

HOW TO ADAPT YOUR INCIDENT AND BREACH RESPONSE STRATEGY TO TODAY'S REGULATORY ENVIRONMENT

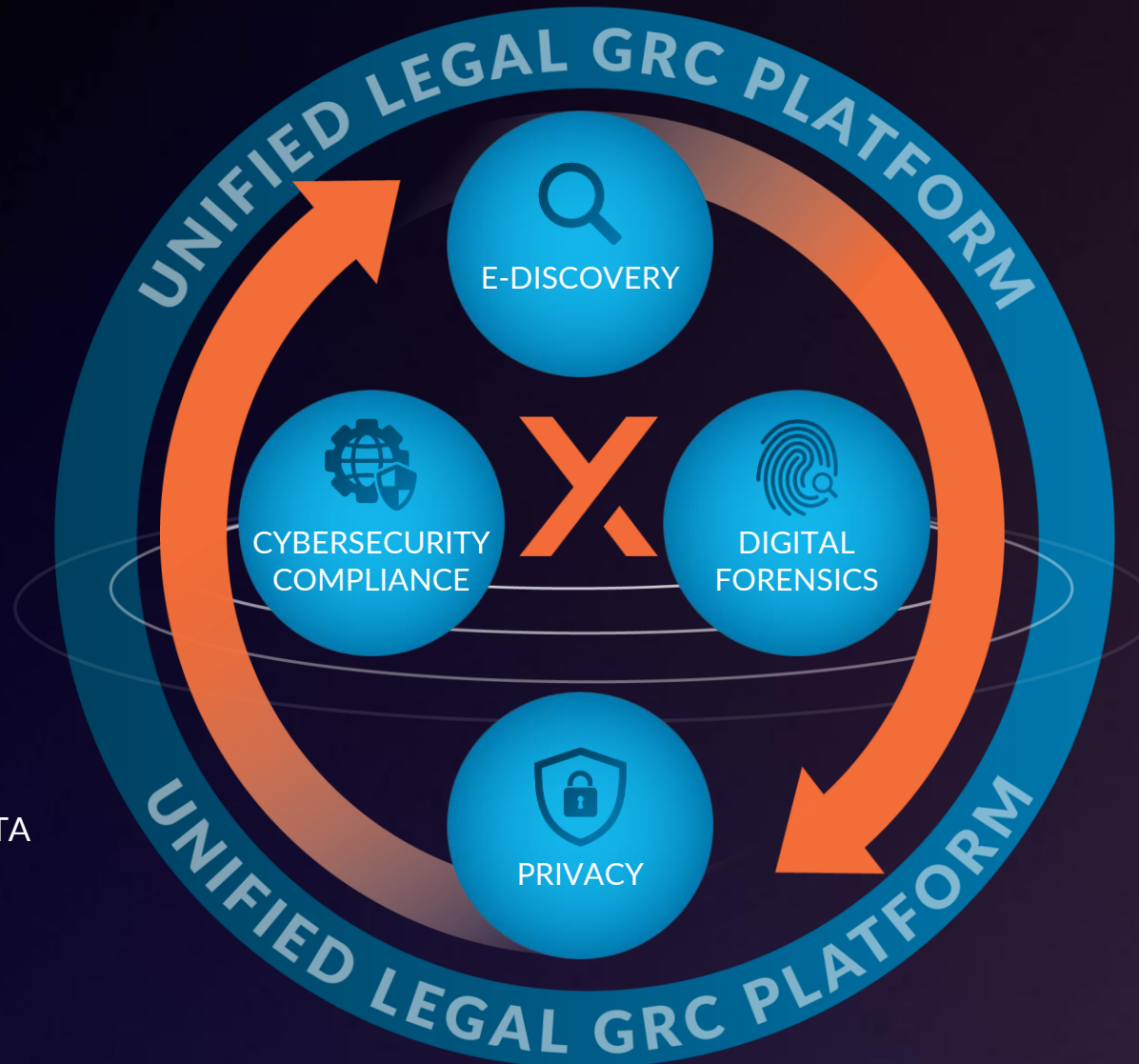
exterro®



exterro® THE ONLY VENDOR TO BRING IT ALL TOGETHER

PLATFORM FEATURES:

- ✓ INTEGRATED PLATFORM
- ✓ PROCESS ORCHESTRATION
- ✓ ARTIFICIAL INTELLIGENCE
- ✓ ROBUST DATA INVENTORY
- ✓ DATA MANAGEMENT
- ✓ HARDENED SECURITY
- ✓ COMPREHENSIVE DATA CONNECTORS
- ✓ OPEN API'S



BUILT FOR:



CORP. GENERAL
COUNSEL



LAW FIRMS



GOVERNMENT



CORP. IT/INFO.
SECURITY



LEGAL SERVICE
PROVIDERS



LAW
ENFORCEMENT

exterro® Legal GRC Platform



In this webcast our panel will review...

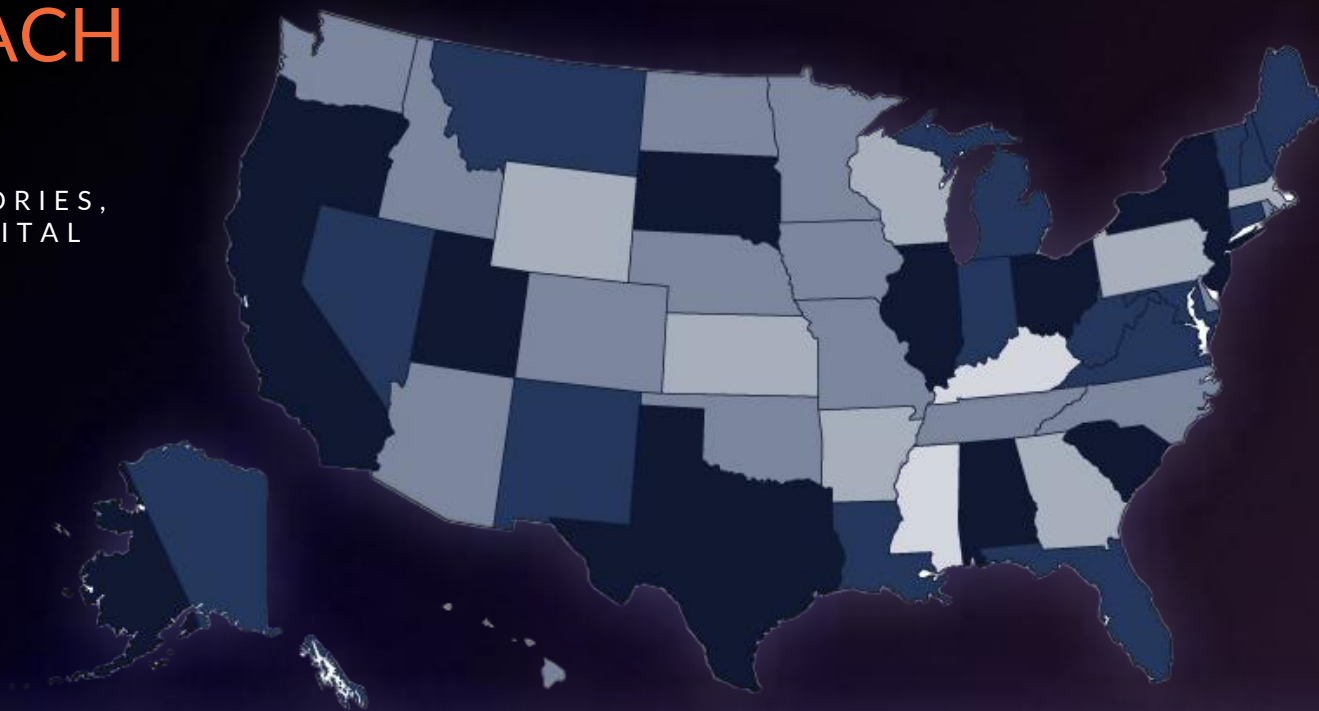


The background of the slide is a dark, pixelated image. It features a large, faint question mark in the center, composed of many small squares in shades of blue, purple, and red. The overall effect is a digital or data-themed aesthetic.

DATA BREACH AND INFO. SEC. LAWS IN THE US

DATA BREACH LAWS

IN STATES, TERRITORIES,
AND THE U.S. CAPITAL



← Stricter laws			Less strict laws →								
5	Alabama	5	Texas	4	Michigan	3	Colorado	3	North Dakota	2	Kansas
5	California	5	Utah	4	Montana	3	Delaware	3	Oklahoma	2	Massachusetts
5	Illinois	4-5	Alaska	4	Nevada	3	Hawaii	3	Rhode Island	2	Pennsylvania
5	New Jersey	4	Connecticut	4	New Hampshire	3	Idaho	3	Tennessee	2	Wisconsin
5	New York	4	Florida	4	New Mexico	3	Iowa	3	Washington	2	Wyoming
5	Ohio	4	Indiana	4	Vermont	3	Minnesota	3	Guam	2	Washington, D.C.
5	Oregon	4	Louisiana	4	Virginia	3	Missouri	3	Puerto Rico	2	U.S. Virgin Islands
5	South Carolina	4	Maine	4	West Virginia	3	Nebraska	2	Arkansas	1	Kentucky
5	South Dakota	4	Maryland	3	Arizona	3	North Carolina	2	Georgia	1	Mississippi



U.S. Law Regarding Data Breaches

- All 50 states have their own, similar breach notification laws.
- These laws apply if the *individual* is a resident of that state.
- Focus is *not* on where the company is located.
- Certain industries are regulated by federal law (finance, healthcare).
- Only apply if certain data elements are exposed – e.g., social security number, driver's license number, financial account number, username/password for online account, and sometimes medical/health, insurance, passport number, and biometrics.
- Generally can conduct a risk assessment.



U.S. Law – Owner vs. Licensee or User

- The obligation to notify individuals/regulators belongs to the data owner.
- *To whom did the individual entrust their personal information?*
- The licensee or user of the data has to notify the owner (should be done right away).
- In practice, the owner looks to the licensee or user to take the lead to notify the individuals.
- Often data security provisions are included in vendor contracts (in some instances, the law requires it).



California Consumer Privacy Act (CCPA): A Litigation Game Changer

- First state to provide for statutory damages from a breach
- \$100-750 per incident – no need to prove actual damages (but you can)
- Consumer's nonencrypted or nonredacted personal information is subject to unauthorized access and exfiltration, theft or disclosure as a result of a business's failure to maintain reasonable security procedures





ENFORCEMENT UNDER THE CCPA

What is the CPRA?

California Privacy Rights Act

[Ballot Initiative]

Will go into effect January 2023

CALIFORNIANS FOR CONSUMER PRIVACY

Data Privacy Law Comparison

Components	GDPR (EU Law)	CCPA	CPRA	Components	GDPR (EU Law)	CCPA	CPRA
Right to Know What Information a Business has Collected About You				Storage Limitation: Right to Prevent Companies from Storing Info Longer than Necessary			
Right to Say No to Sale of Your Info				Data Minimization: Right to Prevent Companies from Collecting More Info than Necessary			
Right to Delete Your Information				Right to Opt Out of Advertisers Using Precise Geolocation (< than 1/3 mile)			
Data Security: Businesses Required to Keep Your Info Safe				Ability to Override Privacy in Emergencies (Threat of Injury/ Death to a Consumer)			
Data Portability: Right to Access Your Information in Portable Format				Provides Transparency around "Profiling" and "Automated Decision Making"			
Special Protection for Minors				Establishes Dedicated Data Protection Agency to Protect Consumers			
Requires Easy "Do Not Sell My Info" Button for Consumers				Restrictions on Onward Transfer to Protect Your Personal Information			
Provides Ability to Browse with No Pop-ups or Sale of Your Information				Requires High Risk Data Processors to Perform Regular Cybersecurity Audits			
Penalties if Email Plus Password Stolen due to Negligence				Requires High Risk Data Processors to Perform Regular Risk Assessments			
Right to Restrict Use of Your Sensitive Personal Information				Appoints Chief Auditor with Power to Audit Businesses' Data Practices			
Right to Correct Your Data				Protects California Privacy Law from being Weakened in Legislature	N/A		

New Era in Class Action Litigation

Who Stand to Benefit the Most
From New Data Privacy Laws?

LAWYERS



Will the CCPA be the New TCPA for Plaintiffs?

By Elliot Golding and Petrina McDaniel on May 28, 2019

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

[REDACTED] an individual and
California resident, on behalf of herself and all
others similarly situated,

Plaintiff,

vs.

[REDACTED] and
[REDACTED]

Defendants.

Case No.:

CLASS ACTION COMPLAINT

- 1.) Negligence
- 2.) Declaratory Relief
- 3.) Violation of the California Unfair Competition Law, Business & Professions Code § 17200, *et seq.*

DEMAND FOR JURY TRIAL

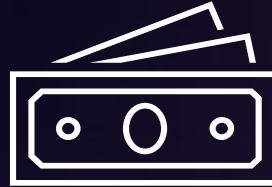


Enforcement & Litigation Actions

VIOLATIONS

REG. FINES
\$2,500
TO
\$7,000

PER VIOLATION



DATA BREACH

DAMAGES
\$100
TO
\$750

PER DATA SUBJECT



Understanding Your Requirements

- Breached information must contain PII
- PII must be nonencrypted *and* nonredacted
- The breach must have been “a result of the business’s violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.”
- Once notified of breach, organizations have thirty days to cure the violation and provide the consumer with a written statement



Improving the Incident Response Function

- Activate the incident response team
- Identify a project manager
- Set up bridge for regular calls
- Discourage communication in writing
- Limit any writings to facts – not speculation
- Outline expectations for confidentiality
- Identify final decision-makers

Improving the Incident Response Function

- Evaluate whether notification is required
 - Regulators
 - Payment card processor if relevant
 - Data owner/controller if required
 - Individuals
 - Employees
 - Law enforcement
 - Insurer





3 STRATEGIES TO COMBAT ENFORCEMENT ACTIONS

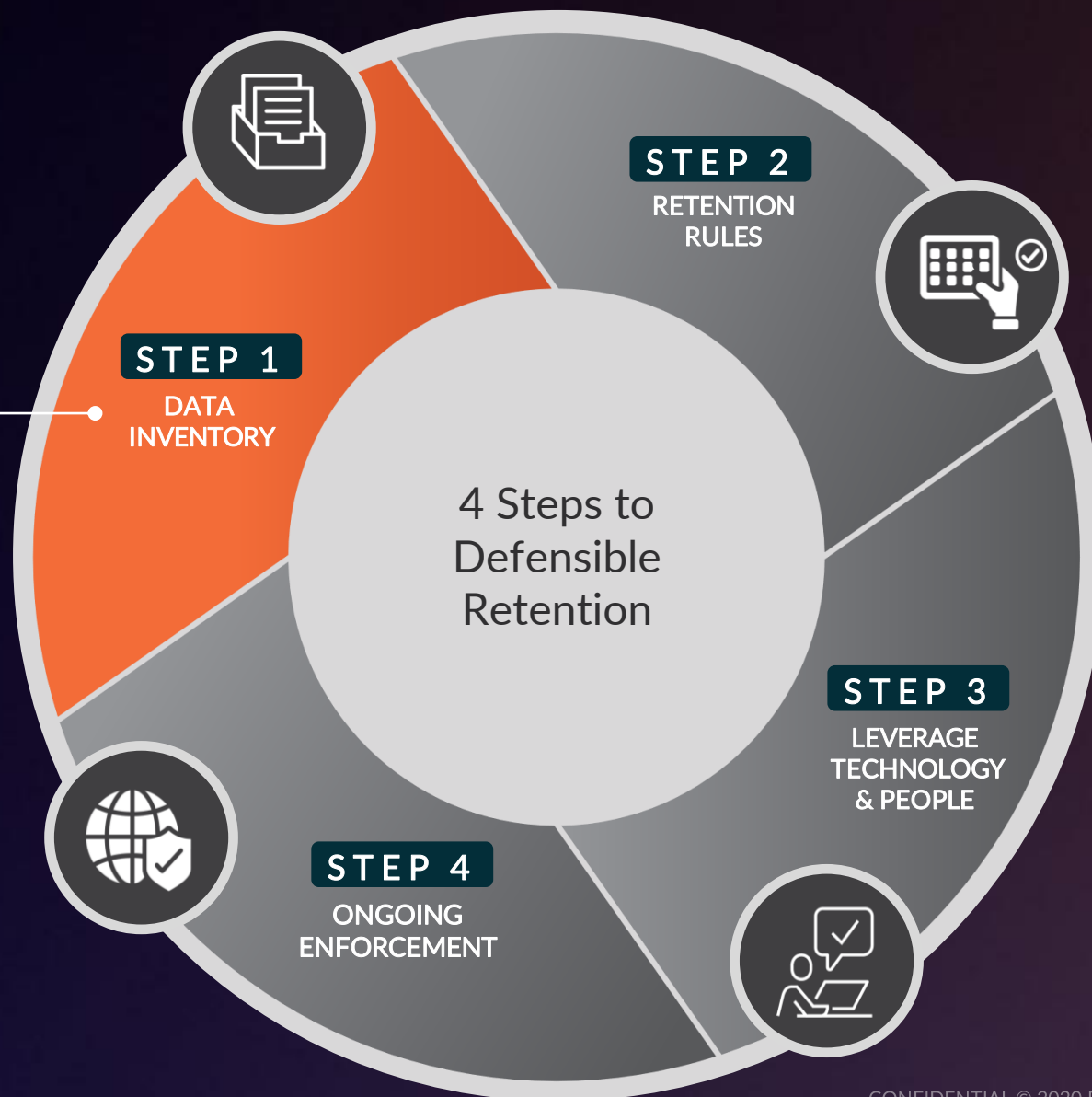
- 1 Know Your Data
- 2 Minimize Your Data
- 3 Consistent Incident Response Process



KNOW YOUR DATA

The Foundation for Defensible Retention & Deletion

- ✓ WHAT DATA YOU HAVE
- ✓ PERSONAL DATA ELEMENTS
- ✓ WHERE IT EXISTS
- ✓ WHO YOU SHARE IT WITH
- ✓ BUSINESS NEEDS
- ✓ RETENTION REGULATIONS

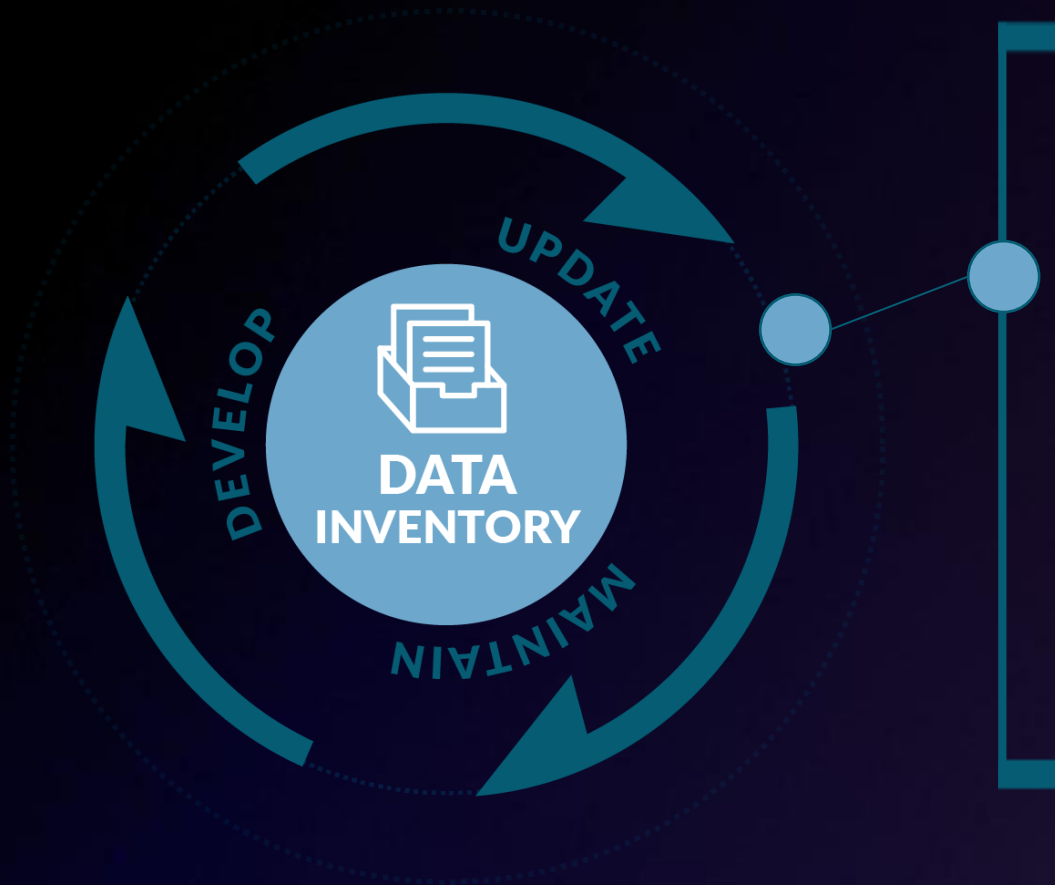


BUSINESS PROCESS

HR - ONBOARDING



Informs Compliance Roadmap



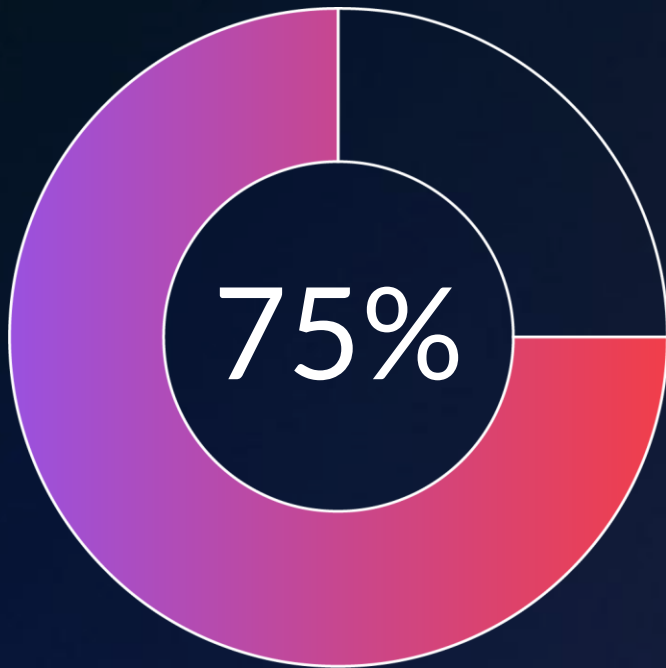
- ✓ DSAR Processes
- ✓ Vendor Risk Profiling
- ✓ Data Retention/Minimization
- ✓ Notices & Disclosures
- ✓ Privacy Policy
- ✓ Employee Privacy Policy
- ✓ Incident Response
- ✓ Vendor Agreements



MINIMIZE YOUR DATA

Data Privacy

Most companies vastly
over-retain records and an
average of



of that contains Personal Data



Minimize
Collection



Dispose when
bargain for
collection has
been fulfilled



How to go from Regulations...

The screenshot shows the official website of the United States Department of Labor, Occupational Safety and Health Administration (OSHA). The header includes the OSHA logo and navigation links. The main content area displays the regulation 1910.1020, titled "Access to employee exposure and medical records." The regulation text is visible, starting with "Purpose." and "Scope and application."

UNITED STATES
DEPARTMENT OF LABOR

Occupational Safety and Health Administration

CONTACT US FAQ A TO Z INDEX ENGLISH ESPAÑOL

OSHA STANDARDS TOPICS HELP AND RESOURCES

SEARCH OSHA

By Standard Number / 1910.1020 - Access to employee exposure and medical records.

- Part Number: 1910
- Part Number Title: Occupational Safety and Health Standards
- Subpart: 1910 Subpart Z
- Subpart Title: Toxic and Hazardous Substances
- Standard Number: 1910.1020
- Title: Access to employee exposure and medical records.
- Appendix: A; B
- GPO Source: e-CFR

1910.1020(a)
"Purpose." The purpose of this section is to provide employees and their designated representatives a right of access to relevant exposure and medical records; and to provide representatives of the Assistant Secretary a right of access to these records in order to fulfill responsibilities under the Occupational Safety and Health Act. Access by employees, their representatives, and the Assistant Secretary is necessary to yield both direct and indirect improvements in the detection, treatment, and prevention of occupational disease. Each employer is responsible for assuring compliance with this section, but the activities involved in complying with the access to medical records provisions can be carried out, on behalf of the employer, by the physician or other health care personnel in charge of employee medical records. Except as expressly provided, nothing in this section is intended to affect existing legal and ethical obligations concerning the maintenance and confidentiality of employee medical information, the duty to disclose information to a patient/employee or any other aspect of the medical-care relationship, or affect existing legal obligations concerning the protection of trade secret information.

1910.1020(b)
"Scope and application."

1910.1020(b)(1)

To Data?

The screenshot shows a 'New Data Set - SQL Query' window. It contains fields for Name, Data Source, and Type of SQL. Below these fields is a 'Query Builder' button and a text area containing a SQL query. The query selects employee information and joins it with department information.

New Data Set - SQL Query

* Name: Employees

* Data Source: demo (Default)






* Type of SQL: Standard SQL

Query Builder

```
select  "EMPLOYEES"."FIRST_NAME" as "FIRST_NAME",
        "EMPLOYEES"."LAST_NAME" as "LAST_NAME",
        "EMPLOYEES"."HIRE_DATE" as "HIRE_DATE",
        "EMPLOYEES"."SALARY" as "SALARY",
        "EMPLOYEES_1"."LAST_NAME" as "MANAGER",
        "DEPARTMENTS"."DEPARTMENT_NAME" as "DEPARTMENT_NAME"
from    "OE"."EMPLOYEES" "EMPLOYEES_1",
        "OE"."DEPARTMENTS" "DEPARTMENTS",
        "OE"."EMPLOYEES" "EMPLOYEES"
where   "EMPLOYEES"."MANAGER_ID"="EMPLOYEES_1"."MANAGER_ID"
and     "EMPLOYEES"."DEPARTMENT_ID"="DEPARTMENTS"."DEPARTMENT_ID"
```

Generate Explain Plan OK Cancel

Global Retention Considerations

Retention Standards By Record Type																	
Benefit Enrollment & Participation Records	Reported Retention -(9), 0(7), 1(1), 2(3), 5(1), PERM(9)																
		AUT 7 BEL 10 BGR 50 CHE 10 CZE 10 DEU 6 DNK 10 ESP 15 EST - FIN 10 FRA 5 GBR 6 HUN 5 IRL 6															
Employee Medical Records	Reported Retention -(8), 0(4), 1(2), 4(1), 5(5), 7(3), 10(3), PERM(16)																
		USA 6 ISL 7 ITA 10 LIE 30 LTU - LUX 30 LVA - NLD 5 NOR 10 POL 10 PRT 20 ROU 10 SVK 3 SW 10 UKR 6															
Employment Equality Compliance Records	Reported Retention -(1), 0(1), 2(1), PERM(2)																
		AUT 25 BEL 10 BGR 5 CHE 10 CZE 3 DEU 10 DNK 10 ESP 15 EST 3 FIN 10 FRA 5 GBR 6 HUN 5 IRL 6															
																	
		USA 10 ISL 4 ITA 10 LIE 30 LTU 10 LUX 30 LVA 10 NLD 5 NOR 10 POL 10 PRT 20 ROU 10 SVK 3 SW 3 UKR 3															



A Clear Path to Data Minimization

DEVELOP

- ✓ Retention Schedules
- ✓ Scheduling Logic
- ✓ Policies
- ✓ Deletion Strategies
- ✓ Hold Process

IMPLEMENT

- ✓ Program Training
- ✓ Attestation
- ✓ Email
- ✓ File Share
- ✓ Structured Data
- ✓ Paper Records

MAINTAIN

- ✓ Audit Trail
- ✓ Documentation
- ✓ Policies
- ✓ Program Monitoring
- ✓ Program Updates
- ✓ Annual Review





CONSISTENT INCIDENT RESPONSE PROCESS

Creating Consistent and Documented Process



EVIDENCE
COLLECTION



CONDITIONAL
WORKFLOWS



REGULATORY
REQUIREMENTS

Questions?



Thank You to Our Panelists!



Robert Fowler,
Director of Strategic Partnerships,
Exterro
Robert.Fowler@Exterro.com



Jena Valdetero,
Shareholder,
Greenberg Traurig, LLP
Valdeteroj@gtlaw.com