives a copy of a vaccination record via electronic mail (e-mail),

---

[1] ADA, Rehabilitation Act, 29 CFR Part 1630, 29 CFR Part 1614.

[2] *See* EEOC (last updated 13 October 2021) What You Should Know About COVID-19 and the ADA, the Rehabilitation Act, and Other EEO Laws. Accessed October 14, 2021 at https://www.eeoc.gov/wysk/what-you-should-know-about-covid-19-and-ada-rehabilitation-act-and-other-eeo-laws.

[3] *Id. See also* ADA, Rehabilitation Act, 29 CFR Part 1630, 29 CFR Part 1614.

[4] *Id.*

[5] *See* EEOC (last updated 13 October 2021) What You Should Know About COVID-19 and the ADA, the Rehabilitation Act, and Other EEO Laws. Accessed October 14, 2021 at https://www.eeoc.gov/wysk/what-you-should-know-about-covid-19-and-ada-rehabilitation-act-and-other-eeo-laws.

other considerations come into play, such as the security of the company's email server and the risk of a potential data breach. Beyond this, questions regarding who will have access to the email records, where the email records will be stored (as well as any supporting metadata), if the email records will be printed and converted to a paper file, and the company's data retention policy will also come into play. For example, a California employer is required to maintain medical records separately from the employee personnel file. Under Cal/OSHA Emergency Temporary Standards (ETS), an employer is not compelled to use any specific method of documenting their employees' vaccination status.[6] However, the method used should ensure that the information is kept confidential. Some acceptable options include, requesting employees provide a copy of their vaccine card, an image of their vaccine card or health care document showing vaccination status and a copy is maintained by the employer. An alternative is for an employee to sign an attestation or the employer maintains a record of which employees self-attested. With respect to how long vaccination records must be maintained, there is some ambiguity under the Cal/OSHA ETS as to whether vaccine record collection triggers the length of employment plus thirty (30) year retention period placed upon employers for employee medical records or if the records can be maintained for a shorter period of time.[7] Whether California employers under the Cal/OSHA ETS have to maintain vaccination records for thirty (30) years after termination of employment or for some shorter length of time, an employer should not use their e-mail system as their method for storing vaccination records, given the vulnerabilities to phishing attacks and other mistakes that are made sending, receiving and deleting e-mails.

If electronic storage is used, files should be secure and separate, with limited access available and need-to-know principles in place. Consideration must be given to whether the company will rely on physical data centers for data storage or a cloud platform, and in which jurisdiction(s) the information may be transferred or stored. In both scenarios, location of the data center or the cloud, involvement of third-party companies to service said storage method, and whether that third party is a controller or processor of data will dictate what notice of data processing or use, disclosure of data breach, waiver, and/or employee consent the company must obtain. It may further dictate specific language addressing duty of care obligation within the respective vendor agreements for employee sensitive data. Finally, an inquiry into whether there are country, federal, state, or other local laws applicable which may impose a stricter data privacy structure must also occur.

2. Applicability of HIPAA to Employer Vaccine Record Collection

Generally, the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule does not regulate what information an employer can be requested from employees and does not apply to employers or employment records. HIPAA only applies to entities which qualify as HIPAA covered entities – health care providers, health plans, and health care clearinghouses.[8] Even if an employer is a "covered entity," HIPAA still does not apply to health information contained "in employment records held by a covered entity in its role as an employer." While HIPAA may apply to health information employers acquire in their capacities as covered entities, it does not apply to health information they acquire in their roles as employers.[9]

Privacy law principles still come into play, because even though HIPAA does not apply to health related employment records, employers still have other legal obligations to protect the confidentiality of employee health information in their possession.

The HIPAA Privacy Rule does come into play if an employer requests that employees provide proof of vaccination through the disclosure of medical records from their health care providers. The Privacy Rule requires covered entities responding to a request to disclose an individual's protected health information (*e.g.*, information about

---

[6] *See* California Department of Industrial Relations "COVID-19 Emergency Temporary Standards Frequently Asked Questions" (last updated 17 June 2021), accessed October 14, 2021 at https://www.dir.ca.gov/dosh/coronavirus/COVID19FAQs.html#vaccines.

[7] *See* California Department of Industrial Relations "COVID-19 Emergency Temporary Standards Frequently Asked Questions" (last updated 17 June 2021), accessed October 14, 2021 at https://www.dir.ca.gov/dosh/coronavirus/COVID19FAQs.html#vaccines. ("Stating vaccination records created by the employer under the emergency standards need to be maintained for the length of time necessary to establish compliance with the regulation, including during any Cal/OSHA investigation or appeal of a citation. In order to encourage documentation using vaccination records, Cal/OSHA has determined that it would not effectuate the purposes of the Labor Code to subject such records to the thirty (30) year record retention requirements that apply to some medical records"); *see also* 8 CCR 3204(c)(5)(D).

[8] *See* 45 CFR 160; *see also* HHS.Gov "HIPAA Covered Entities and Business Associates" (last updated 16 June 2017), accessed October 14, 2021 at https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html.

[9] *Id*.

whether the individual has received a vaccine, such as a COVID-19 vaccine; the individual's medical history or demographic information) to a third party to obtain authorization from the individual prior to making the disclosure.

3. Reliance on International SMART Health Card and Locality Verifier Applications

As an alternative to storage of electronic or paper files, an employer can verify an employee's vaccination status by asking to see a vaccination digital passport. While universal technology has yet to be adopted, the SMART Health Card framework developed by the Vaccine Credential Initiative ("VCI") is already in use by several states, universities and corporations.[10] The VCI framework boasts that it is based on international standards and open technologies which are interoperable across countries and regions; transparency; privacy which protects the health data of an individual; and a design compatible with stringent privacy regulations.[11] Notably, the technology can present a QR code which can be displayed digitally on a smart phone or can be downloaded and printed in paper form (no smart phone required). When the employee pulls the QR code up, only the individual's name, date of birth and vaccination information is shared. This code is also digitally signed to ensure that the card was issued from a verified location to prevent forgery. Employees can also use their SMART Health Card credential to obtain access to other venues, since it has been integrated into other apps, like the Excelsior App, the LA Wallet and VaccineCheck, to name a few. Consequently, an employer could scan the QR code, verify an employee's vaccination status and avoid the storage, privacy and potential liability issues for maintaining employee vaccination data.

Relying on the VCI technology, Apple recently announced that it is adding verifiable COVID-19 vaccination cards to Wallet as part of a future iPhone software update.[12] The feature will take advantage of the VCI international SMART Health Cards standard to produce proof of vaccination, sign it with a private key and create a public key to verify individual information. The portability of the SMART Health technology for safe return to work is promising. However, in certain jurisdictions, where requiring verification and the technologies to track vaccination status have been banned, an employer would not be permitted to share the list of vaccinated employees that are working onsite with the state or local public health authorities as evidence that the worksite is in compliance with local law.

4. Collecting and Maintaining Vaccination Information from Contractors, Consultants, Vendors and Customers/ Patrons

On September 9, 2021, President Biden issued Executive Order No. 14042, *Ensuring Adequate COVID Safety Protocols for Federal Contractors*, raising awareness to the subject and complexity of the role that contractors play in keeping workplaces and employees safe from exposure to COVID-19.[13] The Executive Order directed executive departments and federal agencies to require federal contractors to implement COVID-19 safety protocols, including mandatory vaccination policies through clauses in FAR contracts and contract-like instruments. Under the Executive Order and guidance published by OMB[14], all covered contractors are required to review the documentation of covered contractor employees to prove vaccination status. Contractors can rely on immunization records of a hospital or pharmacy, COVID-19 Vaccination Record Cards, medical records documenting vaccination, immunization records from a public health or state immunization system, or other official documentation verifying vaccination containing information on the vaccine, date of administration, and the name of the health care professional/clinic site administering the vaccine, as proof of vaccination. However, an attestation of vaccination or proof of prior COVID-19 infection and antibody testing, do not qualify as sufficient proof. Vaccination status can be verified electronically, digitally or with a scanned copy. While contractors are required to verify proof of vaccination, there is no requirement for contractors to maintain such proof of vaccination.

As noted above, businesses are within their rights to require that anyone wishing to enter their premises provide

---

[10] Frieden, Tom, "I Ran the CDC Here's How to Prove that Americans are Vaccinated" 21 September 2021, accessed September 14, 2021 at https://www.nytimes.com/2021/09/21/opinion/cdc-coronavirus-vaccine.html

[11] The VCI Charter, last visited 14, September 2021, accessed at https://vci.org/about.

[12] Fingas, John, "Apple Wallet is Getting Verifiable COVID-19 Vaccination Cards" 21 September 2021. Accessed October 14, 2021 at https://techcrunch.com/2021/09/21/apple-wallet-is-getting-verifiable-covid-19-vaccination-cards/.

[13] Executive Order on Ensuring Adequate COVID Safety Protocols for Federal Contractors Accessed, issued September 9, 2021. Accessed on October 17, 2021 at: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/09/09/executive-order-on-ensuring-adequate-covid-safety-protocols-for-federal-contractors/.

[14] New Guidance on COVID-19 Workplace Safety for Federal Contractors, published on September 24, 2021. Accessed on October 17, 2021 at: https://www.whitehouse.gov/omb/briefing-room/2021/09/24/new-guidance-on-covid-19-workplace-safety-for-federal-contractors/.

proof of vaccination. That includes employees, contractors, consultants, vendors or customers/patrons. If a business decides to impose such a restriction on their contractors, consultants or vendors, the parties may need to review and renegotiate their contracts to include that only workforce members of a contractor, consultant or vendor who have been vaccinated are allowed to work on-site. Absent an express term in an agreement to the contrary, the respective employers would likely be responsible party to collect and maintain the vaccination records. With respect to customers or patrons, businesses may require proof of vaccination upon entry and turn away anyone who has not been vaccinated. The CDC still recommends that vaccinated individual should take precautions (e.g., testing and masking indoors) if they have had close contact with someone who tests positive for COVID-19. Therefore, depending on the venue and any state or local requirements, a business that is collecting proof of vaccination may want to consider whether to retain proof of vaccination beyond the date of collection in case they become aware of any break-through cases of COVID-19.[15]

C. Maintaining Confidentiality of Vaccination Information, State Specific Considerations, and Future Data Use

1. Maintaining Confidentiality

Paper or electronic documentation concerning an employee's vaccination status provided by an employee will constitute confidential medical information under both the ADA and the state specific regulations such as the California Confidentiality of Medical Information Act ("CMIA"). As previously mentioned, employers are still subject to the confidentiality requirements of both the ADA and the CMIA even if they are not considered covered entities within the meaning of the HIPAA. Both statutes impose strict statutory obligations related to the protection and preservation of confidential medical information.

Under the ADA, employers must keep confidential medical information in a file that is separate and distinct from the employee's personnel records. When collecting a new kind of sensitive health information, best practice is for a business to conduct a review of its privacy and retention policies regarding storage and use of such medical information to ensure compliance with those existing policies. Use of security measures such as password protection, encryption, limiting access to the separately stored file to those employees or third parties who need to have access to the information are a starting point for protecting this sensitive employee health data.

2. California's Heightened Data Privacy Requirements: CCPA, CPRA, CMIA

The CMIA is more stringent than HIPAA in imposing more rigorous confidentiality obligations, requiring that employers "establish appropriate procedures to ensure the confidentiality and protection from unauthorized use and disclosure of [employees' confidential medical] information." These procedures may include instructions to handlers of the confidential medical information and implementation of security safeguards. Furthermore, upon receipt of a vaccination health record, the employer cannot further disclose that employee health information to another third party (e.g., a public health authority) unless the employer receives written authorization from the employee to further disclose that information.[16]

As a general rule, employers who operate in California may collect certain health information from job applicants and employees. That said, in order to fully analyze whether or not an employer must take an additional step to obtain employee consent, a review of the Notice that employees receive under the California Consumer Protection Act (CCPA) during onboarding is required. The Notice described in the CCPA and its regulations[17], requires employers to provide applicants and employees that are residents of California with a Notice, at the time that any data collection takes place, that includes:

- A list of the categories of personal information that will be collected. Examples of the categories

---

[15] *See* Centers for Disease Control (CDC) COVID-19 Vaccine guidance, *When You've Been Fully Vaccinated How to Protect Yourself and Others*, Updated October 15, 2021. Accessed on October 17, 2021 at: https://www.cdc.gov/coronavirus/2019-ncov/vaccines/fully-vaccinated.html.

[16] The CMIA sets forth certain requirements in order for an employee authorization to be considered valid. Pursuant to the CMIA, the authorization must satisfy each of the following requirements: be handwritten by the employee, or else typed in at least 14-point font; is clearly separate from any other language on the page and must be executed by a signature that serves only to execute the authorization; signed and dated by the employee; state the limitations, if any, on the types of medical information to be disclosed; state the names or functions of both the person(s) authorized to make disclosures and the persons or entities authorized to receive disclosures of the medical information; state a specific date after which the employer may no longer disclose the medical information; state the limitations, if any, on the use of the information; and advise the employee that he or she may receive a copy of the authorization.

[17] *See* 11 Calif. Code of Regulations § 999.305(b).

of information that an employer maintains about employees may include:

- New applicant/Onboarding information (e.g., resumes, employee applications, background checks, IRS Forms W-4 (withholding), etc.) collected;
- Payroll/Financial information (may include employee bank account numbers for direct deposit) collected;
- Health/Health related information: vaccination records, drug test results, documents requesting sick leave, FMLA leave, maternity/paternity leave collected;
- Online activity on employer furnished equipment (browsing history, search history, and information regarding the employee's interaction with an Internet Web site or application);
- The business reason for which the information is being collected;
- Information on how to opt out of the sale of personal information (if information is being sold); and
- Information on how to find the company's complete privacy notice.

After January 1, 2023, the California Privacy Rights Act (CPRA) will expand the information required in a Notice of collection to include:

- Whether that information is "sold or shared"; and
- The "length of time" that the business intends to retain each category of personal information.

Unless the employer expects to disclose the vaccination records, a clear Notice, provided to employees, with the elements enumerated above should be sufficient to collect and retain vaccination records. If the Notice includes information about the potential for the employer to further disclose the vaccination records to third parties (e.g., local, state or federal public health authorities), the Notice should be affirmed either with a wet signature or electronically in a manner that complies with the California Uniform Electronic Transactions Act (UETA)[18] and the Electronic Signatures in Global and National Commerce Act (E-SIGN).[19] There was some ambiguity as to whether the California UETA applied to medical records. However, that ambiguity was resolved when the California Health and Safety Code related to Medical Records was recently amended to authorize a health care provider to honor a request to disclose a patient record.[20]

3. Other State Privacy Considerations

Several states have recently enacted data security and privacy laws that impose notice and records retention requirements as methods to protect the vaccination records that employers are maintaining. Two states highlight the slight variance in state law which can make an employer's approaches nuanced – particularly where a company operates and has employees in multiple locations.

Connecticut

Connecticut's data privacy law tracks closely with the requirements imposed by HIPAA. However, with respect to an employer's responsibility to maintain employee medical, Connecticut General Statutes require employers to maintain any medical records for at least three years following the termination of employment and that the medical records must be kept in a separate file that is not part of any personnel file.[21] In contrast to the CMIA, Connecticut law allows personal health information to be disclosed without a patient's consent to certain state agencies and other entities in certain circumstances.[22]

Oregon

Under Oregon's Protected Health Information law[23], patients have the right to expect that their medical records will be safeguarded from unlawful disclosure. However, the law does not provide broader protections to employee health information like the CMIA. The Oregon Consumer Identity Theft Protection Act, however, provides protection for personally identifiable information and medical information in an employer's possession, requiring businesses in Oregon to implement and maintain certain security

[18] Uniform Electronic Transactions Act. (Added by Stats. 1999, Ch. 428, Sec. 1. Effective January 1, 2000). Accessed 14 October 2021 at https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=2.&lawCode=CIV&title=2.5.

[19] Public law 106-229 June 30, 2000.

[20] The amendment became effective January 1, 2021. See California Department of Public Health, "Vaccine Records Guidelines and Standards" (last updated August 25, 2021). Accessed October 14, 2021 at https://www.cdph.ca.gov/Programs/CID/DCDC/Pages/COVID-19/Vaccine-Record-Guidelines-Standards.aspx.

[21] Conn. Gen. Stats., Ch. 563, § 31-128a (2019).

[22] https://www.cga.ct.gov/2016/rpt/2016-R-0050.htm.

[23] *See* Protected Health Information, Oregon Revised Statutes §§ 192.553 through 192.581, https://oregon.public.law/statutes/ors_chapter_192, (scroll to Protected Health Information). Cite last access on October 17, 2021.

safeguards to protect personal information and to report data breaches of personal information.[24]

Virginia, Colorado, and Oklahoma are all states that also recently enacted data privacy laws; however, unlike the CCPA, each of these laws carved out employees and employment records from their reach. The Virginia Consumer Data Privacy Act (VCDPA) is similar to the CCPA, in that HIPAA covered entities and their business associates are exempt from the new Virginia law. However, the VCDPA excludes employment information from the definition of "consumer information" and even though the definition of "consumer" includes Virginia residents, it expressly excludes "any person acting in a commercial or employment context." The Colorado Privacy Act (CPA) also does not grant the new law's data privacy rights to all Colorado residents; the CPA expressly exempts individuals acting in the commercial or employment context, including job applicants. Finally, similar to Virginia, the Oklahoma Computer Data Privacy Act defines "consumer" as Oklahoma residents, but does not include an employee or contractor of a business acting in their role as an employee or contractor.

Consequently, employers should be nimble and prepared to revise their policies to reflect the changing data privacy landscape. Notably, there are currently over twenty (20) states that maintain data breach notification laws, requiring that employers stay on top of changes to the privacy law and report when there has been an unauthorized disclosure of personal medication information.[25]

D. Conclusion

The regulatory landscape regarding COVID-19, return to work, and the collection of vaccination records is evolving. As more employers adopt mandatory vaccine policies, and technology becomes available for the universal management of vaccine data, employers must become familiar with the changing regulatory obligations related to the privacy and use of vaccination records. Insuring that companies implement policies that are sufficiently transparent; provide proper notice regarding how vaccination information will be used, with whom it will be shared, and for how long it will be maintained; and that security safeguards are in place to protect any sensitive information, will serve as the framework for navigating compliant collection and maintenance of such data as employees return to the in-person work environment.

Karen Mandelbaum is Senior Counsel at Epstein Green Becker. RyAnn M. Cooper is an Associate at Epstein Becker Green. Susan Gross Sholinsky is a Member of Epstein Becker Green.

[24] Oregon Identity Theft Protection Act – Oregon Revised Statute 646A.600 https://www.oregonlegislature.gov/bills_laws/ors/ors646A.html (Scroll to Identity Theft Prevention). Oregon Administrative Rule – Identity Theft http://arcweb.sos.state.or.us/pages/rules/oars_400/oar_441/441_646.html (Scroll to Identity Theft OAR Chapter 441, Div. 646, Section 0010 through 0040.). Cites last accessed on October 17, 2021.

[25] The U.S. Senate Committee on Commerce, Science and Transportation recently launch privacy hearings aimed at enhancing the enforcement authority for the FTC and enacting comprehensive federal privacy legislation with strong consumer rights. A national privacy law or agency rulemaking at the FTC aimed at protecting consumer data (like confidential medical/vaccine records) could go into effect at some point in the future.