

Firefighter Occupational Health and Safety Data Privacy: An Analysis of Statutory, Regulatory, and Contractual Governance Mechanisms

NEW SOLUTIONS: A Journal of
Environmental and Occupational
Health Policy
2026, Vol. 36(1) 36–50
© The Author(s) 2026
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/10482911261422422
journals.sagepub.com/home/new
Mary Ann Liebert
A Part of Sage

Rachel J. Topazian^{1,2} , Paul Locke³, Joseph Ali^{4,5},
Shannon Fattaroli²  and Cassandra K. Crifasi²

Abstract

Despite interest in collecting occupational health and safety data to protect high-risk workers such as firefighters, there is limited research on public policies governing this data. We reviewed policies impacting firefighter occupational health and safety data. We identified laws, regulations, and union contracts at the federal level, and in Maryland and Virginia. We collected data using secondary sources and Westlaw (March–May 2023). We reviewed 20 laws and regulations: nine federal, three in Maryland, and eight in Virginia, and 11 union contracts. We developed a framework for evaluating each policy: permissiveness of data collection, data use/purpose, storage conditions, and sharing/access privileges. We found few policies directly related to occupational health and safety data privacy, and only two fire service-specific laws. Union protections varied, with many limiting data access, while others authorized electronic surveillance. The current legal structure provides some protection, but additional policymaking is needed to further safeguard firefighter data.

Keywords

firefighters, data privacy, occupational health and safety, unions, public policy

Introduction

Firefighters provide essential public services. Despite experiencing high rates of injury and their important societal role, they remain an understudied worker population from an occupational safety and health perspective. In 2023, the National Fire Protection Association reported over 60,000 on-duty firefighter injuries and 89 on-duty fatalities.^{1,2} There are ongoing efforts to leverage firefighter health and safety data to understand and prevent injury and fatality. This includes individual research studies, national surveillance systems, and employer-led initiatives that could collect more and higher-quality firefighter occupational health and safety data.

Fire service researchers consistently highlight the need for more sophisticated data collection and analysis,^{3–6} and propose using new software platforms or wearable technology.^{7,8} Government agencies are leading efforts to strengthen national surveillance. In 2023, the National Institute for Occupational Safety and Health (NIOSH) launched the National Firefighter Registry for Cancer, the largest ever national system for tracking and studying cancer in the fire

service.⁹ In 2023, the U.S. Fire Administration announced that it will create a new data analytics platform that could improve tracking of firefighter injuries.¹⁰ In addition to these surveillance efforts, there are calls for studies examining specific health outcomes, such as cancer, reproductive health, and mental health.¹¹ Fire service leaders have

¹Center for Bioethics and Humanities, University of Colorado Anschutz Medical Campus School of Medicine, Aurora, CO, USA

²Department of Health Policy and Management, Johns Hopkins Bloomberg School of Public Health, Baltimore, MD, USA

³Department of Environmental Health and Engineering, Johns Hopkins Bloomberg School of Public Health, Baltimore, MD, USA

⁴Berman Institute of Bioethics, Johns Hopkins University, Baltimore, MD, USA

⁵Department of International Health, Johns Hopkins Bloomberg School of Public Health, Baltimore, MD, USA

Corresponding author:

Rachel J. Topazian, Center for Bioethics and Humanities, University of Colorado Anschutz Medical Campus School of Medicine, 13080 E. 19th Ave, Aurora, CO 80045-2581, USA.
Email: rachel.topazian@cuanschutz.edu

encouraged individual fire departments to collect and leverage data on exposures, injuries, and general health or fitness information to improve the health and safety of their personnel, via internal health and safety programs or through adopting wearable technology.^{12,13}

The introduction of these new data initiatives has been accompanied by concerns about firefighter data privacy.^{3,14} Firefighters may resist sharing personal information with government agencies, their employers, or researchers. In 2022, OSHA proposed publishing some deidentified electronically reported injury data online and received many comments discussing employee privacy concerns. While this regulation did not specifically address firefighters, it suggests that employees may have concerns about national injury surveillance.^{15,16} The National Firefighter Registry has put forth extensive guidance on its confidentiality protections to mitigate firefighter privacy and confidentiality concerns.¹⁷

Within fire departments, employers could use a wearable device to collect biometric data on firefighters responding to a fire, providing insights on exertion and temperature that could be used in real time and for post-incident analysis.³ However, firefighters might oppose sharing this kind of information with their employers based on concerns that it could be used to place them on light duty (which is viewed as punitive to many firefighters, as it often requires shift changes and removes firefighters from fire stations) or even result in termination. Other data collection might take place through individual research studies that collect identifiable information, biospecimens, or health information to examine a specific occupational exposure or health outcome of interest. While these studies might be conducted independently of a firefighter's employer, research participants' privacy concerns are well documented, and there is long running debate about the best strategies for protecting participant privacy.^{18–21}

Fire service researchers recognize these privacy concerns³ but there is relatively little research on data privacy in the fire service. Studies examining views towards wearable devices document divergent views between firefighters who feared that the use of wearables—and the data generated—would have adverse impacts on their work, autonomy, and privacy, and leadership who identified safety benefits.^{22,23} This is consistent with the broader literature on health and safety data in employment settings, which typically examines attitudes towards new technologies. Researchers have identified broad support for health and safety-oriented technology among employers, while employees express privacy concerns about how wearable data would be used and accessed.^{24,25}

Firefighters are an important occupational group with whom to examine occupational health and safety data privacy issues. They are an understudied worker population experiencing high rates of injury, illness, and fatality while providing critical services to the public. New data initiatives

have the potential to improve the health and safety of firefighters, but prompt serious privacy concerns. There are compelling health and safety arguments for why firefighters should consider sharing sensitive personal information with an employer, researcher, or government agency, but the best way to balance these imperatives with privacy protections is unclear.

Our study focuses on the policies governing career firefighter occupational health and safety data. The new data efforts described above are being introduced in an opaque policy environment. It is unclear how occupational health and safety data are currently regulated, and whether existing policies adequately protect against disclosure of personal health and safety data. Privacy scholars have criticized the lack of policies protecting workers from monitoring and surveillance and called for additional data privacy policies specifically addressing worker data.^{26,27} However, there is little to no research that comprehensively examines the policies dictating how occupational health and safety data are collected, used, stored, and shared. It is important to understand how these new firefighter health and safety data would be governed and to assess whether existing protections are sufficient.

Our study examined two key questions related to (1) how occupational health and safety data are currently regulated and (2) whether current policies sufficiently protect firefighter data. In this paper, we identify a subset of the current laws and regulations governing firefighter occupational health and safety data at the federal level and in Maryland and Virginia, as well as state and local union contracts in Maryland and Virginia fire departments. We include a range of data provisions with an emphasis on data policies with privacy implications. We use these findings to develop a framework for understanding the nature of data policies and assessing the policies in each jurisdiction. To our knowledge, this is the first study to assess the policy environment for this topic and population. Our findings offer an initial overview of the regulatory landscape for firefighter health and safety data and can be utilized to identify gaps and opportunities for future policymaking.

Methods

Because of our emphasis on workplace data, we defined firefighters as career (sometimes referred to as paid) firefighters. Of the approximately 1 million firefighters in the United States, one-third are career firefighters who are employed full-time by a fire department or district.²⁸ Two-thirds are volunteers. While career firefighters are smaller in number, they cover a disproportionate share of the U.S. population and are largely concentrated in urban and suburban locations. We chose to focus on career firefighters because of our interest in occupational health and safety data. While volunteer firefighters experience similar occupational hazards and are often eligible for similar benefits (e.g., workers'

compensation coverage for injuries), they are not employed by fire agencies. In addition, many career firefighters are unionized—the International Association of Fire Fighters membership includes over 350,000 firefighters and emergency medical service providers across the United States and Canada.²⁹ For unionized firefighters, negotiated contracts or collective bargaining agreements may include additional policies covering health and safety data.

We examined laws and regulations in three domains: labor, health and safety, or data (i.e., laws or regulations addressing the collection, storage, use, or sharing/access of employee or firefighter information). We chose to focus on policies enacted by legislatures or relevant regulatory bodies and to maintain a reasonable scope that would allow us to conduct in depth examination of these policies and union contracts. As a result, guidance documents that are not legally enforced and state case law were not included. We conducted a two-stage data collection process using the Westlaw legal database to identify laws and regulations. In the first stage, we queried secondary sources in Westlaw to identify law review articles that discussed relevant laws and regulations, using search terms related to data privacy, health and safety, and labor or employment.^{26,30,31} We also relied on the Westlaw Practical Law Employee Privacy Law resources for Maryland and Virginia.^{32,33}

In the second stage, we conducted targeted searches of laws and regulations. For each jurisdiction, we used standardized search strings that covered at least two of our three domains: labor, health and safety, or data (see Supplemental Appendix 1 for search terms). We conducted searches specific to firefighters and the fire service, as well as searches using general employment terms to capture other labor policies that would apply to firefighters. As we reviewed each law or regulation, we added policies that were referenced and met the inclusion criteria. We excluded proposed legislation and rulemaking, laws or regulations specific to non-fire service sectors, those related to surveillance of non-health or safety information (e.g., email), laws that did not address data, and narrowly scoped laws (e.g., those applying to voluntary protection programs). Regulations inherently flow from laws, and so in some cases, we included both a law and an associated regulation if both addressed our topic of interest. In other cases, if a statute did not specifically address data privacy but authorized a broad scope of rulemaking that ultimately led to regulations addressing data privacy topics, we included the regulation but not the law so that we could focus on policies relevant to occupational health and safety data privacy.

To aggregate union contracts, we first identified state and local fire departments reporting “career” or “mostly career” staffing to the U.S. Fire Administration’s National Fire Department Registry.³⁴ We included unionized departments that negotiate contracts with the state of Maryland or Virginia, or counties or cities within each state. We then searched for the most recent publicly available contracts (in

some cases, expired contracts which had not been renegotiated). In cases where we could not find the most recent contract online, we contacted union leaders and local officials. For one jurisdiction, Annapolis, Maryland, we were unable to obtain a recent contract and excluded it from our analysis. We will refer to “policies” when describing our collective findings.

After identifying relevant policies, we developed a data abstraction tool to examine features such as jurisdiction, covered entities, covered data, and data privacy factors (data collection, data use or purpose, data storage, and data sharing or access). This tool was created in an iterative fashion based on a preliminary review of the documents and existing data privacy frameworks.^{35,36} Within each data privacy factor, we generated subcategories capturing additional nuance on privacy-oriented provisions and other data management provisions. We reviewed each policy using the data abstraction tool and aggregated the findings across jurisdictions. Data collection took place between March 2023 and May 2023. This study was approved by the Johns Hopkins Bloomberg School of Public Health Institutional Review Board.

Results

Data Privacy Policy Framework

While there were variations in the nature of each policy, they typically related to one of four data-related considerations: collection, use or purpose, storage, and sharing or access. Differences within each of these categories reflect the varied design, strength, and breadth of policies across and within jurisdictions. Data collection provisions fell into four subcategories: restrictive, permissive, mandated, or presumed. Some policies limited the collection of medical, disability, or genetic information (restrictive), whereas others required the collection of injury or fatality data (mandated). In other cases, laws allowed for the collection of information under specific circumstances (permissive), or inherently presumed data collection occurred (presumed). Data use or purpose provisions described appropriate uses of data and reflected the intent of each policy: anti-discrimination, employment benefits, injury surveillance, or data privacy. Anti-discrimination laws prevented data from being used to distinguish prejudicially in employment. Benefits-related policies allowed data to be used to process benefits such as workers’ compensation or presumptive firefighter benefits, which are intended to ease access to benefits for work-related diseases such as cancer.³⁷ Injury surveillance policies were designed to track worker illness, injuries, or fatalities in a population, and data privacy policies were explicitly aimed at privacy considerations.

Data storage considerations addressed the location or retention of data. This might include storing medical, disability, or genetic information separately from personnel records,

or mandating that data be kept for a specific number of years. Data sharing and access provisions included those that are limiting, required, or encouraged. Some limited access to or sharing of disability, medical, injury, or fatality information, whereas others required reporting of injuries and fatalities to government agencies, and/or required that employees may access their own data. A small number of policies encouraged data sharing in aggregate form for educational or prevention purposes.

We used this framework to analyze the strength and breadth of policies we identified. Some policies addressed all four parent categories, whereas others addressed only a few. Subcategories are not mutually exclusive: a law might address both the location and duration of data storage, or limit sharing while maintaining individual employees' access to their own data.

Importantly, while the framework captures the breadth of data policies and can offer insights into the strength of data protections, there is nuance within and across categories. For example, a policy might offer strong protections against unauthorized individuals accessing firefighter data but not address the collection of these data. We seek to capture this nuance in describing the policies we identified and offer examples of how data might be governed by different policies.

Overview Across Jurisdictions

We identified 20 laws and regulations that impact the occupational health and safety data of career firefighters: nine at the federal level, three in Maryland, and eight in Virginia; we also identified nine union contracts in Maryland and two in Virginia. Across jurisdictions, there were three laws or regulations directly aimed at occupational health and safety data privacy, and only two laws directly related to the fire service. Federal laws and regulations more comprehensively addressed each data privacy factor than Maryland and Virginia laws and regulations (Table 1).

All nine of the federal policies addressed data collection, use or purpose, and storage, and eight addressed sharing and access. The two states have enacted policies that are more limited in scope. While all addressed data use or purpose, only one Maryland law highlighted data storage, and we did not identify Virginia laws or regulations within our scope of firefighter occupational health and safety data privacy that explicitly discussed data storage. However, while federal policies addressed a range of privacy factors, we did not identify any federal data privacy legislation, whereas the two states have both passed data privacy laws. We found only one federal regulation directly aimed at data privacy in occupational health and safety contexts, but it narrowly applied to OSHA employee access to medical data.³⁸ On the state level, Maryland had a law requiring secure storage of information, including health and biometric data³⁹; in 2023, Virginia passed a law authorizing broad

Table 1. Nature of Data Privacy Laws and Regulations by Jurisdiction.

	Federal	Maryland	Virginia
Overall	9	3	8
Collection	8	2	6
Restrictive	2	1	1
Permissive	1	0	1
Presumed	0	1	3
Mandated	5	0	1
Use/Purpose	9	3	8
Anti-discrimination	2	1	2
Injury surveillance	4	1	3
Benefits	3	0	4
Data privacy	1	1	1
Storage	9	1	0
Location	5	1	0
Duration	6	0	0
Access	8	1	5
Limited access, sharing	4	1	2
Required reporting, access	3	1	3
Encouraged sharing	1	0	0

Note: Some policies address more than one subcategory. "Restrictive" policies limit the collection of data. "Permissive" policies allow data collection. "Presumed" indicates that the policies do not explicitly address data collection, but presume it has or will take place. "Mandated" requires data collection.

future data privacy rulemaking.⁴⁰ Table 2 provides an overview of each data privacy policy provision.

At the union level, we identified more collective bargaining agreements in Maryland than in Virginia (Table 3). Union contracts varied in scope, with most addressing the collection of injury, exposure, or sick leave information for injury surveillance or benefits. Three Maryland contracts limited the sharing of and access to medical or injury information, and two required firefighters have access to their own information.^{41–44} In Virginia, Alexandria's contract required that employees report injury information and that the department share personal exposure reports with employees. In Arlington, the contract included a range of provisions limiting access to sick leave, medical, and injury information while requiring that employees have access to their own data. Both Virginia contracts authorized electronic monitoring for health and safety purposes without imposing storage or sharing limits.^{45,46} Table 4 details each contract's data privacy provisions. Supplemental Appendix 2 contains detailed summaries of all policies.

Overview by Jurisdiction

The bulk of federal laws and regulations we identified either established injury and fatality reporting requirements or prevented sensitive data from being used in a discriminatory fashion in employment. Five of the nine federal policies required reporting of injury or fatality data, including the

Table 2. Overview of Data Privacy Laws and Regulations.

	Data Collection Permissions	Data Use and Purpose	Data Storage Parameters	Data Access Provisions	Notes
Federal					
Americans with Disabilities Act, 42 U.S.C. § 12101 et seq.	Restrictive	Anti-discrimination	Location	Limited access, limited sharing	Bars discriminatory collection, use of disability information; storage location; limits sharing to key people
Genetic Information Nondiscrimination Act, 42 U.S.C. § 2000ff et seq.	Restrictive	Anti-discrimination	Location	Limited access, limited sharing	Bars discriminatory collection, use of genetic information; storage location; limits sharing to key people
Family and Medical Leave Act, 42 U.S.C. § 2601	Permissive	Benefits	Location, duration	Limited access, limited sharing	Allows employers to collect medical information for FMLA; storage length and location; limits sharing to key people
Federal Fire Prevention and Control Act of 1974, 15 U.S.C. § 2201 et seq.	Mandated	Injury surveillance	Location	Encouraged aggregate sharing	Requires creation of National Fire Data Center to collect fatality, injury data; encourages sharing in aggregate
Occupational Safety and Health Act of 1970, 29 U.S.C. § 651 et seq.	Mandated	Injury surveillance, benefits	Duration	Required reporting, required employee access	Authorizes DOL to collect fatality, injury, illness, exposure data; requires individual sharing with DOL, employees. Applies to MD, VA firefighters due to state OSHA plans
29 CFR § 1602 Recordkeeping regulation	Mandated	Benefits	Duration	N/A	Requires state, local employers to retain all personnel, employment records for at least two years; one year for unions
29 CFR § 1910.1020 Access to employee exposure and medical records	Mandated	Injury surveillance	Duration	Required reporting, employee access	Requires employers to maintain exposure, medical records; storage length; requires individual sharing with employee, OSHA. Applies to MD, VA firefighters due to state OSHA plans
29 CFR § 1904 OSHA Recordkeeping Rules	Mandated	Injury surveillance	Duration	Required reporting, aggregated sharing, employee access	Requires employers to maintain fatality, injury, illness records; storage length; requires aggregate sharing. Applies to MD, VA firefighters due to state OSHA plans
29 CFR § 1913.10 Rules of Agency Practice and Procedure Concerning OSHA Access to Employee Medical Records	N/A	Injury surveillance, data privacy	Location, duration	Limited access, sharing	Limits circumstances in which OSHA may access employee medical records, imposes privacy-oriented requirements

(continued)

Table 2. Continued.

	Data Collection Permissions	Data Use and Purpose	Data Storage Parameters	Data Access Provisions	Notes
Maryland					
Personal Information Protection Act, Md. Code Ann. Comm. Law § 14-3504	N/A	Data privacy	Location (security)	Limited access	Requires secure destruction; treatment of data as confidential; requires individual notification in case of data breach
Inquiries Regarding Medical History, Md. Code Ann. Lab. & Empl. 3-701	Restrictive	Anti-discrimination	N/A	N/A	Bars discriminatory collection of disability information
COMAR 09.12.21 Employee Injury and Illness Records and Reports	Presumed	Injury surveillance	N/A	Required reporting	Requires employers to report fatalities, injuries, illnesses; requires MOSH reporting
Virginia					
Va. Code Ann. § 8.01-413.1 Labor and Employment—Records and Recordation—Disclosure	Presumed	Injury surveillance, benefits	N/A	Required employee access	Requires employers to share individual injury data with employee if requested
Va. Code Ann. § 40.1-28.7:1 Genetic Testing or Genetic Characteristics as a Condition of Employment	Restrictive	Anti-discrimination	N/A	N/A	Bars collection of genetic information in employment
Genetic Data Privacy, VA ST § 59.1–593 through 59.1-602	N/A	Anti-discrimination	N/A	Limited sharing	Bars DTC companies from sharing genetic information without consent
Va. Code Ann. § 65.2-900(A) Records and reports of accidents	Mandated	Benefits	N/A	Required reporting	Requires employers to maintain injury, fatality records; required to report to workers comp, insurers, DLOI
Va. Code Ann. § 40.1-51.1(D) Duties of employers	Presumed	Injury surveillance	N/A	Required reporting	Requires employers to report injuries, fatalities to DLOI
Va. Code Ann. § 2.2-203.2:4 Office of Data Governance and Analytics; Chief Data Officer; creation; report.	TBD	Data privacy	TBD	TBD	2023 law authorizes creation of chief data officer. May develop data storage, sharing policies
Presumption as to death or disability from respiratory disease, hypertension or heart disease, cancer, VA ST § 65.2–402	Permissive	Benefits	N/A	N/A	Allows employers to collect firefighter medical information for presumptive benefits
16VAC25-60-80 Access to employee medical and exposure records	Presumed	Benefits, injury surveillance	N/A	Limited access	Imposes privacy safeguards on health professional, labor commissioner access to records

Note: “Restrictive” policies limit collection of data. “Permissive” policies allow data collection. “Presumed” indicates that the policies do not explicitly address data collection, but presume it has or will take place. “Mandated” requires data collection.

Federal Fire Prevention and Control Act of 1974, which established epidemiologic surveillance of firefighter injuries and fatalities.^{47–51} This law mandated the creation of the National Fire Data Center to conduct voluntary reporting of firefighter fatality and injury data. The law required that the Data Center collect information on serious fatalities (those

requiring medical treatment by a doctor), deaths occurring while preparing for work or a test, and injuries and deaths from motor vehicle and aircraft accidents. A smaller number of federal laws restricted the collection of medical, disability, or genetic information to prevent discrimination in employment,^{52,53} and one allowed for the collection of

Table 3. Nature of Union Data Privacy Policies by Jurisdiction.

	Maryland	Virginia
Overall	9	2
Collection	9	2
Restrictive	0	1
Permissive	4	1
Presumed	4	2
Mandated	4	2
Use/Purpose	8	2
Anti-discrimination	1	1
Injury surveillance	6	2
Benefits	5	1
Data privacy	0	0
Storage	2	1
Location	2	1
Duration	0	1
Access	5	2
Limited access, sharing	3	2
Required reporting, access	4	2
Encouraged sharing	0	0

Note: Some policies address more than one subcategory. "Restrictive" policies limit the collection of data. "Permissive" policies allow data collection. "Presumed" indicates that the policies do not explicitly address data collection, but presume it has or will take place. "Mandated" requires data collection.

medical information to process Family and Medical Leave Act (FMLA) benefits.⁵⁴ All of the policies addressed the location and retention of data; the Americans with Disabilities Act (ADA) and Genetic Information Nondiscrimination Act (GINA) required that medical and disability information be stored separately from personnel files.^{52,53} Four of the policies limited access to and sharing of medical and disability information,^{38,52–54} whereas three encouraged or required reporting of injury and fatality information (including individual employees' access to their own data).^{48,50,51} The lone fire service law encouraged the sharing of aggregated firefighter injury and fatality data collected by the National Fire Data Center.⁴⁷ These federal laws and regulations also applied at the state level. While federal OSHA does not necessarily cover state and local employees like firefighters, if states voluntarily enact their own OSHA plans, as Maryland and Virginia have, then federal standards apply.⁵⁵

Of Maryland's three statewide policies, two were similar to federal laws. One law barred the discriminatory collection of disability information in employment contexts, although, unlike the ADA, it did not contain storage, sharing, or access stipulations.⁵⁶ A regulation addressing employee injury and illness records required that employers report illnesses, injuries, and fatalities to Maryland's OSHA office (MOSH) but similarly lacked storage requirements. The Personal Information Protection Act, a data privacy law, emphasized data security, requiring secure storage (generally defined) of employee information, including health and

biometric information; it also required that employees be notified if their information is breached.³⁹

Virginia's eight statewide policies encompassed a range of data provisions, including injury and fatality reporting, benefits, limiting data access, and ensuring employees' data rights. Two statutes required reporting of injury and fatality data to the state Department of Labor and Industry (DOLI) and/or workers' compensation commission for injury surveillance or to process benefits.^{57,58} A fire-specific bill establishing presumptive benefits for firefighters allowed employers to collect medical information to confirm eligibility.⁵⁹ Several other policies addressed access to employee health and injury data, including a regulation that imposed limits on health professionals and the labor commissioner accessing employee records⁶⁰ and a law granting employees the right to access their own injury data.⁶¹ These protections are echoed in a consumer genetic testing law specifying that direct-to-consumer (DTC) companies cannot disclose consumer data to entities making decisions about employment without the consumer's consent.⁶² Virginia also laid the groundwork for future data privacy rulemaking: a 2023 law authorized the creation of a state Chief Data Officer and authorized extensive rulemaking, specifically around data collection, use, storage, sharing, and other privacy concerns related to data collected or maintained by state, regional, or local public entities.⁴⁰

Several collective bargaining agreements in Maryland addressed data related to physical exams, medical exams, or injuries, for the purposes of certifying leave or encouraging health and fitness. However, over half did not address storage or access/sharing,^{44,63–67} whereas three placed limits on who can access medical information and required that employees be able to access their own data.^{41–43} Montgomery County had the most comprehensive contract, which covered sick leave, injury, and medical information, but also specified that the department must collect fitness records. It also included detailed access and sharing provisions, mandating that fitness data must be treated as confidential and not shared outside of the fitness team, and that employee assistance program (EAP) information must not be shared without written consent from an employee.⁴³

As in Maryland, Virginia's two union contracts addressed recordkeeping requirements for injury and exposure data, as well as regular physical examinations.^{45,46} However, both contracts authorized broad use of electronic monitoring device data, with Arlington specifically allowing such data to be used for health and safety purposes. The Arlington contract authorized Arlington County's use of video, audio, or other electronic monitoring. Employees must be notified of audio and video recording, and the county cannot proactively use this data to identify policy violations. However, the contract specifically stated that "The County shall utilize video, audio, and data streams to ... improve the health and safety of employees, conduct training and professional development,

Table 4. Overview of Union Data Privacy Policies.

	Data Collection Permissions	Data Use and Purpose	Data Storage Parameters	Data Access Provisions	Notes
Maryland					
Anne Arundel County and IAFF 1563 (2022–2023)	Presumed	N/A	N/A	N/A	Requires the Safety Committee to make recommendations regarding a Personal Exposure Recording Program to document exposures
City of Baltimore and IAFF 734 (2022–2024)	Mandated, permissive, presumed	Injury surveillance	Location	Limited access (employer); required employee access	The department must include exposure reporting to injury reports and share injury reports with the union. Medical file access is limited to select department employees and individual employee access
Baltimore County and IAFF 1311 (2021–2023)	Permissive	Injury surveillance	N/A	Limited access	The department will offer hearing tests, medical exams, and physicals, and explore medical screening. Medical exam and physical data will be kept confidential
State of Maryland and IAFF 1742 (2022–2024)	Presumed	Benefits	N/A	N/A	Employees may take temporary, unpaid medical leave if it is medically documented; return to work based on the State Medical Director's declaration
Cumberland and IAFF 1715 (2017–2020)	Permissive	Benefits	N/A	N/A	Requires medical certification from a treating physician or other health care provider to obtain sick leave benefits beyond one shift in length
Hagerstown and IAFF 1605 (2018–2022)	Mandated	Injury surveillance	N/A	Required reporting	Requires a fitness for duty physical, but does not address storage or access, aside from reporting a lack of fitness for duty to HR
Montgomery County and IAFF 1664 (2022–2024)	Mandated	Anti-discrimination, benefits, injury surveillance	Location	Limited access, required employee access	Comprehensive guidance requiring documentation of medical or fitness information to provide benefits, promote health and safety, and prevent injury. Limits access to medical and fitness information and requires employee access to certain records
Ocean City and IAFF 4269 (2019–2024)	Permissive	Benefits, injury surveillance	N/A	N/A	The department may require a physical fitness assessment and medical exam annually. May also require a medical exam to facilitate return to duty following injury or illness
Prince George's County and IAFF 1619 (2022–2024)	Presumed, mandated	Benefits, injury surveillance	N/A	Required access	Requires annual medical physicals, accident reviews, and recordkeeping. Allows for medical information to be used in

(continued)

Table 4. Continued.

	Data Collection Permissions	Data Use and Purpose	Data Storage Parameters	Data Access Provisions	Notes
Virginia					certifying benefits, but data provisions are vague
Alexandria and IAFF 2141 (2023–2026)	Presumed, mandated, permissive	Injury surveillance	N/A	Limited access, required reporting, required employee access	Requires exposure recordkeeping, injury reports, and authorizes broad electronic monitoring. Allows for voluntary disclosure of injury or fatality to the union. Requires employee access to exposure records
Arlington and IAFF 2800 (2023–2026)	Mandated, restrictive, permissive	Anti-discrimination, benefits, injury surveillance	Location, duration	Limited access, required reporting, required employee access	Allows for the collection and maintenance of injury, fatality, illness, accident, and exposure information. Authorizes electronic monitoring for health and safety purposes, but does not address storage or access/sharing for this data

Note: “Restrictive” policies limit collection of data. “Permissive” policies allow data collection. “Presumed” indicates that the policies do not explicitly address data collection but presume it has or will take place. “Mandated” requires data collection.

facilitate promotional examinations, and perform research or investigations.”⁴⁵ While both Virginia contracts addressed access and sharing more generally, they did not include specific language regarding how this kind of electronic surveillance data might be accessed, shared, or stored within fire departments.

Examples Within Jurisdictions

Here we present examples of how firefighter data would be governed in different jurisdictions under the policies we identified. We provide examples of how injury and fitness data would be governed in Montgomery County, Maryland, and Arlington County, Virginia, which have unique union contracts and distinct state statutes that illustrate a range of data privacy policies. These examples are meant to be illustrative, but not exhaustive, examples of how firefighter data might be governed.

Injury data would be governed similarly in Montgomery County and in Arlington County. In both Maryland and Virginia, if a firefighter was injured, fire departments would be required to report injuries and would be able to use injury information to inform health and safety programs, although there were slight differences in how injury data would be handled. In both states, serious injuries that involved hospitalization, amputation, or loss of an eye must be reported within 24 hours to state agencies (both states were also covered by OSHA recordkeeping requirements because they have state OSHA plans). For firefighters in

both Montgomery and Arlington County, the union contracts authorized the use of injury information by the department’s Health and Safety Committee to inform health and safety recommendations.

In Virginia, state law required injury recordkeeping and sharing of these records with the state workers’ compensation commission and the employer’s insurance carrier within 10 days of an incident. If an injured firefighter requested his or her injury data, fire departments would be required to provide them copies of their records within 30 days. The Arlington County contract required that the department provide copies of injury documentation to employees and notify the union about serious injuries or fatalities. In Montgomery County, injury data would be subject to additional protections through the Maryland Personal Information Protection Act, which required that employee and former employee records be treated as confidential information. If injury information was breached, employers would be required to contact affected individuals. For Montgomery County firefighters, the union contract also required that injury information be redacted to protect firefighter confidentiality.

Fitness data would be governed differently in Montgomery and Arlington Counties. The Montgomery County union contract included detailed provisions about fitness data, including limits on how it could be used, whereas the Arlington County contract had looser protections for this data. The Montgomery County contract required the department’s Exercise Physiologist to maintain firefighter fitness records and detailed specific kinds of data to be collected,

such as capacity, body composition, flexibility, muscular strength, and endurance. The contract included descriptions of acceptable and unacceptable uses for this data, explicitly barring this information from being used to evaluate firefighter performance, for disciplinary purposes, to evaluate workers' compensation or disability claims, or other personnel decisions, while allowing it to be used to help maintain fitness for duty. There were also specific limits on data storage and data access, as only the Exercise Physiologist and Peer Fitness Trainers performing a fitness assessment were allowed to access the data. Fitness data in this department would also be subject to Maryland and federal policies, such as the Maryland Personal Information Protection Act, which required that employee data be stored and treated as confidential information.

By contrast, the Arlington County contract included provisions about fitness data but had fewer protections surrounding the use of such data. The contract authorized the department to refer a firefighter for a fitness evaluation and notify the Fire Chief if a firefighter could not perform job functions. However, the contract did not prohibit the use of these data for performance evaluations or disciplinary purposes, as in Montgomery County, leaving the potential for fitness information to be used to make personnel decisions or evaluate performance and fitness for duty. A general provision of the Arlington contract required that test results be retained for 30 years, whereas the Montgomery County contract only addressed the location of data.

Discussion

Our research identified a range of policies governing occupational health and safety data, highlighting strengths and gaps in the existing regulatory framework protecting firefighters federally and in Maryland and Virginia. We identified only one narrowly scoped federal regulation specifically addressing employee occupational health and safety data privacy: 29 CFR § 1913.10 Rules of Agency Practice and Procedure Concerning OSHA Access to Employee Medical Records.⁶⁸ This regulation applied only to OSHA staff, and did not apply to employers, researchers, or commercial entities that frequently obtain employee data. Although we identified several federal-level policies that required the collection of serious injury and fatality data, laws and regulations requiring the reporting of injuries and fatalities failed to address access or sharing concerns, instead encouraging the sharing of aggregated data. While publishing injury and fatality trends is essential for understanding and improving workplace health and safety, public policies should ensure that the reporting of such information does not threaten worker privacy. These safeguards will become even more essential as technology advances. With the advent of sensors and wearable devices, employers could begin to collect highly sensitive data, including biometric information, in greater quantities than ever before.³

On the federal level, our review included GINA but excluded the Health Insurance Portability and Accountability Act (HIPAA). These two laws are commonly cited in data privacy discussions^{35,36} but we found that they have limited applicability to our topic of interest. HIPAA applied only to covered entities and their associates; HIPAA covers neither employers nor employee data collected in an occupational context.^{35,69} GINA has implications for employee health and safety data, as its provisions addressed genetic information broadly defined (e.g., information from genetic tests of the employee or family member, and family medical history). This offers some protections for employee health and safety data, such as firefighters' personal or family medical histories, which might arise during annual physicals or fitness for duty assessments. However, GINA included several exceptions through which employers may collect genetic information, including through voluntary workplace wellness programs and when monitoring toxic substances.^{35,53} Employers might gain access to sensitive information depending on the circumstances under which they obtain genetic information, although in these cases, employers would still be prohibited from using such information in a discriminatory fashion. This emphasis on preventing discriminatory use of genetic information might be sufficient for ensuring such data is not used inappropriately, but employees might prefer stronger prohibitions on the collection of such data in the first place. And while GINA protected a broad array of genetic information, it may not address the full range of health information covered in other contexts (e.g., HIPAA in health care settings), reflecting gaps in federal data privacy policies in occupational settings.

The path to future federal rulemaking to protect firefighter data privacy is uncertain. For instance, in the early months of the Trump Administration, the National Firefighter Registry for Cancer was taken offline for several weeks before being reinstated.⁷⁰ While federal support for firefighter data initiatives is unclear, our findings highlight the need for strengthened firefighter privacy protections at the federal level. State policies such as those we identified in Maryland and Virginia could serve as models to inform future federal policymaking. From a fire service standpoint, in May 2023, the U.S. Fire Administration announced that it will transition from its legacy injury surveillance system, the National Fire Incident Reporting System (NFIRS), to a modernized platform, the National Emergency Response Information System (NERIS).¹⁰ NERIS, which fulfills statutory requirements of the Federal Firefighting Control Act, will modernize and streamline the fire service's data procedures and expand its data capabilities. Policymakers should consider how to design this platform in ways that respect firefighter data privacy and incorporate input from a diverse array of fire service stakeholders on appropriate data protections.

On the state level, Maryland and Virginia serve as two distinct examples. Virginia's occupational data privacy laws and regulations appeared to be stronger in quantity and quality,

but it had fewer collective bargaining agreements, and they authorized broad electronic monitoring of firefighters. Despite the breadth of Virginia's existing policies, we did not identify laws or regulations addressing the storage of occupational health and safety data, and only Arlington's contract addressed storage. Virginia may want to consider enacting uniform policies for where and how employee occupational health and safety information is stored. The small number of union contracts is likely due to historic labor laws in the state. Virginia is a right-to-work state, and until 2021, public employees were banned from engaging in collective bargaining.^{71,72} In 2023, Alexandria ratified the first firefighter contract in the state in over 40 years, quickly followed by Arlington.^{73,74} While Arlington's contract prohibited the department from conducting proactive searches of electronic monitoring data for discipline or retaliation, both contracts allowed for review of such data as part of an investigation. Neither contained specifications for how such data should be stored or for who may access or share the data. These unions, and unions attempting to negotiate for the first time in Virginia, could advocate for stronger data protections in future contracts.

Maryland's firefighter data privacy protections were primarily found in union contracts. Maryland's data privacy law included general requirements that data be stored securely, and was amended to specifically cover health and biometric information, which could serve as a model for sophisticated biometric data storage policies.³⁹ However, this legislation did not address other key data considerations, such as data collection or sharing. The state should consider adopting public policies that address these factors or, like Virginia, emphasize employees' rights to access and/or disclose their data. Several of Maryland's collective bargaining agreements build on state and federal policies by limiting fire department personnel's access to sensitive information such as medical, injury, or fitness data; jurisdictions without these protections may wish to incorporate them in future negotiations. While none of Maryland's contracts explicitly authorized the kinds of electronic surveillance included in Virginia's contracts, in Maryland, leadership of local union affiliates of the International Association of Fire Fighters (IAFF) should consider raising surveillance issues to protect firefighters' privacy in future negotiations.

Our findings are consistent with the conclusions of data privacy law experts who criticize the lack of federal data privacy legislation and call for the development of privacy-oriented labor laws.²⁶ There is robust debate about the best regulatory approach towards data privacy, as future laws and regulations should protect privacy across multiple populations while not imposing unreasonable administrative burdens. Some scholars have argued that privacy should be viewed as an instrumental good—something valuable as a means to other non-privacy goals—meaning that future legislation or rulemaking should also account for non-privacy objectives, such as enhanced worker safety.^{26,35,36} The path

towards comprehensive privacy legislation is complex, as lawmakers could opt for laws applying across worker populations, in the consumer space, or based around kinds of data or technologies. Alternatively, regulators might promulgate new privacy-oriented rulemaking within the bounds of existing legislative mandates, strengthening OSHA's injury surveillance data protections or incorporating privacy safeguards into the Fire Administration's NERIS system. National-level reforms could secure data for large swaths of workers and minimize patchwork protections across states and localities. But national-level policymaking, particularly if aimed at large and diverse populations, faces a host of challenges, both conceptual and practical. Advancing federal policy is challenging due to the complexity of defining and gaining recognition for a problem, developing an appropriate policy solution, and navigating complex political dynamics.⁷⁵ Advancing firefighter data privacy policies at the federal level seems particularly challenging at the time of this writing, given the highly polarized political environment and shifting landscape for federal firefighter data initiatives.

In highly unionized workforces like the fire service,⁷⁶ unions may be the most effective advocates for enacting occupational health and safety policies in individual workplaces. Legal scholars have begun to debate the merits of collective bargaining as a pathway for securing privacy protections for the use of wearable technology.³⁵ Some believe unions are best positioned to negotiate for these reforms, while others point out that this route excludes non-unionized employees and industries. There are few examples of unions addressing wearable technology. Unions representing professional athletes have begun to consider wearable data privacy, although experts suggest that most contracts fail to address core privacy issues.^{35,77}

In both states we examined, union contracts contained the most granular protections for firefighter data and reflected unique department characteristics and cultures. Union-led privacy reforms are not without challenges. Not all departments are unionized, contracts are renegotiated frequently, and contracts can vary significantly, as we observed in our sample in two neighboring states. The collective bargaining process is unique in that unions negotiating a contract face different pressures and priorities compared to the public policymaking process. While unions might be best equipped to negotiate on behalf of their members, they bear responsibility for other priorities such as obtaining pay raises, insurance benefits, and leave allowances. Public policy making, which could cover a broader range of employees, offers a more comprehensive pathway towards securing data privacy protections, and might result in stronger and more equitable protections across worker populations and employers. However, policymaking is often a slow process, and there may be tradeoffs between covering a larger array of employees and addressing concerns specific to individual sectors such as the fire service. In the absence of federal or state legislation or rulemaking, unions can serve as

firefighters' best advocates for appropriate data privacy protections. Collective bargaining agreements can also serve as examples of what occupational health and safety data protections should look like in the fire service, and as test cases for ensuring such policies are not overly burdensome. Union leaders preparing for future collective bargaining negotiations should anticipate increased monitoring or surveillance and be prepared to negotiate provisions that protect their members' data privacy and prevent discriminatory use of such data.

Beyond unions, our findings have implications for other stakeholders with an interest in firefighter occupational health and safety data. Researchers, who may not actively engage in bargaining, can help establish an evidence base on firefighters' data privacy preferences. And as OSHA and the U.S. Fire Administration attempt to modernize injury surveillance systems, researchers whose work relies on such data can serve as advocates for expanding access to important data while maintaining the privacy of workers. As we described above, the outlook for federal firefighter data initiatives and any associated privacy considerations remains uncertain in the current political environment. However, our study documents existing policies and policy gaps that researchers and advocates can attempt to strengthen in the coming years. More generally, our study highlights the need for greater consideration of occupational health and safety data in data privacy discussions. Our findings contribute an exploratory analysis of this topic to the growing literature on worker data and can serve as a starting point for legal experts and privacy advocates to consider as they seek policy reforms.

Limitations

Our study has several limitations. We did not conduct a comprehensive review of federal, Maryland, or Virginia guidance documents, nor did we include a review of federal, Maryland, or Virginia case law. Our scope was narrowly defined to identify the laws, regulations, and union contract provisions oriented around firefighter health and safety data, but did not necessarily capture all of the policies that might govern this data (e.g., state laws dictating how personnel data should be handled more generally). While we examined union contracts, we did not include municipal, county, or fire department policies or procedures that might cover firefighter data. Put simply, our findings are not an exhaustive legal analysis of all the potential policies that could govern firefighter health and safety data. However, to our knowledge, this is the first study to examine this topic and establish an overview of the policy environment surrounding firefighter health and safety data. This exploratory analysis sheds light on existing occupational health and safety data policy protections and highlights opportunities for future research, advocacy, and policymaking. Policy researchers and legal scholars should examine this topic in other states and

localities and for additional worker populations. Researchers can also build upon this work by exploring the impact and enforcement of these policies in practice settings.

Conclusion

Our study found that career firefighter health and safety data is governed by a patchwork of laws, regulations, and local policies at the federal level and in Maryland and Virginia. While our analysis is preliminary, it demonstrates that these policies address a range of data privacy considerations, including data collection, use, storage, and sharing or access, but few are oriented around data privacy. This research lends support to calls for additional policymaking to ensure that worker data is adequately protected and highlights opportunities for advocates and researchers to more effectively engage with the policymaking process. Policies that appropriately safeguard health and safety data may bolster employees' confidence in injury prevention efforts and ensure that they work in inclusive, healthy, and safe environments.

Funding

The authors disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: Rachel Topazian received tuition and stipend support from a grant from the U.S. Centers for Disease Control and Prevention, National Institute for Occupational Safety and Health to the Johns Hopkins Education and Research Center for Occupational Safety and Health (#T42 OH0008428), as well as the Susan P. Baker Scholarship in Injury Prevention and Control and the Johns Hopkins Bloomberg School of Public Health's Center for Qualitative Studies in Health and Medicine.

Declaration of Conflicting Interests

The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Supplemental Material

Supplemental material for this article is available online.

ORCID iDs

Rachel J. Topazian  <https://orcid.org/0000-0002-7443-4595>
Shannon Fattaroli  <https://orcid.org/0000-0002-2973-277X>

References

1. Campbell R, Hall S and Petrillo J. United States Firefighter Injuries. NFPA Research, National Fire Protection Association, <https://www.nfpa.org/education-and-research/research/nfpa-research/fire-statistical-reports/firefighter-injuries-in-the-united-states> (2025, accessed 21 January 2026).
2. Campbell R and Petrillo JT. Firefighter fatalities in the United States, <https://www.nfpa.org/education-and-research/research/nfpa-research/fire-statistical-reports/fatal-firefighter-injuries> (2025, accessed 21 January 2026).

3. Grant C, Hamins A, Bryner N, et al. *Research roadmap for smart firefighting*. US Department of Commerce, National Institute of Standards and Technology, 2015.
4. McClure LA, Koru-Sengul T, Hernandez MN, et al. Availability and accuracy of occupation in cancer registry data among Florida firefighters. *PLoS One* 2019; 14: e0215867. doi:10.1371/journal.pone.0215867
5. Kahn SA and Mosier M. Firefighter injury data are wrought with discrepancy: pearls from the national burn repository. *J Burn Care Res* 2018; 39: 623–625. doi:10.1093/jbcr/irx025
6. Widman SA, LeVasseur MT, Tabb LP, et al. The benefits of data linkage for firefighter injury surveillance. *Inj Prev* 2018; 24: 19–28. doi:10.1136/injuryprev-2016-042213
7. Kritzler M, Bäckman M, Tenfält A, et al. Wearable technology as a solution for workplace safety. In: *Proceedings of the 14th International Conference on Mobile and Ubiquitous Multimedia* 2015; 213–217.
8. Harris A, Sims R and Roberts A. BioErgo Surveillance: New Approaches for Total Worker Health. In: *Association AIH. Synergist*, 2020.
9. Fent KW, Siegel M, Mayer A, et al. National Firefighter Registry Protocol. 2023.
10. U.S. Fire Administration. About the National Emergency Response Information System (NERIS), <https://www.usfa.fema.gov/nfirs/neris/about-neris/> (2024, accessed 15 January 2026).
11. Jahnke SA, Poston WS, Jitnarin N, et al. Health concerns of the US fire service: perspectives from the firehouse. *Am J Health Promot* 2012; 27: 111–118. doi:10.4278/ajhp.110311-QUAL-109
12. Averill JD, Moore-Merrell L, Notarianni K, et al. Proceedings of the National Fire Service Data Summit. 2011.
13. Moore-Merrell L. The Importance of Data to the Fire Service. *Firehouse*. 2021.
14. Amidon TR, Williams EA, Lipsey T, et al. Sensors and gizmos and data, oh my: informing firefighters' personal protective equipment. *Communication Design Quarterly Review* 2018; 5: 15–30. doi:10.1145/3188387.3188389
15. Occupational Safety and Health Administration. Improve Tracking of Workplace Injuries and Illnesses Final Rule. In: Labor Do, (ed.). 2023.
16. Occupational Safety and Health Administration. Improve Tracking of Workplace Injuries and Illnesses Proposed Rule. In: Labor Do, (ed.). 2022.
17. International Association of Firefighters. Mythbusting the National Firefighter Registry for Cancer: 5 facts you should know, <https://www.iaff.org/news/mythbusting-the-national-firefighter-registry-for-cancer-5-facts-you-should-know/> (2024, accessed 15 January 2026).
18. Robling M, Hood K, Houston H, et al. Public attitudes towards the use of primary care patient record data in medical research without consent: a qualitative study. *J Med Ethics* 2004; 30: 104–109. doi:10.1136/jme.2003.005157
19. Kaufman DJ, Murphy-Bollinger J, Scott J, et al. Public opinion about the importance of privacy in biobank research. *The American Journal of Human Genetics* 2009; 85: 643–654. doi:10.1016/j.ajhg.2009.10.002
20. Emanuel EJ, Wendler D and Grady C. What makes clinical research ethical. *JAMA* 2000; 283: 2701–2711. DOI: 10.1001/jama.283.20.2701
21. Gray EA and Thorpe JH. Comparative effectiveness research and big data: balancing potential with legal and ethical considerations. *J Comp Eff Res* 2015; 4: 61–74. doi:10.2217/ce.14.51
22. Rumsey A and Le Dantec CA. Clearing the smoke: the changing identities and work in firefighters. In: *Proceedings of the 2019 on designing interactive systems conference* 2019; pp. 581–592.
23. Topazian RJ, Wec A, Ali J, et al. Ethical use of wearable device data in occupational settings: perspectives from the fire service. *J Occup Environ Med* 2025: 10.1097.
24. Jacobs JV, Hettinger LJ, Huang Y-H, et al. Employee acceptance of wearable technology in the workplace. *Appl Ergon* 2019; 78: 148–156. doi:10.1016/j.apergo.2019.03.003
25. Schall JM, Sesek RF and Cavuoto LA. Barriers to the adoption of wearable sensors in the workplace: a survey of occupational safety and health professionals. *Hum Factors* 2018; 60: 351–362. doi:10.1177/0018720817753907
26. Ifeoma Ajunwa KC and Schultz J. Limitless worker surveillance. *Calif Law Rev* 2018; 105: 735–776.
27. Levy K. Data driven: Truckers, technology, and the new workplace surveillance. 2022.
28. Fahy RF, Evarts B and Stein GP. *US fire department profile 2020*. Quincy, MA, USA: National Fire Protection Association, 2022.
29. International Association of Firefighters. Home - IAFF, <https://www.iaff.org/> (2026, accessed 15 January 2026).
30. Valentino J. Setting the framework for biometric privacy legislation after the “Big Bang” of biometrics in the workplace. *Hofstra Lab & Emp LJ* 2020; 38: 167.
31. Schuman A. Who's checking? A proposal to protect employee health screening data. *Hofstra Lab & Emp LJ* 2021; 39: 177.
32. Anne G and Bibeau VBL. *Employee privacy laws*. Virginia, 2023.
33. Fiona W and Ong ET-D. *Employee privacy laws*. Maryland, 2023.
34. U.S. Fire Administration. Search the National Fire Department Registry, <https://apps.usfa.fema.gov/registry/search> (2026, accessed 15 January 2026).
35. Ajunwa I. *The quantified worker: Law and technology in the modern workplace*. Cambridge University Press, 2023.
36. Richards NM. Why privacy matters: an introduction. *Neil Richards, Why Privacy Matters (Oxford Press 2021)* 2021.
37. International Association of Firefighters. Presumptive Health Initiative, <https://www.iaff.org/presumptive-health/> (2026, accessed 15 January 2026).
38. Occupational Safety and Health Administration. *Rules of agency practice and procedure concerning OSHA access to employee medical records*. 29 CFR Sect 191310. 2020.
39. Maryland General Assembly. Title 14 Subtitle 35 Maryland Personal Information Protection Act. 2008.
40. Virginia General Assembly. § 2.2-203.2:4 Chief Data Officer; position created. 2019.
41. Memorandum of Understanding Fiscal Years 2022-2024 between the Mayor and City Council of Baltimore and

- Baltimore Fire Fighters Local 734, IAFF AFL-CIO, CLC. 2022.
42. Memorandum of Understanding between the Baltimore County Administration and the Baltimore County Professional Firefighters Association IAFF Local 1311. 2022.
 43. Agreement Between Montgomery County Career Fire Fighters Association, International Association of Fire Fighters, Local 1664, AFL-CIO and Montgomery County Government/ Montgomery County, Maryland For the Years July 1, 2022 Through June 30, 2024. 2022.
 44. Agreement Made by and between Prince George's County, Maryland, and International Association of Fire Fighters Local 1619 (Fire Fighters, Paramedics and Fire Fighter/ Medics) July 1, 2022 Through June 30, 2024. 2022.
 45. Collective Bargaining Agreement Between Arlington Professional Firefighters and Paramedics Assoc., IAFF Local 2800 and Arlington County Government July 1, 2023 Through June 30, 2026. 2023.
 46. Collective Bargaining Agreement between the City of Alexandria, Virginia, and the International Association of Fire Fighters Local 2141 Effective From July 1, 2023-June 30, 2026. 2023.
 47. 106th U.S. Congress. Fire Administration Authorization Act of 2000. 2000.
 48. 91st U.S. Congress. Occupational Safety and Health Act 1970.
 49. Equal Employment Opportunity Commission. Recordkeeping and Reporting Requirements Under Title VII, the ADA, GINA, and the PWFA. 2023.
 50. Occupational Safety and Health Administration. Access to employee exposure and medical records. 1980.
 51. Occupational Safety and Health Administration. Recording and Reporting Occupational Injuries and Illnesses. 2001.
 52. 101st U.S. Congress. Americans with Disabilities Act. 1990.
 53. 110th U.S. Congress. Genetic Information Nondiscrimination Act. 2008.
 54. 103rd U.S. Congress. Family and Medical Leave Act. 1993.
 55. Occupational Safety and Health Administration. State Plans. <https://www.osha.gov/stateplans> (2026, accessed 16 January 2026).
 56. Maryland General Assembly. Labor and Employment Title 3 - Employment Standards and Conditions Subtitle 7 - Miscellaneous Section 3-701 - Medical Questions. 2024.
 57. Virginia General Assembly. § 65.2-900 Records and reports of accidents. 1995.
 58. Virginia General Assembly. § 40.1-51.1 Duties of employers. 2016.
 59. Virginia General Assembly. § 65.2-402 Presumption as to death or disability from respiratory disease, hypertension or heart disease, cancer. 2023.
 60. Virginia General Assembly. 16VAC25-60-80 Access to employee medical and exposure records. 2006.
 61. Virginia General Assembly. § 8.01-413.1 Certain copies of employment records or papers admissible; right of employee or his attorney to copies of such records or papers; subpoena; damages, costs and attorney's fees. 1987.
 62. Virginia General Assembly. § 59.1-593 through 59.1-602 Genetic Data Privacy - Limitations. 2023.
 63. Memorandum of Agreement, Anne Arundel County and Local 1563 IAFF. 2022.
 64. Collective Bargaining Agreement Between the Town of Ocean City, Maryland and Career Fire Fighter Paramedics Association of Ocean City, IAFF Local 4269, International Association of Firefighters, Local 4269, AFL-CIO Effective July 1, 2019 - June 30, 2022 (later amended through 2024).
 65. Agreement Between the City of Hagerstown, Maryland and International Association of Fire Fighters, Local Number 1605 Effective July 1, 2018 - June 30, 2022. 2018.
 66. IAFF Local 1715 Collective Bargaining Agreement with the Mayor and City Council of Cumberland, MD July 1, 2017 through June 30, 2020. 2017.
 67. Memorandum of Understanding between the State of Maryland and the Baltimore/Washington International Airport Professional Fire Fighters Local 1742 IAFF, AFL-CIO, CLC January 1, 2022-December 31, 2024. 2022.
 68. Occupational Safety and Health Administration. Rules of agency practice and procedure concerning OSHA access to employee medical records, <https://www.osha.gov/laws-regs/regulations/standardnumber/1913/1913.10> (2020, accessed 16 January 2026).
 69. U.S. Department of Health and Human Services. HIPAA Privacy Rule. 2002.
 70. Carey B. National Firefighter Registry for Cancer back online following earlier NIOSH program cuts, <https://www.firerescue1.com/niosh/national-firefighter-registry-for-cancer-back-online-following-changes-to-niosh-programs> (2025, accessed 16 January 2026).
 71. Virginia General Assembly. § 40.1-58 Denial or Abridgement of Right to Work. 1970.
 72. Guzman ER. HB582 Employees of local governments; collective bargaining, <https://www.vaco.org/wp-content/uploads/2020/02/CollectiveBargainingAdditionAnalysis21320.pdf> (2020, accessed 16 January 2026).
 73. International Association of Firefighters. VA Local Ratifies State's First Contract in 40 years, <https://www.iaff.org/news/va-local-ratifies-states-first-contract-in-40-years/#:~:text=Alexandria%2C%20VA%20Local%202141%20became,collective%20bargaining%20unconstitutional%20in%201977.> (2023, accessed 16 January 2026).
 74. Rizzo S. *Arlington signs first contract with fire and EMS union since 1975. The Washington Post*, 2023.
 75. Kingdon JW. *Agendas, Alternatives, and Public Policies*. 2nd ed, 2002.
 76. U.S. Bureau of Labor Statistics. Union Members. <https://www.bls.gov/news.release/pdf/union2.pdf> (2025, accessed 16 January 2026). 2024.
 77. Studnicka A. The emergence of wearable technology and the legal implications for athletes, teams, leagues and other sports organizations across amateur and professional athletics. *DePaul J Sports L* 2020; 16: i.

Author Biographies

Rachel J. Topazian is an assistant professor in the Division of General Internal Medicine at the University of Colorado School of Medicine and a core faculty member at the Center for Bioethics and Humanities at the University of Colorado Anschutz Medical Campus.

Paul Locke is a professor in the Department of Environmental Health and Engineering at the Johns Hopkins Bloomberg School of Public Health.

Joe Ali is an associate professor in the Department of International Health at the Johns Hopkins Bloomberg

School of Public Health and associate director for Global Programs at the Johns Hopkins Berman Institute of Bioethics.

Shannon Frattaroli is a professor in the Department of Health Policy and Management and director of the Center for Injury Research and Policy at the Johns Hopkins Bloomberg School of Public Health.

Cassandra K. Crifasi is an associate professor in the Department of Health Policy and Management and co-director of the Center for Gun Violence Solutions at the Johns Hopkins Bloomberg School of Public Health.