2019

Employee Benefit Technology and Compliance

Presented by Benefit Comply

- Welcome! We will begin at 3 p.m. Eastern
- There will be no sound until we begin the webinar. When we begin, you can listen to the audio portion through your computer speakers or by calling into the phone conference number provided in your confirmation email.
- You will be able to submit questions during the webinar by using the “Questions” or “Chat” box located on your webinar control panel.
- Slides can be printed from the webinar control panel – expand the “Handouts” section and click the file to download.

Assurex Global Partners

- Bolton & Co.
- Catto & Catto
- Cottingham & Butler
- Cragin & Pike, Inc.
- Daniel & Henry
- Foa & Son
- The Graham Co.
- Haylor, Freyer & Coon, Inc.
- Henderson Brothers, Inc.
- The Horton Group
- The IMA Financial Group
- INSURICA
- Kapnick Insurance Group
- Lanier Upshaw, Inc.
- Lipscomb & Pitts Insurance
- LMC Insurance & Risk Management
- Lyons Companies
- The Mahoney Group
- MJ Insurance
- Oswald Companies
- Parker, Smith & Feek, Inc.
- PayneWest Insurance
- Pritchard & Jerden
- R&R/The Knowledge Brokers
- RCM&D
- The Rowley Agency
- Starkweather & Shepley
- Sterling Seacrest Partners
- Woodruff Sawyer

Agenda

- How Technology can Assist with Required Notices and Disclosures
- Using Technology to Assist with Other Compliance Obligations
- Compliance Risks and Challenges Related to Technology
- Technology Thoughts and Ideas

How Technology Can Help With Required Notices and Disclosures

Notices and Disclosures

- DOL ERISA Rules vs. IRS Electronic Delivery of Benefit Information Rules
  - Requirements are similar but IRS rules may not be sufficient for ERISA documents
- IRS Electronic Delivery Rules
  - Applies to “participant elections,” which include consents, elections, requests, agreements, or similar communications made by a participant or other individual entitled to plan benefits
    - Section 125 plans, HSAs, Transportation plans, Section 129 Dependent Care plans
- DOL Safe Harbor for Electronic Delivery or ERISA Notices and Disclosures
  - The DOL's electronic disclosure safe harbor applies to a wide array of ERISA-required documents including SPDs, SMMs, and SARs for all ERISA plans, as well as QMCSO notices,
  - Also May be Appropriate to Notices Other that ERISA specific
    - COBRA notices, HIPAA Notice of Special Enrollment Rights, Notice of Exchange

Notices and Disclosures

- IRS Electronic Delivery Rules -Two Methods
- Method 1 - Follows the “consumer consent” rules of E-SIGN
  - Requires that a plan obtain a recipient's affirmative consent before providing an electronic notice
    - Before consenting, a disclosure must be provided; (1) right to obtain a paper document; (2) right to withdraw consent; (3) the scope of the consent and procedures for updating information; and (5) system requirements
    - Due to complexity, this method more often used for non-employees (e.g., former employees or dependents).
- Method 2 - Less Complicated
  - Requires that participants;
    - Have the “effective ability to access” the electronic medium being used to provide the notice
    - Are advised that they can request a paper version of the notice at no charge
    - Are alerted at the time of notice to its significance and are provided instructions needed to access the notice
  - “Effective ability to access” will depend on the particular facts and circumstances;
    - Regular use of system for job
    - May be met by use of information kiosks where employees do have regular electronic access
  - No prior consent required

Notices and Disclosures

- DOL Safe Harbor for Electronic Delivery or ERISA Notices and Disclosures
  - The DOL safe harbor generally allows electronic distribution if an employee;
    - (i) has access to a computer at their regular workplace as part of their everyday duties, or
    - (ii) if the employee consents to electronic delivery
  - "Access to a computer at their regular workplace"
    - Ability to access electronic documents where employee performs their duties
    - Includes employees who work at home or travel, if they regularly access employer's information system
    - Access to workplace kiosks in common areas is not sufficient (e.g., lunchroom or human resources offices)
    - Employees who do not meet these criteria must be provided a paper copy of required ERISA notices and disclosures
  - Notification
    - When providing notices electronically each participant must be notified (in electronic or other means)
      - (i) the documents that are being distributed electronically
      - (ii) the significance of the documents
      - (iii) the right to request a paper copy of the document from the plan administrator.

Notices and Disclosures

- DOL Safe Harbor for Electronic Delivery or ERISA Notices and Disclosures
  - Posting on Website
    - The safe harbor applies to disclosures on a company's website
      - Provide a written or electronic notice to employees directing them to the website at the time the document is posted describing its significance and the right to request a paper copy at no charge
      - Take “appropriate and necessary” measures to make sure the posting on a company's website results in actual receipt could including:
        - Adding a prominent link from the website's homepage to the separate section that contains the information
        - providing directions on the website for how to replace a lost or forgotten password
        - maintaining the documents on the website for a reasonable period of time
  - DOL Safe Harbor does not override other rules
    - Who must receive the notice or disclosure – e.g. SPD to employee only but initial COBRA notice must be sent to covered spouses (more later)

Notices and Disclosures

- Summary of Benefits and Coverage (SBC) Delivery
  - For participants covered by the plan
    - Can follow DOL safe-harbor for ERISA documents
    - Alternatively – allowed to use online enrollment system
      - DOL allows SBCs to be provided electronically to participants and beneficiaries in connection with online enrollment or renewal of coverage under the plan
      - The individual must still have the option to receive a paper copy of the SBC upon request
  - For participants eligible but not enrolled
    - SBC may be provided via Internet
      - Individuals must be notified in paper form or via email that the documents are available on the Internet
      - The postcard or email must provide the Internet address and indicate that the documents are available in paper form upon request
  - Uniform Glossary of Terms
    - In either case a link to DOL or HHS can be provided to the required Uniform Glossary

Notices and Disclosures

- IRS Electronic Distribution of 1095s and W-2s
  - Different than IRS benefits rules mentioned earlier
  - Employer must get employees consent to receive electronically
    - An individual may consent on paper or electronically
    - A statement may be furnished electronically by email or by informing the individual how to access the statement on the employer's site
  - The consent must relate specifically to receiving the Form 1095 or W-2 electronically
    - Employees who previously consented to receive Form W-2 electronically but that consent did not specifically identify Form 1095 must provide a separate consent to receive Form 1095 electronically

Notices and Disclosures

- HIPAA Notice of Privacy Practice (NPP)
  - Background
    - Employer sponsored health plans, not the employer itself (unless employer is a medical provider), is the covered entity
      - Medical, Dental, Health FSA, HRA, Rx, etc.
      - Employer can delegate delivery of NPP to carrier –however – carrier typically does not provide NPP for all of employer's plan subject to HIPAA
    - The NPP must be individually delivered, posting on a website is not sufficient
    - May include the privacy notice with other materials such as SPD or enrollment materials.
  - Electronic Delivery
    - NPP can be provided by email if the recipient has agreed to receive an electronic notice
    - If the covered entity knows that the email transmission has failed, a paper copy must be provided.
  - If Covered Entity has a website NPP must be posted on website
    - Applies to providers and insurance companies
    - Most employers are not a covered entity in its capacity as group health plan sponsor
      - An typical employer does not have to post its plan NPP on the general company website

Notices and Disclosures

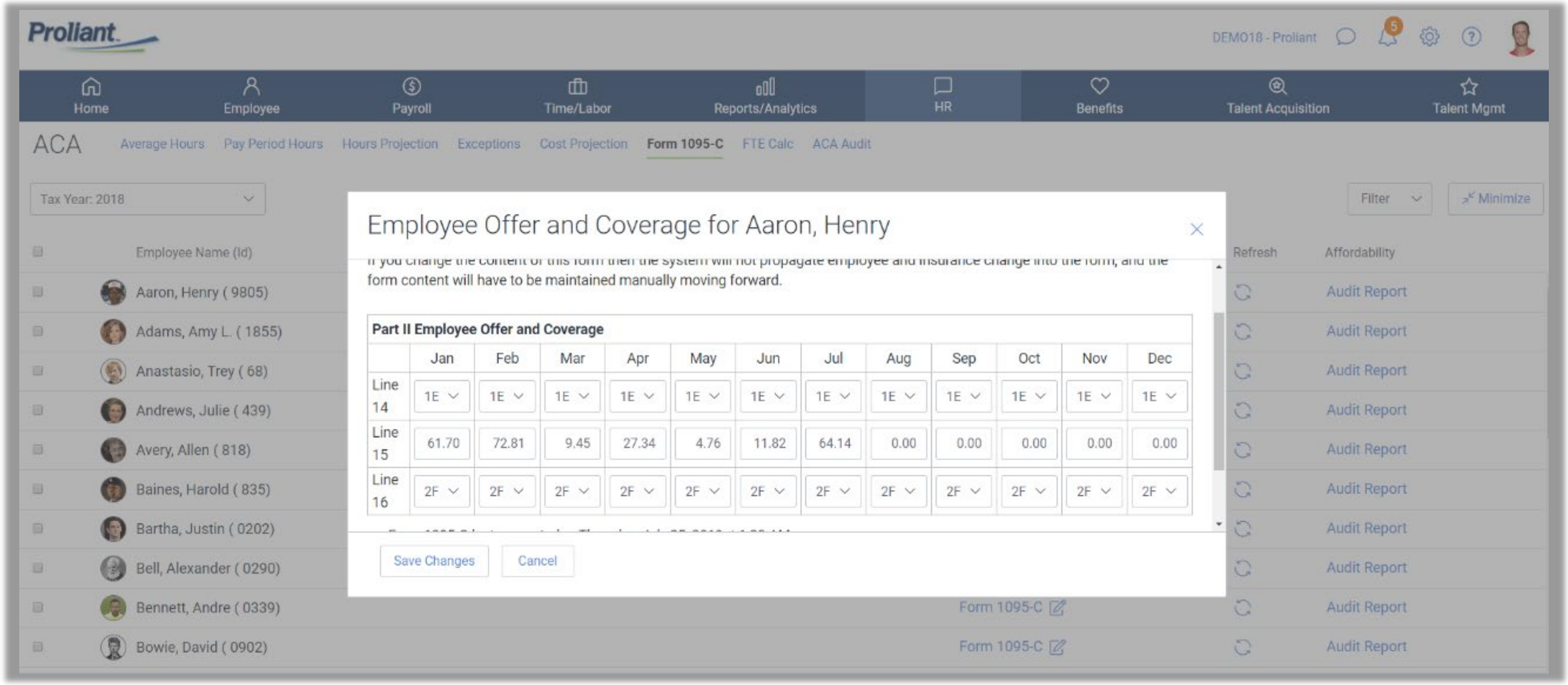
- Thoughts on Other Notices and Disclosures
  - HIPAA Special Enrollment Notice
    - Must be provided with enrollment material PRIOR to enrollment
    - Can follow the DOL safe-harbor for ERISA docs
    - Must also be included in SPD
  - COBRA Notices
    - Initial COBRA notice
      - Must be provided to all new covered employees AND spouses
      - Can follow DOL Safe-harbor for ERISA docs for employees, but that often will not fulfill employer's obligation to notify covered spouses

Using Technology to Assist with Compliance Obligations

Employee Tracking and Administration

- §4980H Employer Shared Responsibility Rules
  - Tracking Full-time employee status - Full-time can be defined using monthly or look-back measurement period method
    - Using payroll systems
    - Using separate tracking system integrated with time or payroll data
  - Employer Reporting
    - System choices
      - Integrated vs. stand-alone
      - Technology only vs. full-service
      - Bigger is not always better
  - “Proof” of offer of coverage
    - Signed waivers not required but documentation of an offer of coverage is important

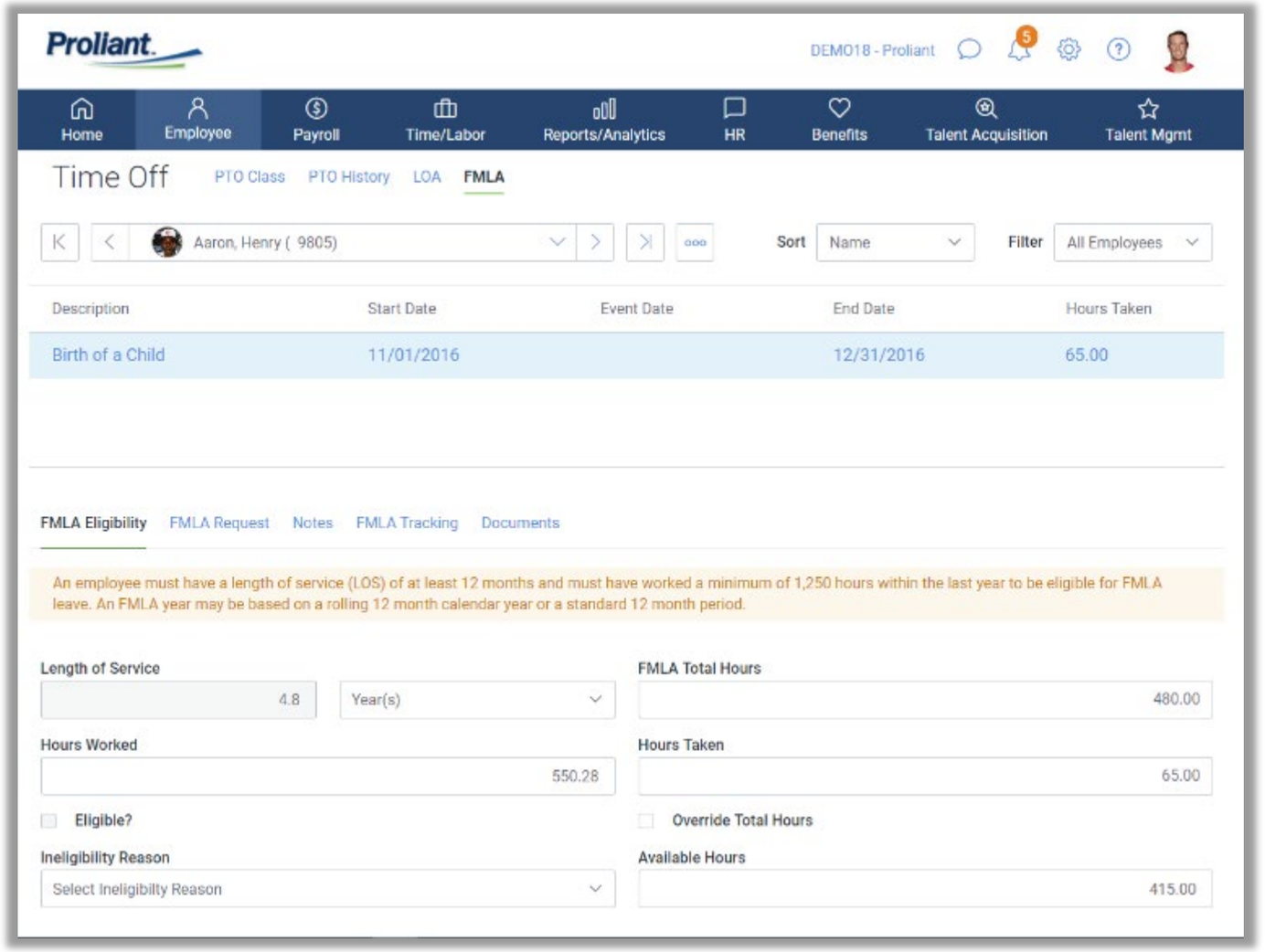
ACA Audit


Prollant
DEMO18 - Prollant
Home
Employee
Payroll
Time/Labor
Reports/Analytics
HR
Benefits
Talent Acquisition
Talent Mgmt
ACA
Average Hours
Pay Period Hours
Hours Projection
Exceptions
Cost Projection
Form 1095-C
FTE Calc
ACA Audit
Tax Year: 2018
Filter
Minimize
Employee Name (Id)
Refresh
Affordability
Aaron, Henry (9805)
Adams, Amy L. (1855)
Anastasio, Trey (68)
Andrews, Julie (439)
Avery, Allen (818)
Baines, Harold (835)
Bartha, Justin (0202)
Bell, Alexander (0290)
Bennett, Andre (0339)
Bowie, David (0902)
Audit Report
Form 1095-C
Employee Offer and Coverage for Aaron, Henry
form content will have to be maintained manually moving forward.
Part II Employee Offer and Coverage
Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec
Line 14 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E
Line 15 61.70 72.81 9.45 27.34 4.76 11.82 64.14 0.00 0.00 0.00 0.00 0.00
Line 16 2F 2F 2F 2F 2F 2F 2F 2F 2F 2F 2F 2F
Save Changes
Cancel

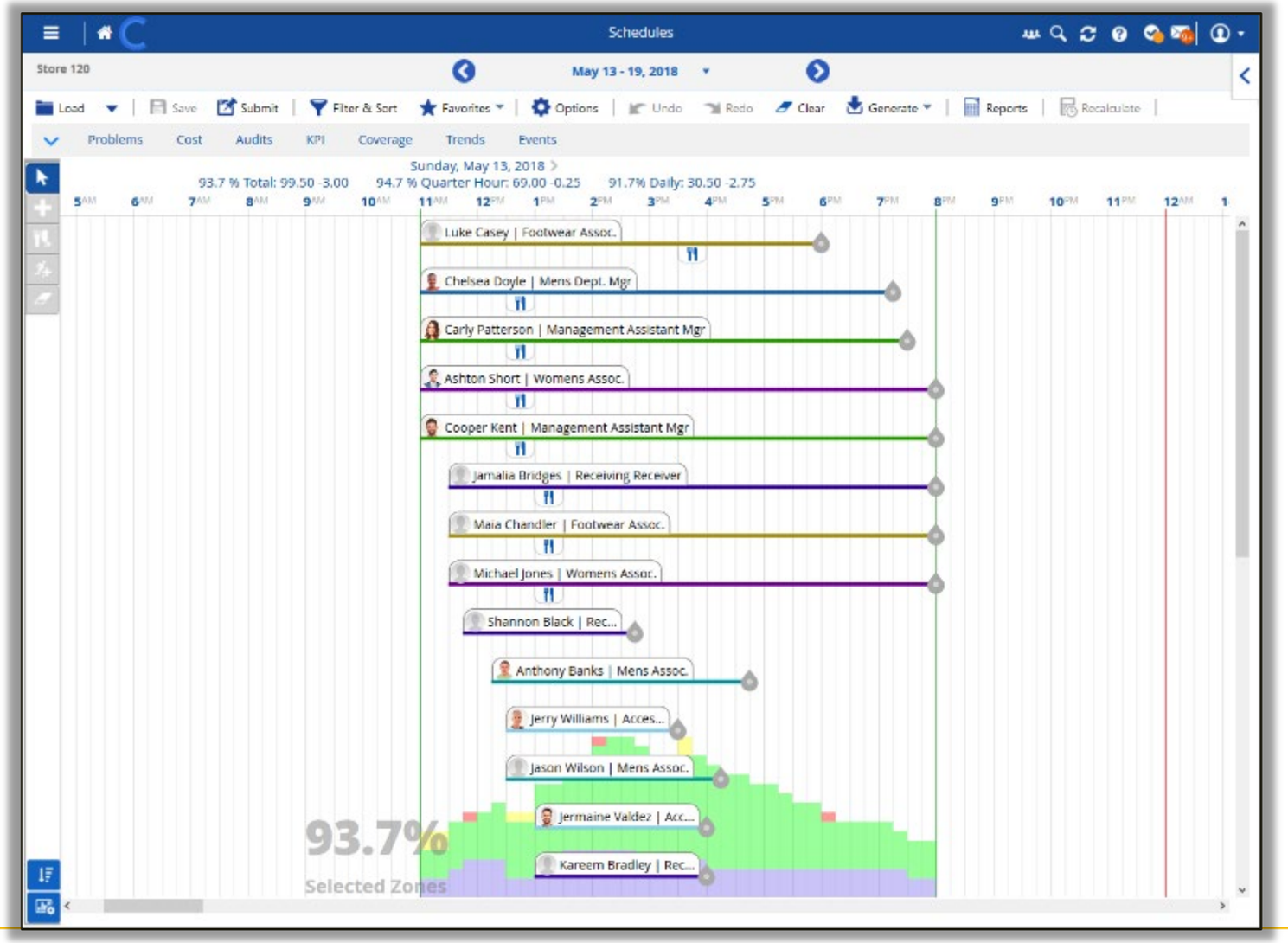
Employee Tracking and Administration

- A Few Words on Broader HR Technology Support
  - Onboarding Employees
    - I-9 & e-Verify
    - Capture consent for various notices
  - Employer Reporting
    - EEOC
    - Workers Comp
    - OSHA
    - FMLA
  - Benefit Disclosures

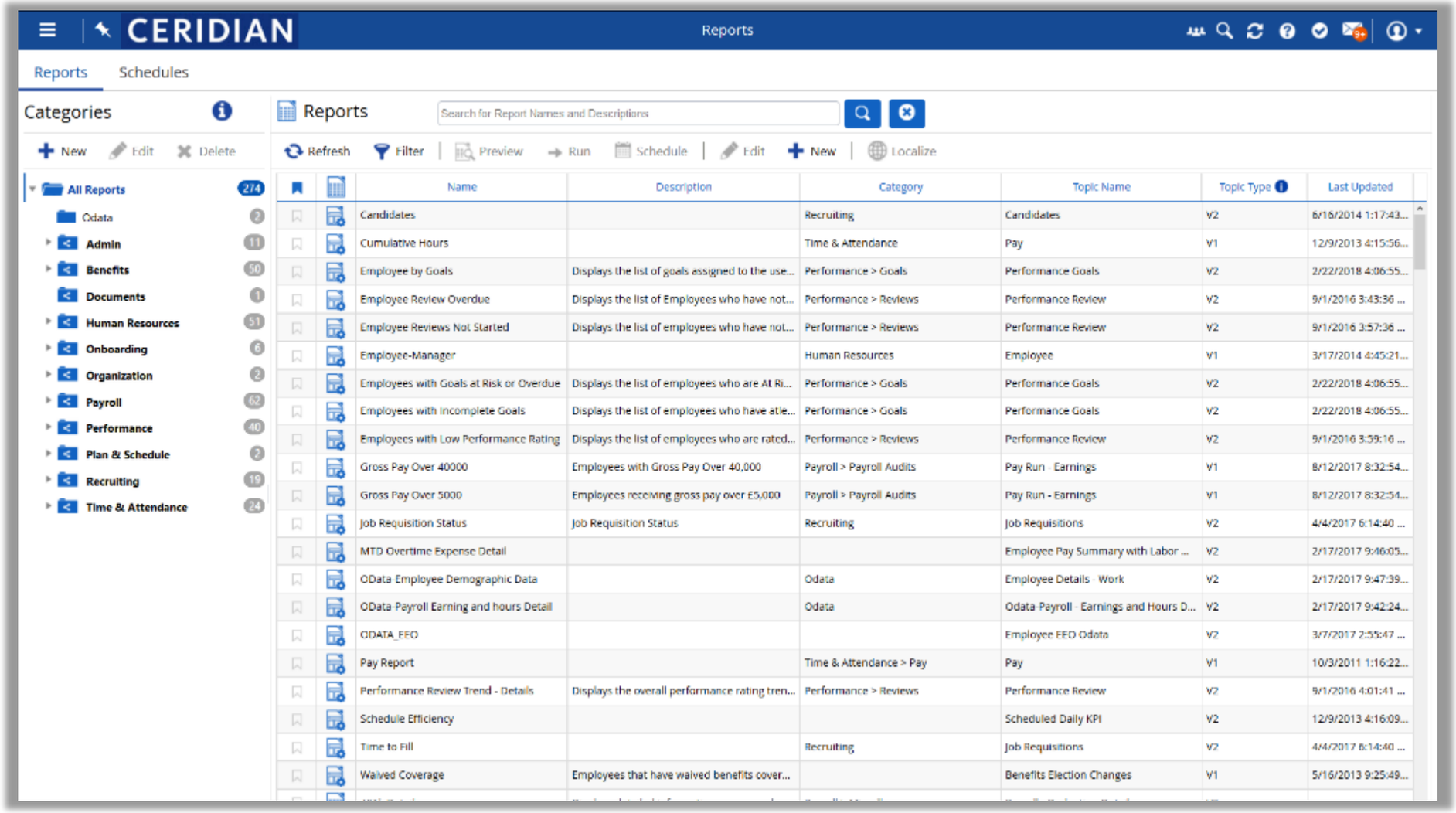
FMLA Tracking



Time & Attendance



Reporting


CERIDIAN
Reports
Reports
Schedules
Categories
New
Edit
Delete
All Reports 274
Odata 2
Admin 11
Benefits 50
Documents 1
Human Resources 51
Onboarding 6
Organization 2
Payroll 62
Performance 40
Plan & Schedule 2
Recruiting 19
Time & Attendance 24
Reports
Search for Report Names and Descriptions
Refresh
Filter
Preview
Run
Schedule
Edit
New
Localize
Name
Description
Category
Topic Name
Topic Type
Last Updated
Candidates
Recruiting
Candidates
V2
6/16/2014 1:17:43...
Cumulative Hours
Time & Attendance
Pay
V1
12/9/2013 4:15:56...
Employee by Goals
Displays the list of goals assigned to the use...
Performance > Goals
Performance Goals
V2
2/22/2018 4:06:55...
Employee Review Overdue
Displays the list of Employees who have not...
Performance > Reviews
Performance Review
V2
9/1/2016 3:43:36 ...
Employee Reviews Not Started
Displays the list of employees who have not...
Performance > Reviews
Performance Review
V2
9/1/2016 3:57:36 ...
Employee-Manager
Human Resources
Employee
V1
3/17/2014 4:45:21...
Employees with Goals at Risk or Overdue
Displays the list of employees who are At Ri...
Performance > Goals
Performance Goals
V2
2/22/2018 4:06:55...
Employees with Incomplete Goals
Displays the list of employees who have atle...
Performance > Goals
Performance Goals
V2
2/22/2018 4:06:55...
Employees with Low Performance Rating
Displays the list of employees who are rated...
Performance > Reviews
Performance Review
V2
9/1/2016 3:59:16 ...
Gross Pay Over 40000
Employees with Gross Pay Over 40,000
Payroll > Payroll Audits
Pay Run - Earnings
V1
8/12/2017 8:32:54...
Gross Pay Over 5000
Employees receiving gross pay over £5,000
Payroll > Payroll Audits
Pay Run - Earnings
V1
8/12/2017 8:32:54...
Job Requisition Status
Job Requisition Status
Recruiting
Job Requisitions
V2
4/4/2017 6:14:40 ...
MTD Overtime Expense Detail
Employee Pay Summary with Labor ...
V2
2/17/2017 9:46:05...
OData Employee Demographic Data
Odata
Employee Details - Work
V2
2/17/2017 9:47:39...
OData Payroll Earning and hours Detail
Odata
Odata Payroll - Earnings and Hours D...
V2
2/17/2017 9:42:24...
ODATA_FED
Employee FED Odata
V2
3/7/2017 2:55:47 ...
Pay Report
Time & Attendance > Pay
Pay
V1
10/3/2011 1:16:22...
Performance Review Trend - Details
Displays the overall performance rating tren...
Performance > Reviews
Performance Review
V2
9/1/2016 4:01:41 ...
Schedule Efficiency
Scheduled Daily KPI
V2
12/9/2013 4:16:09...
Time to Fill
Recruiting
Job Requisitions
V2
4/4/2017 6:14:40 ...
Waived Coverage
Employees that have waived benefits cover...
Benefits Election Changes
V1
5/16/2013 9:25:49...

Compliance Risks and Challenges Related to Technology

HIPAA and Data Security

- HIPAA Security Rules
  - Security Rule requires covered entities and business associates to implement safeguards to protect the confidentiality, integrity, and availability of ePHI (i.e., PHI that is transmitted or maintained electronically)
  - Covered entities include employer sponsored health plans
    - Medical, dental, HRA, Health FSA, etc.
    - All employers who sponsor a self-insured (and many fully-insured) plans must comply with HIPAA security rules
  - Entities must address a specific set of security standards and implementation specifications
    - First step is a risk analysis to identify known or potential gaps in security
    - Based on results of risk analysis, entities must implement appropriate controls
    - Standards are the same for all entities, but flexible - An entity's security measures will depend on its size, organizational structure, and risks to ePHI
    - Entities must have written HIPAA policies and procedures
  - Centers for Medicare and Medicaid Services (CMS) does random audits

HIPAA and Data Security

- HIPAA Breaches
  - Definition of Breach
    - …“the acquisition, access, use, or disclosure of PHI in a manner not permitted under HIPAA which compromises the security or privacy of the PHI”
    - Must constitute a violation of the Privacy or Security Rule
    - Limited exceptions apply (unintentional access by employees; certain inadvertent disclosures, etc.)
  - Breach is assumed to have occurred unless plan can demonstrate a low probability that PHI has been compromised using Four-Factor analysis:
    - Nature and extent of PHI involved, including types of identifiers and likelihood of re-identification
    - Unauthorized person to whom unauthorized disclosure was made
    - Whether the PHI was actually viewed or accessed
    - Extent to which risk to PHI can be mitigated
  - Breach reporting and notifications
    - Participants whose PHI was part of breach much be notified
    - All breaches must be reported breaches to CMS (additional reporting requirements for large breaches)

HIPAA and Data Security

- Common Areas of HIPAA Security Risk
  - Emailing ePHI
    - Encryption protects an email while it is in transit
    - Some encryption technologies don't prevent any end user from creating an account and accessing the email
    - Examples of risks:
      - An unencrypted email containing ePHI could be intercepted by a malicious third party
      - An encrypted email containing ePHI that is sent to the wrong recipient could still be a breach
  - Malware in email
    - Email is one of the most common ways for malware to infect system
    - Phishing (tricking user into divulging confidential information) and spoofing (posing as email from trusted sender) especially common
    - Examples of risks:
      - User provides login credentials to "Windows support" to "help resolve an issue"
      - User receives email from "business colleague" and clicks on attachment that contains malware

New Technologies

- Virtual Health Care Delivery - Telehealth and e-Visits
  - Regulations have not kept up with innovation
  - Telehealth and e-visits that provide care beyond preventive can make an employee ineligible for HSA contributions
- Increased Use of Portable Devices
  - Entities should evaluate use of mobile devices (especially any Bring Your Own Device (BYOD policies)
  - Consider all portable devices (phones, tablets, USB drives, laptops, etc.)
    - Lost or stolen unencrypted device that is used to access email containing ePHI
    - Improper disposal of devices

Technology Horror Stories

- Technology Horror Stories
  - Employer Reporting Horror Stories
    - Employer failure to audit or review employer reporting systems output
    - Many employers assumed that systems would report properly after completing “employer information” required by system
  - Employers trying to build systems internally
    - Example – trying to build internal WC report for auditor
  - Failure to manage separate systems involved in one “process”
    - Often employer policies and procedures fall down with coordinating interaction between separate systems
    - Example – employee contributions taken from payroll, but plan enrollment never happened
  - Relying on technology based on a “brand”
    - Employer not having the expertise to vet systems, so they buy a “name brand”
    - Just because a system is good at payroll processing does not mean it is a good employer reporting system

Additional Technology Considerations

HRIS vs BenAdmin Thoughts

- Integrated Payroll or HRIS system vs. Stand-alone Benefits Administration (BenAdmin)
  - Benefits decision support
  - Subject matter expertise - true employee benefits support
  - Outsourced capabilities such as benefits call-center
  - Employee expectation
    - Employees are expecting a better online experience in the employee's online access
- Not all BenAdmin Systems are the Same
  - Outsource Services
  - Decision Support
  - Configuration
  - Billing/Reconciliation

Vendor Security & Best Practices

- Assessing Vendor Security
  - Local vs Cloud
  - Historically most systems were managed internally on-site - now most are in the cloud – how do you validate that the vendor is handling security
  - Assessing vendor in a larger project (costs, functionality, etc.) and sometimes vendor security is not considered carefully enough.
  - Has the vendor completed a SOC audit?
    - Employer may not understand the SOC audit – if the system really matters – you may need professional help
  - Multi-Factor Authentication (MFA)

Assurex Global Partners

- Bolton & Co.
- Catto & Catto
- Cottingham & Butler
- Cragin & Pike, Inc.
- Daniel & Henry
- Foa & Son
- The Graham Co.
- Haylor, Freyer & Coon, Inc.
- Henderson Brothers, Inc.
- The Horton Group
- The IMA Financial Group
- INSURICA
- Kapnick Insurance Group
- Lanier Upshaw, Inc.
- Lipscomb & Pitts Insurance
- LMC Insurance & Risk Management
- Lyons Companies
- The Mahoney Group
- MJ Insurance
- Oswald Companies
- Parker, Smith & Feek, Inc.
- PayneWest Insurance
- Pritchard & Jerden
- R&R/The Knowledge Brokers
- RCM&D
- The Rowley Agency
- Starkweather & Shepley
- Sterling Seacrest Partners
- Woodruff Sawyer