LANE POWELL

Privacy and Data Security for Senior Living & Long Term Care Employers: Cyber Threats in Your Workplace

Jeff Duncan Brecht, Shareholder
brechtj@lanepowell.com / 503.778.2162
Lane Powell PC

March 1, 2018: OHCA Spring 2018

Disclaimer

This presentation reflects the views of its author, which are not necessarily the views of OHCA, or Lane Powell PC.

It is intended to provide general information only.

It is not intended to provide any legal opinions or advice applicable to any particular situation, and does not create an attorney-client relationship with any attendee or reader.

If you would like more information regarding whether we may assist you in any particular matter, please contact one of our attorneys, using care not to provide us any confidential information until we have notified you in writing that there are no conflicts of interest and that we have agreed to represent you on the specific matter that is the subject of your inquiry.

WHAT'S AT STAKE FOR SL / LTC EMPLOYERS?

Public Relations Problems

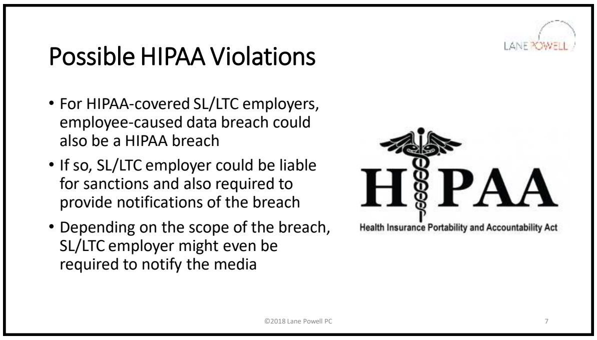
- Most states, including Oregon, require businesses (which could include SL/LTC employers) to notify their "customers" as soon as possible if there has been a data security breach. (See ORS 646A.600 - 646A.628).
- Depending on the scope of the breach, employer may also be required to notify the Oregon Attorney General.

Lawsuits - Residents

Where employee's employment-related conduct discloses "customers'" (i.e., residents) private data, SL/LTC employer could be named as a defendant in a lawsuit brought by the customer whose private information was disclosed.

Resident Rights - Privacy

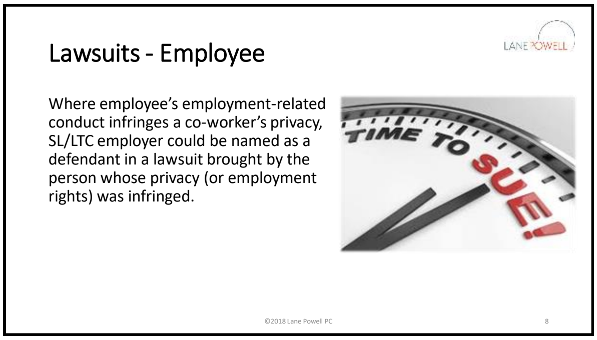
- NF - 411-085-0310: "Each resident and the resident's legal representative, as appropriate, have the right to:
  - ➢be treated with consideration, respect, and dignity and assured complete privacy during treatment and when receiving personal care."
  - ➢be provided privacy for visits when requested, including meetings with other residents and family groups."
- ALF - 411-054-0027: "The Bill of Rights must state that residents have the right:
  - ➢to receive services in a manner that protects privacy and dignity."



Possible HIPAA Violations

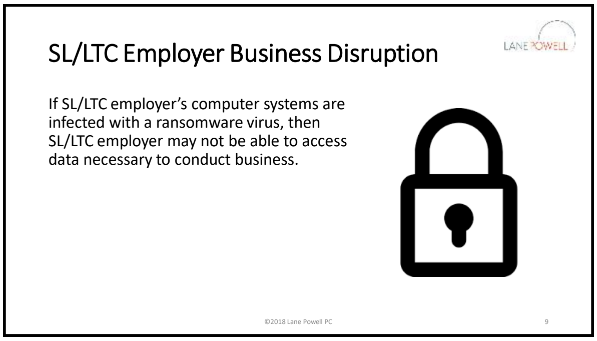
- For HIPAA-covered SL/LTC employers, employee-caused data breach could also be a HIPAA breach
- If so, SL/LTC employer could be liable for sanctions and also required to provide notifications of the breach
- Depending on the scope of the breach, SL/LTC employer might even be required to notify the media

HIPAA
Health Insurance Portability and Accountability Act



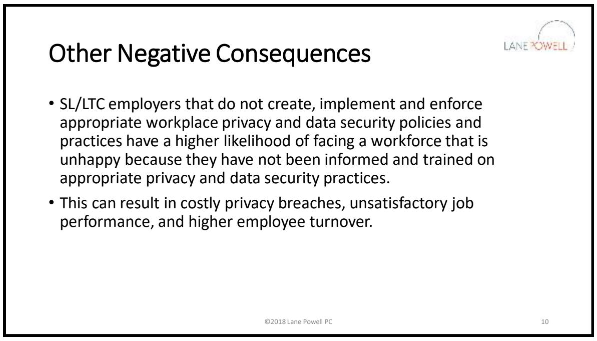
Lawsuits - Employee

Where employee's employment-related conduct infringes a co-worker's privacy, SL/LTC employer could be named as a defendant in a lawsuit brought by the person whose privacy (or employment rights) was infringed.



SL/LTC Employer Business Disruption

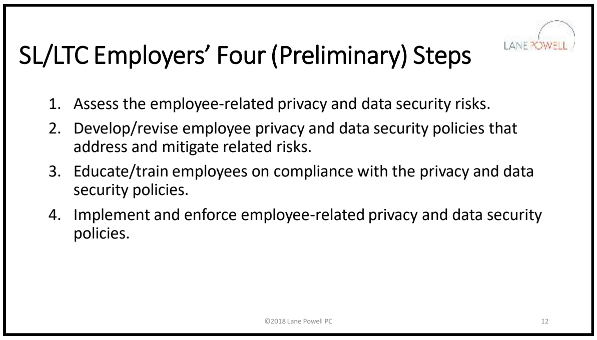
If SL/LTC employer's computer systems are infected with a ransomware virus, then SL/LTC employer may not be able to access data necessary to conduct business.



Other Negative Consequences

- SL/LTC employers that do not create, implement and enforce appropriate workplace privacy and data security policies and practices have a higher likelihood of facing a workforce that is unhappy because they have not been informed and trained on appropriate privacy and data security practices.
- This can result in costly privacy breaches, unsatisfactory job performance, and higher employee turnover.

So…



SL/LTC Employers' Four (Preliminary) Steps

1. Assess the employee-related privacy and data security risks.
2. Develop/revise employee privacy and data security policies that address and mitigate related risks.
3. Educate/train employees on compliance with the privacy and data security policies.
4. Implement and enforce employee-related privacy and data security policies.

Step One: Assess Employee-Related Privacy and Data Security Risks

- Use the information garnered from this employee-related privacy and data security risk assessment process to create and implement policies that most effectively fit your workplace.

What questions should SL/LTC employers ask?

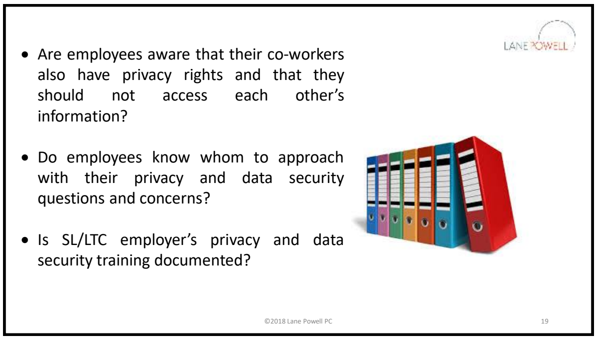
- SL/LTC Employers should modify their assessment to best fit their particular circumstances
- In general, SL/LTC employers should include at least the following queries in their employee-related privacy and data security risk assessment:

- What policies are in place to make sure that only employees who need to have access to private data have access to that data?
- Do employees use their own laptops, tablets and smart phones related to the work duties?
- Do employees have non-public workspaces where they may privately discuss customer matters?
- What password policies and practices must employees comply with?

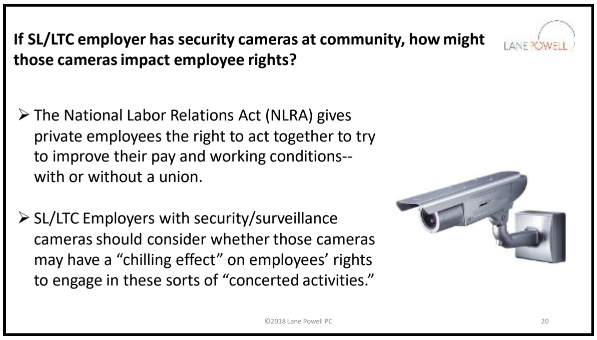
- Does SL/LTC employer require employees to utilize encryption technology to protect private data?
- Are employees required to promptly remove and secure materials from printers and fax machines?
- Do employees log-out of workstation computers, tablets, and laptops before they step away?
- How quickly (if at all) do employee workstation computers, tablets, and laptops "auto-lock" when those devices are inactive?

- Do employees share work-related passwords?
- Do employees transport private, work-related information in their vehicles?
- Do employees use laptops and other devices that contain private, work-related information at their homes, coffee shops, or elsewhere offsite?
- Is private, work-related information visible to residents, families/visitors or the public at employee workstations?

- What training is provided to employees regarding privacy and data security policies and practices?
- Do employees verify email addresses and fax numbers before transmitting private information?
- Does SL/LTC employer regularly review and update its employee-related privacy and data security policies?
- How do employees report violations of SL/LTC employer's employee-related privacy and data security policies?

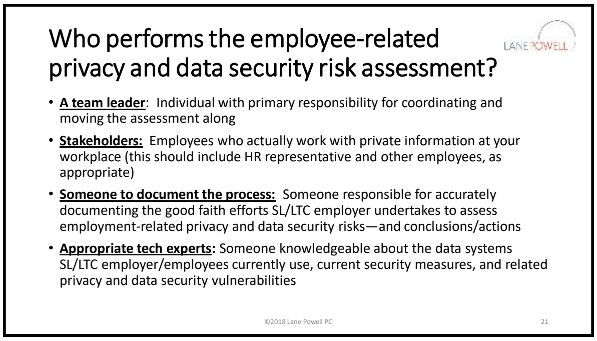


- Are employees aware that their co-workers also have privacy rights and that they should not access each other's information?
- Do employees know whom to approach with their privacy and data security questions and concerns?
- Is SL/LTC employer's privacy and data security training documented?



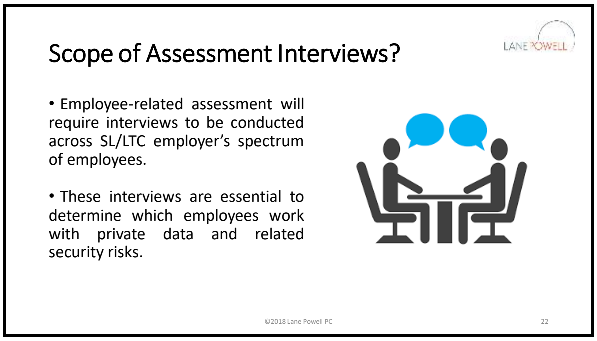
If SL/LTC employer has security cameras at community, how might those cameras impact employee rights?

- ➢ The National Labor Relations Act (NLRA) gives private employees the right to act together to try to improve their pay and working conditions--with or without a union.
- ➢ SL/LTC Employers with security/surveillance cameras should consider whether those cameras may have a "chilling effect" on employees' rights to engage in these sorts of "concerted activities."



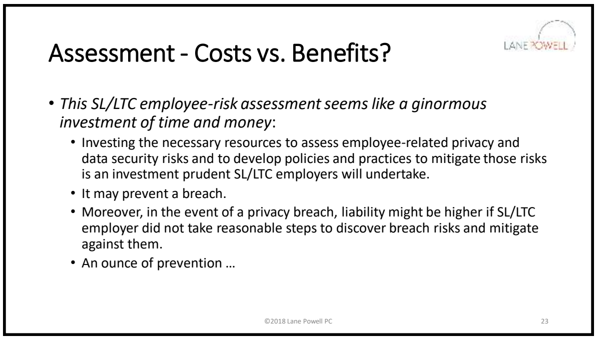
Who performs the employee-related privacy and data security risk assessment?

- **A team leader**: Individual with primary responsibility for coordinating and moving the assessment along
- **Stakeholders:** Employees who actually work with private information at your workplace (this should include HR representative and other employees, as appropriate)
- **Someone to document the process:** Someone responsible for accurately documenting the good faith efforts SL/LTC employer undertakes to assess employment-related privacy and data security risks—and conclusions/actions
- **Appropriate tech experts**: Someone knowledgeable about the data systems SL/LTC employer/employees currently use, current security measures, and related privacy and data security vulnerabilities



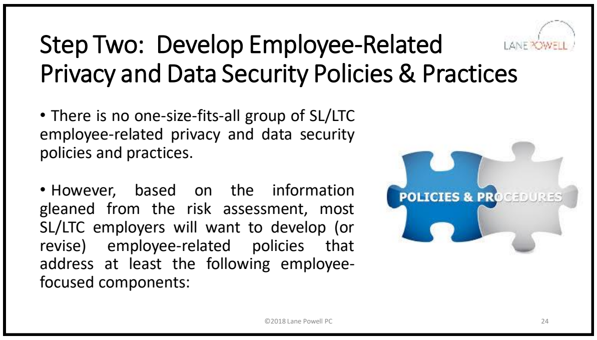
Scope of Assessment Interviews?

- Employee-related assessment will require interviews to be conducted across SL/LTC employer's spectrum of employees.
- These interviews are essential to determine which employees work with private data and related security risks.



Assessment - Costs vs. Benefits?

- *This SL/LTC employee-risk assessment seems like a ginormous investment of time and money*:
  - Investing the necessary resources to assess employee-related privacy and data security risks and to develop policies and practices to mitigate those risks is an investment prudent SL/LTC employers will undertake.
  - It may prevent a breach.
  - Moreover, in the event of a privacy breach, liability might be higher if SL/LTC employer did not take reasonable steps to discover breach risks and mitigate against them.
  - An ounce of prevention …



Step Two: Develop Employee-Related Privacy and Data Security Policies & Practices

- There is no one-size-fits-all group of SL/LTC employee-related privacy and data security policies and practices.
- However, based on the information gleaned from the risk assessment, most SL/LTC employers will want to develop (or revise) employee-related policies that address at least the following employee-focused components:

- **Every employee is responsible for privacy and data security compliance:** SL/LTC Employer's policies should emphasize that every employee is expected to be a team player dedicated to respecting and protecting SL/LTC employer, customer and co-worker privacy and data security.
- **If you see something, say something:** Make sure policies state that employees must immediately report suspected privacy breaches. Your policy should identify who needs to be notified and how.
- **Retaliation prohibited:** Policies should emphasize that (1) employees who make good faith reports of suspected privacy and data security policy violations are protected from retaliation and (2) employees who violate the "no retaliation" policy are subject to discipline up to and including termination. The policy should also provide options for employees to report retaliation.

- **"A need to know" basis:** SL/LTC employer's policies should help make sure that only employees who need to have access to private data have access to that data.
- **Workstations:** Policies should help make sure that private information cannot be viewed by residents / the public.
- **SL/LTC employer computers and devices:** Policies should make sure that employees accessing private information maintain the privacy of that information (i.e., use of passwords, logging off when stepping away from computers, maintaining physical control of employment-use devices)
- **Use of copiers and fax machines:** Policy should include employee protocols to make sure privacy is maintained (i.e., documents with private/sensitive information are not left unattended on copiers, etc.)

- **Physical transportation of private records:** Policies should set out whether, when, why (and if so who and how) employees are permitted to remove/transport private employment-related records.
- **Questions and suggestions:** Policies should identify who employees should approach with questions, concerns, or suggestions regarding SL/LTC employer's privacy and data security policies. (This is an opportunity to emphasize that each employee is a member of the team, and questions and suggestions about privacy and data security are always welcome.)
- **Consequences:** Make sure policy makes clear that compliance with privacy and data security procedures is mandatory and that violations may result in discipline, up to and including termination.

Personal devices: If employees are permitted to use their own laptops, tablets and smart phones related to the work duties, the policies should identify what restrictions apply, such as:

- Use a strong password or other strong user authentication;
- Use encryption (which converts data so it cannot be read without an encryption key/password);
- Activate remote "wiping"/remote disabling (enables SL/LTC employer to erase data on the device, or to lock the device, remotely);
- Use security software (to protect against viruses, spyware, malware and other malicious applications);
- Always maintain physical control of their devices (i.e., to avoid laptop theft from cars);
- Avoid use of public Wi-Fi (which can be used to intercept private data); and
- Make sure all private information is irretrievably deleted before disposing of (or reusing) such personal devices.

Employee Use of SL/LTC Employer's Computers and Devices for Personal Emailing and Texting: SL/LTC employer policy should clarify expectations.

- Employees who use SL/LTC employer's technology for personal emails and texts may assume SL/LTC employer has no right to monitor that personal use.
- Whether or not SL/LTC employer routinely monitors such usage, it may be necessary for employer to do so in certain circumstances.
- In that event, if SL/LTC employer has a written policy that expressly informs employees that employer reserves the right to monitor and review employees' personal use of employer's technology, and that employees should have no expectation of privacy regarding such personal use, such a policy may overcome an employee's objection to such review and monitoring.

- **Social media:** Policies should inform employees how their use of social media may impact such things as:
  - SL/LTC employer's trade secrets,
  - confidential customer information,
  - and employee rights to be free from harassment and retaliation.
- <u>**BUT**</u> … Make sure privacy and data security policies do not violate employee rights—such as the right to freely engage in "concerted activity" related to the terms and conditions of employment.

Red Alert: Employee Social Media-Related Privacy / Data Security Policies

- **NLRA**: The National Labor Relations Board has found that some SL/LTC employers' social media policies violated employee "concerted activity" rights by, for example, imposing restrictions that "chilled" employees' ability to discuss the terms and conditions of their work.
- **Whistleblowing**: Statements made by employees on social networking sites may be protected by state and/or federal whistleblower laws, including Oregon's Private Sector Whistleblower Law (ORS 659A.199). The law protects employees from adverse employment action where the employee has, in good faith, reported information that the employee believes is evidence of a violation of federal or state law.

Employee Rights
Under the National Labor Relations Act

Oregon's statute on "Employee social media account privacy" -- specific statutory prohibitions

Oregon law (ORS 659A.330) prohibits employers from, among other things, requiring or requesting an employee or applicant for employment to:

- Disclose a username or password for the purpose of accessing personal social media
- Access personal social media in the presence of the employer

Oregon's statute also prohibits an employer from discharging or otherwise penalizing an employee, or refusing to hire an applicant for employment based on refusal to provide a password or access to their social media account.

The Bad: Generally, SL/LTC Employers Should Avoid Employee Social Media Policies that:

- Prohibit employees from online discussion of wages or working conditions among employees;
- Require employees to ensure that their posts are completely accurate and not misleading;
- Require employees to check with management before posting about their employment;
- Prohibit employees from making offensive, demeaning, abusive, or inappropriate remarks both online and offline;
- Warn employees to think carefully about "friending" coworkers; and
- Prohibit employees from connecting with certain persons, businesses or organizations via social media.

The (probably) okay. The following employee social media policies are more likely to be deemed appropriate:

- Encouraging employees to be vigilant online to avoid being tricked into disclosing confidential information;
- Encouraging employees to notify management of workplace safety or other concerns;
- Reminding employees of the manner in which they may report workplace concerns to management;
- Reminding employees that they are prohibited from bullying, discriminating and retaliating against their co-workers;
- Prohibiting employees from representing in social media that the employees speak for/on behalf of the SL/LTC employer.

Social Media and Hiring Decisions

- SL/LTC Employers want to hire employees who will perform their work effectively, efficiently, safely—and in compliance with SL/LTC regulations.
- Some job applicants sometimes post things on social media that could reflect badly on their ability to perform their jobs.
- At first blush, it might seem that those persons who make hiring decisions for SL/LTC employers, as a precautionary measure, should do some "Googling" to determine if job applicants' social media postings contain any such information.
- However, checking job applicants' social media postings can create substantial problems for SL/LTC employers. This is because some job applicants make information available online that employers should not consider as part of the hiring process.

It is not unusual for job applicants' social media postings to contain the following types of information:

- Ethnicity and national origin
- Workplace injuries and information about Workers' Compensation claims
- Workplace complaints
- Union affiliation and organizing activities
- Religious affiliation and practices
- Family status
- Gender identity
- Sexual orientation

The list of such information goes on and on.

The Privacy-Related Risk?

- SL/LTC employers who "research" job applicants' social media presence run the risk of being exposed to information like that listed above.
- This means that any hiring decisions those SL/LTC employers then make about those applicants may be tainted by information that, under state and federal laws, must not be considered.
- Job applicants who are not offered a position may then claim that the decision was unlawfully based, at least in part, on factors the SL/LTC employer was prohibited from considering.

Best Practices: SL/LTC Hiring in the Age of Social Media

- Because social media postings often divulge information (race, gender, religion, etc.) that might lead to a claim of discrimination or retaliation, it is best if only trained human resources personnel check applicants' social media activities if SL/LTC employer does review public social media as part of the hiring process.
- Human resources professionals should be better able to focus solely on non-discriminatory information.
- Be consistent. In other words, if SL/LTC employer decides to review job applicants' public social media postings, make that the practice for all jobs (or at least, for all the same positions).
- Print It: If SL/LTC employer decides to make an adverse employment decision based on an applicant's (or employee's) social media posting, print and maintain a copy of that posting. That way, if the posting is later deleted, employer will have a copy available to show the legitimate, lawful, non-discriminatory basis of its decision.

Common SL/LTC Employee Social Media / Privacy Conundrum

Question: A SL/LTC employee who filed a workers' compensation claim related to a workplace lifting injury falsely posts on Facebook that SL/LTC employer refused to provide any appropriate light duty work for that employee. Can SL/LTC employer discipline that employee for posting false statements?

Answer:

- Because the employee has filed a workers' compensation claim, it is possible (if not likely) the employee would claim that the discipline is unlawful retaliation against the employee for exercising workers' compensation rights.
- The employee might also assert that the discipline was a violation of the employee's NLRA right to discuss the terms and conditions of employment.
- Employee might also be concerned as to why the employee's SL/LTC employer is apparently monitoring the employee's personal Facebook account (even if it is a public account).
- Under these facts, the more prudent approach may be to meet with the employee to discuss the employee's concerns, to try to understand them better, and to determine if an informal resolution can be negotiated.
  - ➢ Remember to objectively document all your efforts to address the employee's concerns.

Step Three: Train Your SL/LTC Employees to Comply With Privacy and Data Security Policies & Practices

Even the most clearly written and comprehensive policies on employee-related privacy and data may not be effective unless employees are not only required to review those policies but also given adequate and thorough training.

- **Make it part of new-hire orientation:** New SL/LTC employees can be overwhelmed by the sheer volume of information that comes with a new job. Nonetheless, be sure to include privacy and data security policies and practices as part of new hire orientation.

- **Make comprehensive training an annual event:** Because of the frequent changes in technology and privacy laws, it can be hard to keep up. SL/LTC employers should provide comprehensive refresher training on privacy and data security policies and practices at least annually.

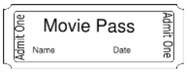
- **Mini-updates:** Include 5 to 10-minute updates on a specific area of your privacy and data security policies at weekly, bi-weekly, and/or monthly staff meetings. This helps employees remember how important privacy and data security is to SL/LTC employer's community.

Document each training session: It cannot be overemphasized how important it is for SL/LTC employers to maintain timely, complete, and accurate records of the privacy and data security training provided to employees:

- Have employees sign and initial policies—and maintain a signed/initialed copy.
- When SL/LTC employer provides training to employees on these policies, make sure every employee who attends that training signs and dates a document to evidence their participation in such training.
- This documentation can provide evidence of the good faith and effective efforts you have made to avoid such a breach.
- If SL/LTC employee is disciplined for violating employer's privacy and data security policies, this documentation can be evidence that the adverse employment decision was not for a discriminatory or retaliatory reason.

Best Practices Tip – Suggestion box

- Encourage employees to make suggestions on how to improve privacy and data security policies and procedures.
- EXAMPLE: If SL/LTC employee makes a suggestion to help employer avoid a "ransomware" attack, and if employer implements that suggestion, sing that employee's praises at a staff meeting—and maybe reward him or her with movie passes or a gift card.



Low-Tech Takeaway

Sticky Note:

- On workstation computer monitor, place a sticky note that states: *"Stop and Think Before You Click That Link."*
- It's a persistent reminder to help avoid a ransomware or other malicious software attack by taking a wary look at the emails received, especially where they have attachments or include internet links.

Another Low-Tech Takaway

Work Area Signage:

- In work areas, hang up a modified version of the typical factory "Days Without Injury" sign.
- A workplace privacy and data security sign could instead say something like: "This Department Has Worked [ ] Days Without a Privacy / Data Security Breach."

Best Practices Tip – What's a data breach look like?

Prudent SL/LTC employers will also train employees not only on how to help prevent data breaches but also how to recognize possible breaches.

- It's hard to prevent or report what you cannot recognize.

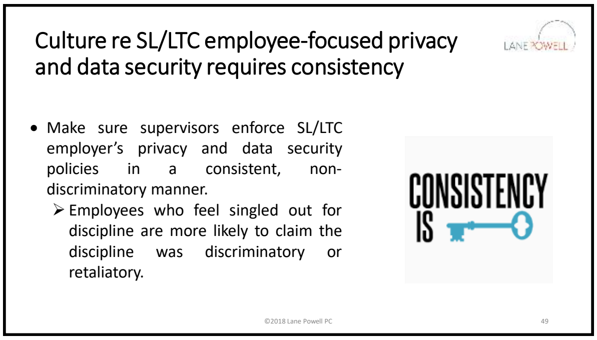
Step Four: Implement and Enforce Employee Privacy and Data Security Policies & Practices

SL/LTC employee-related privacy and data security policies will only be effective if they are implemented and enforced.

Make privacy and data security a core part of your SL/LTC employment culture.

Critical SL/LTC managerial / supervisory role in implementation

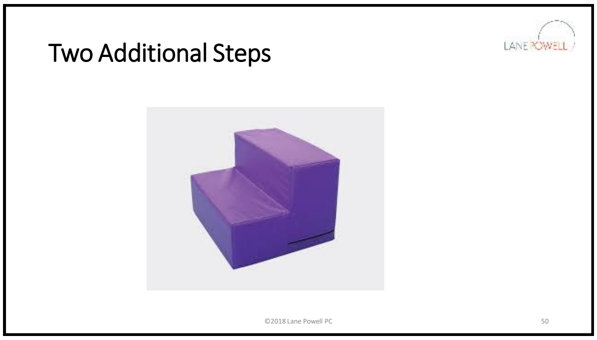
- Train (and retrain) supervisors on the substance of your privacy and data security policies.
  - ➢ Your supervisors need to lead by example when it comes to privacy and data security policy compliance.



Culture re SL/LTC employee-focused privacy and data security requires consistency

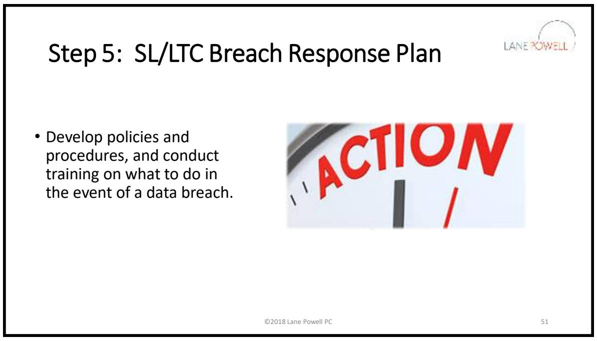
LANE POWELL

- Make sure supervisors enforce SL/LTC employer's privacy and data security policies in a consistent, non-discriminatory manner.
  - ➢ Employees who feel singled out for discipline are more likely to claim the discipline was discriminatory or retaliatory.



Two Additional Steps

LANE POWELL



Step 5: SL/LTC Breach Response Plan

LANE POWELL

- Develop policies and procedures, and conduct training on what to do in the event of a data breach.

Step 6: Apply, Rinse, Repeat

LANE POWELL

- Prudent SL/LTC employers will periodically review, update, and re-implement all the (updated) privacy and data security policies.
- Remember to involve employees in this process!

Today
Rinse
&
repeat

Thank you…

LANE POWELL

Jeff Duncan Brecht
brechtj@lanepowell.com / 503.778.2162
Lane Powell PC