>>> NEWSLETTER <<<

>>> SOLEX HR CONSULTING (HRC) <<<

Solex HRC recognizes that managing your employees and growing your business requires a significant amount of time and effort! Many growing businesses do not have an HR professional, or if they do, they are overburdened with compliance tasks and operational projects. Solex HRC can help! By partnering with Solex HRC, you will have a dedicated HR Consultant that meets with you regularly to stay on top of important tasks, compliance items, and employee relation issues. We take the time to meet with you and to understand your business so we can efficiently managing your workforce. Our intention is to keep your employees happy so you can focus on growing your business.

SOLEX QUARTERLY LUNCH & LEARN WEBINAR

PFML - PAID FAMILY MEDICAL LEAVE

WEDNESDAY March 12th @ 12:00pm

Click Here to Register

Join us for a comprehensive webinar on Massachusetts Paid Family Leave (PFML), where we'll cover key aspects of the program, including eligibility, benefits, and how to apply. Whether you're an employee, employer, or HR professional, this session will provide valuable insights to help navigate the ins and outs of PFML. Get your questions answered and learn how this important benefit can support you or your workforce.

HR COMPLIANCE CORNER

ACA - REPORTING COMPLIANCE

The Affordable Care Act (ACA), enacted in 2010, aims to provide affordable health insurance to more Americans and reduce the overall costs of healthcare. Below is an overview of ACA compliance, reporting requirements, and guidelines.

ACA Compliance Requirements For Employers:

- Employer Shared Responsibility: Applicable large employers (ALEs) (those with 50 or more full-time employees or full-time equivalents) are required to offer affordable health insurance that provides minimum essential coverage to their employees and their dependents. Failure to do so may result in penalties (also known as the "Employer Mandate").
- Affordability & Minimum Value: Health plans offered by employers must meet certain standards for affordability and coverage. The monthly premium for the employee's self-only coverage cannot exceed 8.9% of their household income for the 2024 year. Additionally, the plan must cover at least 60% of the total cost of healthcare services.
- Report Health Insurance Coverage: Employers must report the health insurance coverage they provide to the IRS and their employees on forms 1094-C and 1095-C. These reports are used to demonstrate compliance with the ACA's employer mandate and to help determine if employees are eligible for premium tax credits.

ACA Reporting Requirements: Forms and Deadlines

- Form 1095-C: Employers must file Form 1095-C with the IRS and provide a copy to employees by January 31 each year.
- Form 1094-C: This form is the transmittal form for Form 1095-C and must be filed with the IRS by February 28 (if filing on paper) or March 31 (if filing electronically).

ACA Compliance Guidelines set forth by DOL and IRS

- Minimum Essential Coverage: Health plans must offer a set of benefits covering a wide range of health services. This includes preventative care, emergency services, hospitalization, prescription drugs, maternity and newborn care, mental health services, and more.
- Preventive Care: Plans must cover a range of preventive services at no cost to the patient, including vaccinations, screenings, and counseling services.
- Reporting and Documentation: Employers and insurers must keep accurate records of the coverage offered to employees, the plan's affordability, and other relevant details to demonstrate compliance. Failing to maintain these records can result in penalties.
- Health Coverage Notices: Employers must provide certain notices, such as the Marketplace Notice (also called the Exchange Notice), which informs employees about the availability of the Health Insurance Marketplace and how they may qualify for premium subsidies or Medicaid.
- Non-Discrimination: The ACA prohibits discrimination based on health status or medical history. Employers cannot charge higher premiums or refuse coverage based on pre-existing conditions.

Key Considerations for ACA Compliance

- Tracking Hours and Full-Time Employees: Employers must monitor the number of full-time employees (those working 30 or more hours per week) and their eligibility for health insurance.
- Affordable Care Act vs. State Requirements: Some states have their own mandates and may impose stricter requirements. Employers must ensure they comply with both federal and state laws where applicable.
- Changes in Regulations: The ACA is subject to change through administrative actions or legislative amendments. Employers should stay updated on changes that may impact their reporting or compliance requirements.
- ***Employers that fail to comply with ACA requirements may face substantial penalties.***

HR COMPLIANCE CORNER

WISP - WHAT IS IT & WHY SHOULD YOU HAVE ONE

A business should have a Written Information Security Program (WISP) policy for several important reasons, which primarily focus on protecting sensitive data, ensuring legal compliance, and maintaining operational integrity. Key reasons why a business needs a WISP policy:

Data Protection: A WISP helps protect sensitive business and customer data, including personal information, financial records, and intellectual property. By implementing a robust WISP, businesses reduce the risk of data breaches and unauthorized access, ensuring that sensitive information is handled with care.

Regulatory Compliance: Many industries are subject to strict data privacy regulations, such as the GDPR (General Data Protection Regulation), HIPAA (Health Insurance Portability and Accountability Act), and CCPA (California Consumer Privacy Act). A WISP ensures that businesses comply with these regulations, avoiding fines, penalties, and reputational damage.

Risk Management: A WISP helps businesses assess and mitigate information security risks. It provides clear guidelines on identifying, evaluating, and managing potential threats, including cyberattacks, data leaks, and system vulnerabilities.

Incident Response Preparedness: A WISP outlines procedures for identifying, responding to, and recovering from security incidents. Having a documented response plan in place helps businesses respond quickly and effectively to breaches, reducing the potential damage and downtime.

Employee Awareness and Training: A well-defined WISP policy includes employee training programs on information security best practices. Employees are often the weakest link in security, so educating them on how to handle data securely, recognize phishing attempts, and follow security protocols is critical.

Business Continuity: In case of a data breach or cyberattack, a WISP ensures that there is a clear process for maintaining business operations. The policy includes backup and recovery procedures to protect business continuity, ensuring that essential services and operations are not interrupted.

Client and Stakeholder Trust: Having a WISP in place demonstrates a commitment to safeguarding sensitive data and maintaining a secure environment. This fosters trust with customers, partners, investors, and stakeholders, which is crucial for maintaining long-term business relationships.

Legal Liability Reduction: In the event of a security breach, businesses that lack a WISP could face lawsuits or other legal actions due to negligence. A WISP shows that the business has taken reasonable steps to secure its data and can defend against legal claims related to security failures.

Cybersecurity Insurance: Some insurers may require businesses to have a WISP in place to qualify for cybersecurity insurance or to reduce premiums. Having a policy in place demonstrates proactive risk management and can lower the financial impact in case of a security breach.

Continuous Improvement: A WISP is not static but should evolve over time. It encourages businesses to regularly evaluate and update their security measures, ensuring they stay ahead of emerging threats and industry best practices. This continuous improvement fosters long-term resilience.

HR COMPLIANCE CORNER

MASSACHUSETTS PAY TRANSPARENCY

When do employer requirements take effect?

Wage reporting under the Massachusetts Pay Transparency Act requires employers with over 100 employees to submit wage data reports by 02/01/2025. Additionally, employers with 25 or more employees will be required to post pay transparency data (salary ranges for positions) on all job postings effective 02/01/2025.

Wage Data Reporting:

The required contents of the wage data reports are employer-specific, and different types of employers have different requirements. The requirement applicable to larger employers is the EEO-1 data report (which such employers are (or should be) already filing federally each year).

These employers must file a completed copy of all required components of its Employer Information Report, as issued by the US Equal Employment Opportunity Commission, including any successor report containing the same or substantially similar workforce demographic and pay data categorized by race, ethnicity, sex, and job category. An employer subject to the EEO-1 data filing requirement must submit its report for the prior year to the Secretary of the Commonwealth annually by 02/01/2025 as referenced above.

Compensation information in Job Postings:

A pay range is the annual salary range or hourly wage range that the covered employer reasonably and in good faith expects to pay for such position at the time. A “job posting” is any job posting or advertisement intended to recruit job applicants for a specific job, including both recruitments directly by the employer or indirectly through a third party.

Separately, current employees will be allowed to request the pay range for their current position and when the employer promotes or transfers the employee to a new position with different job responsibilities.

Enforcement and Liability:

The Bill imposes a prohibition on retaliation and discrimination. An employer is not allowed to retaliate or discriminate against an employee or applicant for:

1) pursuing their rights under the Act;
2) making a complaint regarding an alleged violation of the Act;
3) instituting any proceeding under the Act; or
4) testifying in any such proceeding.

The attorney general has exclusive jurisdiction to enforce the Act’s anti-retaliation provisions and may obtain injunctive or declaratory relief. For a first-time violation, an employer receives a warning; for a second offense, the employer is fined up to $500 dollars; for a third offense, the employer is fined up to $1,000 dollars; and for a fourth and subsequent offense the employer is subject to the penalties in M.G.L. c. 149, section 27(c). Violating this section does not carry treble damages.

HR QUESTION OF THE MONTH

What is the IRS Milage Rate Increase for 2025?

The standard mileage rate for 2024 for the use of a car, van, pickup, or panel truck is 67 cents for every mile of business travel driven. For 2025, the rate is 70 cents per mile.