AHLA

PALS Advisor

A Publication of the American Health Lawyers Association
Post-Acute and Long Term Services Practice Group

VOLUME 20
ISSUE 2
December 2017

Table of Contents

"This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering legal or other professional services. If legal advice or other expert assistance is required, the services of a competent professional person should be sought."
—from a declaration of the American Bar Association

Cyber-Threat Reduction: How Employee Policies and Practices Can Help Senior Living and Long Term Care Employers Bolster Privacy and Data Security

Jeff Duncan Brecht
Lane Powell PC
Portland, OR

In the science fiction film *The Terminator* (and its progeny), an artificially intelligent, automated defense network called Skynet becomes self-aware when it spreads into computers around the world. Unfortunately, Skynet then determines humans must be destroyed. During the various iterations of this movie franchise, Skynet, with mixed results, attempts to obliterate humanity by using its control of computer systems to, among other things, launch nuclear weapons and build and control cyborg[1] "terminators." One could argue, however, that Skynet could have saved itself a lot of time and trouble by simply using its control of global computer systems to deny humanity access to electronic health data, or perhaps more insidiously, to alter and falsify that health data.

Although a Skynet-like artificial intelligence does not yet (and might never) exist,[2] the risks associated with the creation and use of, and permanent reliance on, electronic health data are real and present.[3] The dangers associated with threats to electronic health data are reflected in the Security Rule of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which requires covered entities to implement safeguards to preserve the availability and integrity of such data.[4] In fact, in the context of HIPAA security standards that include protecting the "integrity" of electronic health information, the term "integrity" means "the property that data or information have not been *altered* or destroyed in an unauthorized manner."[5]

This year, the Health Care Industry Cybersecurity Task Force (HCIC Task Force)[6] released its report to Congress titled, *Report on Improving Cybersecurity in the Health Care Industry*.[7] In its report, the HCIC Task force repeatedly urges a "holistic" approach to effectively address threats to electronic health data. In fact, the Task Force maintains that "[o]rganizations that do not adopt a holistic strategy not only put their data, organizations, and reputation at risk, but also—most importantly—the welfare and safety of their patients."[8]

According to the HCIC Task Force, an effective, holistic approach toward mitigating the risks of electronic health data use requires a workforce that is cybersecurity vigilant and focused, and trained to implement data security policies and practices.[9] This makes sense, because the largest privacy and data security risks for employers can come from within their own workforce.[10] This is not because senior living and long term care (SL/LTC) employees generally intend to breach privacy and data security policies and practices. Rather, it is often because of avoidable employee mistakes and non-malicious conduct. These SL/LTC employee-related risks can decrease for SL/LTC employers when adequate employment-related privacy and data security policies and practices are developed and explained to employees, and where such policies and practices are regularly reviewed and updated.[11]

What's at Stake for SL/LTC Care Employers?

SL/LTC Employers who do not take steps to assess employee-related privacy and data security risks, and who fail to prepare, implement, and enforce appropriate employment-related privacy and data security issues could be vulnerable to a host of unpleasant consequences, including, but not limited to, HIPAA violations and related sanctions, [12] violations of state privacy laws, public relations nightmares,[13] litigation,[14] and most importantly, resident safety concerns.[15]

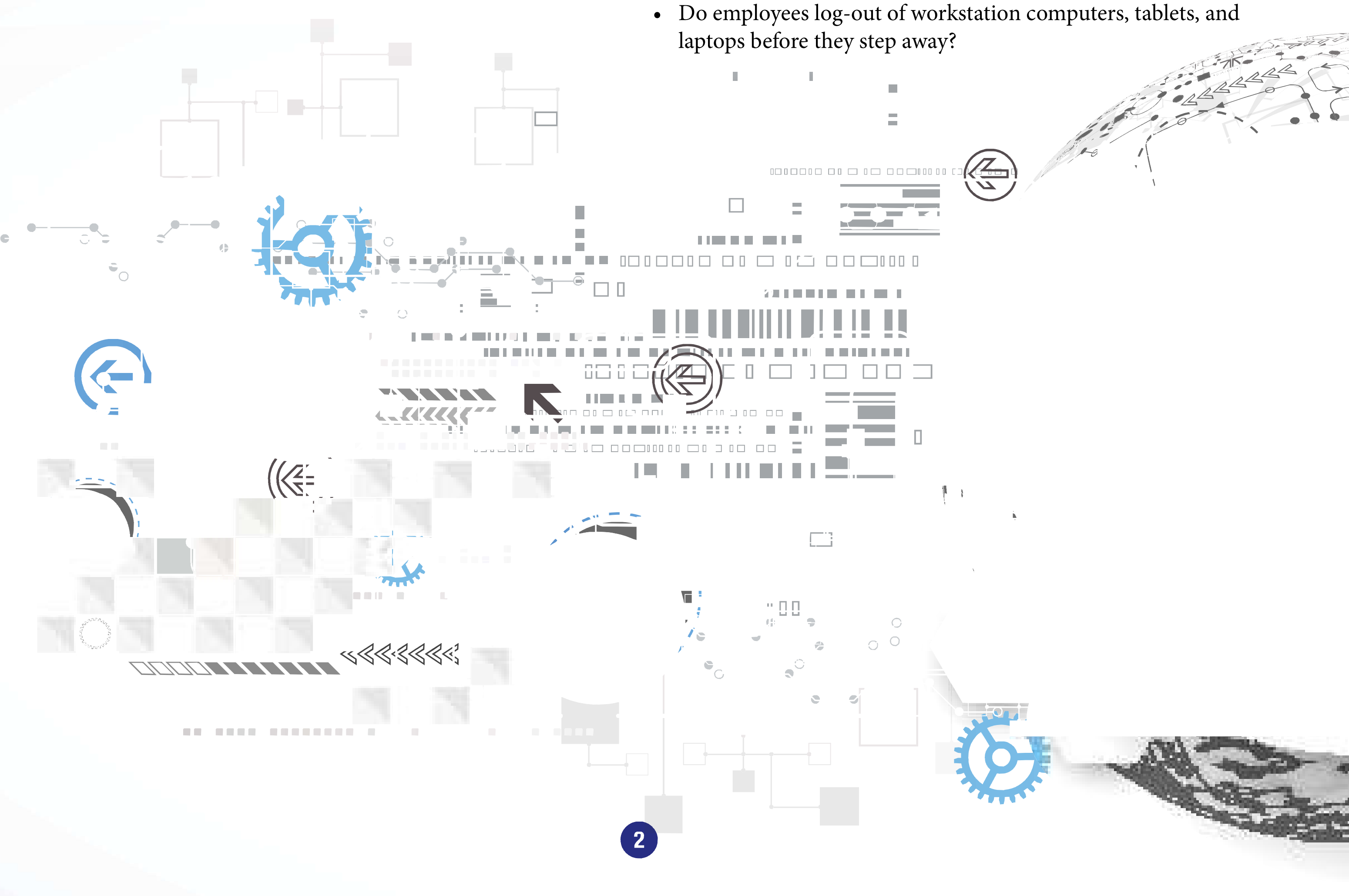
What Should SL/LTC Employers Do?

With the HCIC Task Force's holistic approach in mind, SL/LTC employers should employ[16] a number of steps utilizing a broad selection of their workforces to help make employee-focused strategies and actions an effective component of the employers' overall privacy and data security measures.

STEP ONE - SL/LTC employers should assess the employee-related privacy and data security risks at their communities.

Regardless of the size of the SL/LTC community or the number of its employees, in order to develop and implement effective employee privacy and data security policies and practices, SL/LTC employers need to assess their specific employment-related privacy and data security risks.[17] SL/LTC employers should use the information garnered from this employee-related privacy and data security risk assessment process to create and implement policies that most effectively fit the community. In general, SL/LTC employers should include at least the following queries in their employee-related privacy and data security risk assessment:[18]

- 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 work duties?
- Do employees have non-public workspaces where they may privately discuss resident care matters and employment matters?
- What password policies and practices must employees comply with?
- Does the 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?

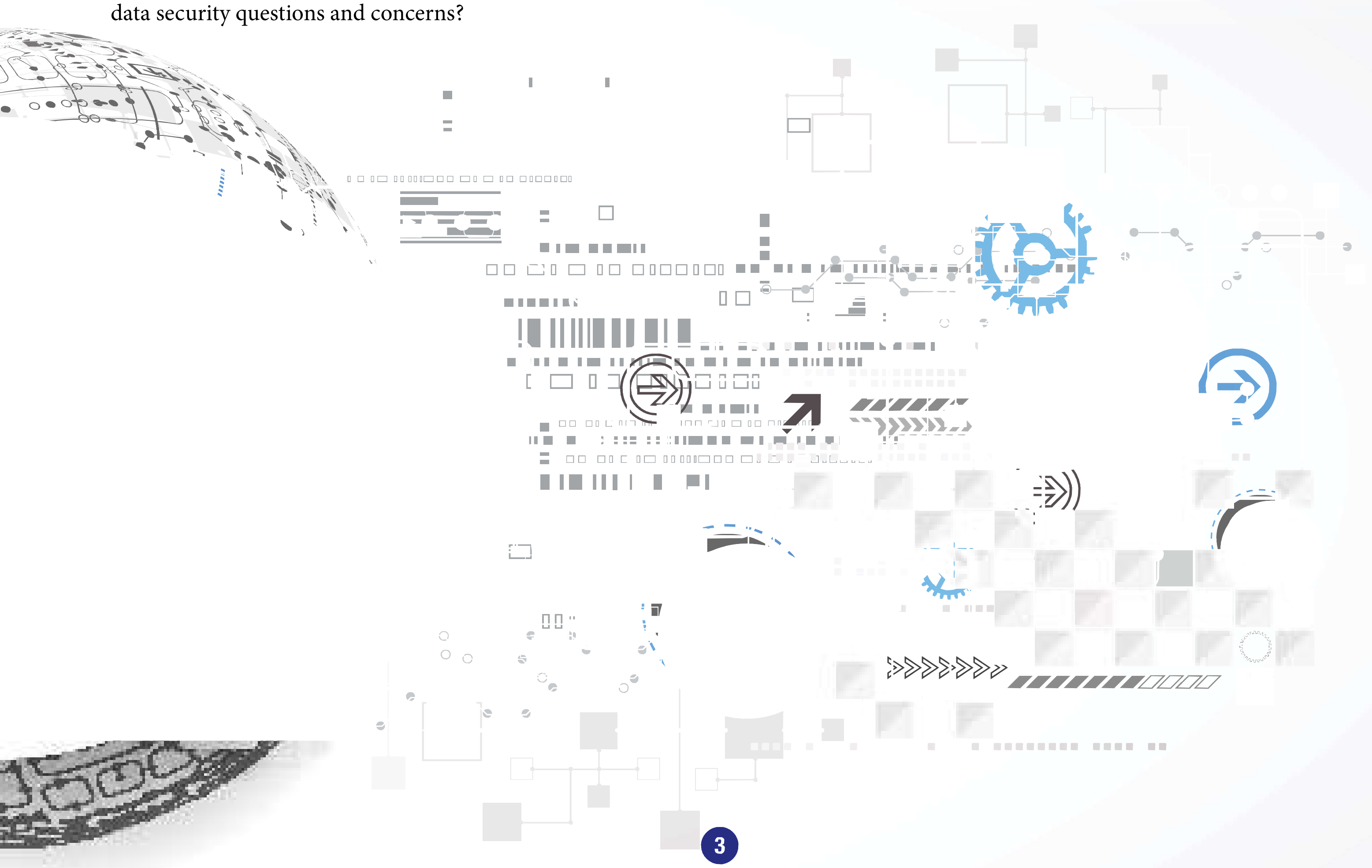


- How quickly (if at all) do employee workstation computers, tablets, and laptops "auto-lock" when those devices are inactive?
- Do employees share work-related passwords?
- Do employees transport private, community-related information in their vehicles?
- Do employees use laptops and other devices that contain private, community-related information at their homes, coffee shops, or elsewhere offsite?
- Is private, work-related information visible to residents or the public at employee workstations?
- What training is provided to employees regarding community privacy and data security policies and practices?
- Do employees verify email addresses and fax numbers before transmitting private information?
- Does the SL/LTC employer regularly review and update its employee-related privacy and data security policies?
- How do employees report violations of the SL/LTC employer's employee-related privacy and data security policies?
- Do employees know what to do when residents request their records?
- Are employees aware that their co-workers also have privacy rights and they should not access each other's information?
- Do employees know who to approach with their privacy and data security questions and concerns?
- Is the SL/LTC employer's privacy and data security training documented?
- If the SL/LTC employer uses workplace security cameras, how might those cameras impact employee rights?

Whether or not a SL/LTC employer conducts the assessment internally, with the assistance of an attorney, or with the assistance of some other third-party, the assessment should be a team effort consisting of at least the following individuals:

- **Team Leader**: An individual with primary responsibility for coordinating and moving the assessment along;
- **Stakeholders**: Caregivers, human resources, and other SL/LTC employees who actually work with private information;
- **Someone to document the process**: The assessment is a labor intensive process, and SL/LTC employers need someone on the assessment team who will be responsible for accurately documenting the good faith efforts your community is undertaking to assess employment-related privacy and data security risks;
- **Appropriate Tech Experts**: Someone who is knowledgeable about the data systems SL/LTC employees use, current security measures, and related privacy and data security vulnerabilities.

The employee-related assessment should include interviews across the SL/LTC employer's spectrum of employees. These interviews are essential to determine which employees work with private data and related security risks.



STEP TWO - SL/LTC employers should develop/revise employee privacy and data security policies that address and help mitigate related risks.

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

- **Every employee is responsible for privacy and data security compliance:** Policies should emphasize that every employee is expected to be a team player dedicated to respecting and protecting resident and co-worker privacy and data security.
- **If you see something, say something:** Policies should require employees to immediately report suspected privacy breaches (and should identify who needs to be notified and how).
- **Retaliation prohibited:** Policies should emphasize that employees who make good faith reports of suspected privacy and data security policy violations are protected from retaliation, and that employees who violate the "no retaliation" policy are subject to discipline up to and including termination. Policies should also provide options for employees to report retaliation.
- **"A need to know" basis:** 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 and guests.
- **Community computers and devices:** Policies should help 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 community devices).
- **Use of copiers and fax machines:** Policies should inform employees of protocols to make sure privacy is maintained (i.e., documents with resident information are not left unattended on copiers).
- **Personal devices:** If SL/LTC employees are permitted to use their own laptops, tablets, and smart phones related to the work duties, policies should establish rules/procedures to help mitigate the risk of a privacy and data breach, such as use of strong passwords, encryption, activated remote "wiping"/remote disabling (which enables the community to erase data on the device, or to lock the device, remotely), and requiring employees to always maintain physical control of their devices.
- **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 records from the community.
- **Records requests:** Policies should inform SL/LTC employees what to do when residents request their records.
- **Social media:** Policies should inform on use of social media—including how it may impact such things as resident rights to privacy and employee rights to be free from harassment and retaliation. (However, SL/LTC employers must also make sure employee social media policies do not violate employee rights—such as the right to freely engage in "concerted activity" related to the terms and conditions of employment).[19]
- **Consequences:** Policies should help SL/LTC employees understand that compliance with privacy and data security procedures is mandatory and that violations may result in discipline up to and including termination.

STEP THREE - SL/LTC employers should educate/train their employees on compliance with the privacy and data security policies.

Even the most clearly written and comprehensive policies on SL/LTC employee-related privacy and data security may not be effective if employees are not only required to review those policies but also given adequate and thorough training.[20] With this in mind, SL/LTC employers should incorporate at least the following into their employee-related privacy and data security protocols:

- **Make it part of new-hire orientation:** New employees can be overwhelmed by the sheer volume of information that comes with starting work for SL/LTC employers. Nonetheless, SL/LTC employers should provide training on employee 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, SL/LTC employers should provide comprehensive "refresher" training on privacy and data security policies and practices at least annually—and also include five to ten minute updates on a specific area of privacy and data security policies at weekly, bi-weekly, and/or monthly staff meetings.
- **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 (including which employees receive policies and training, and when). This documentation can, for example, provide evidence to an agency investigating a privacy breach of all the good faith and effective efforts the SL/LTC employer has made to avoid such a breach. Similarly, if an employee is disciplined for violating privacy and data security policies, this documentation can be evidence that the employer made the adverse employment decision for a lawful and not a discriminatory or retaliatory reason.

STEP FOUR - SL/LTC employers should implement and enforce their employee-related privacy and data security policies.

A SL/LTC employer's employee-related privacy and data security policies will only be effective if they are implemented and enforced. As with every other employee policy, SL/LTC employers should provide:

- **Positive Reinforcement:** Train (and retrain) supervisors on the substance of the employee-related privacy and data security policies. Supervisors need to lead by example when it comes to privacy and data security policy compliance.
- **Consistency and Fairness:** Make sure supervisors enforce the employee-related privacy and data security policy in a consistent, non-discriminatory manner. Employees who feel singled out for discipline are more likely to claim the discipline was discriminatory or retaliatory.

STEP FIVE - SL/LTC employers should prepare and adopt breach-response employee-related policies.

Prudent SL/LTC employers recognize that even with solid privacy and data security policies and practices in place, breaches can (and do) occur. Accordingly, SL/LTC employers should include employee breach-response training as a key part of its overall breach-response and mitigation protocols.[21] Prudent SL/LTC employers will also train employees on how to recognize possible breaches.

STEP SIX - SL/LTC employers should periodically review, update, and re-implement each of the above steps.

A SL/LTC employer's employee-related privacy and data security risk assessment, policy review, training, implementation, and enforcement protocols should be regularly repeated (probably as part of the employer's broader privacy and data security assessments). Technology (and related risks) change frequently. Privacy and data security laws (and industry standards) also change. To be most effective, the assessments, policies, practices, and employee training needs to be part of the employee culture. And that entails keeping these privacy and data security issues a part of ongoing workforce training and discussions.

While the above steps require a substantial investment of time, energy, and other resources, SL/LTC employers who make that investment should have a stronger likelihood of avoiding privacy and data breaches as well as the unpleasant, and costly, consequences such breaches can entail.

[1] The author acknowledges that there is an impassioned, decades-long debate in some circles regarding whether terminators are technically cyborgs, androids, robots, or something else. However, for purposes of this article, the author just doesn't care.

[2] *See, e.g.,* Kevin Kelly, *The Myth of a Superhuman AI,* Wired (Apr. 25, 2017), *available at* https://www.wired.com/2017/04/the-myth-of-a-superhuman-ai/.

[3] Jacob Brogan, *The Hack of a London-Based Plastic Surgeon Provides a Chilling Warning About Medical Data Security,* Slate (Oct. 24, 2017), *available at* http://www.slate.com/blogs/future_tense/2017/10/24/the_hack_of_a_london_based_plastic_surgeon_provides_a_warning_about_medical.html.

[4] 45 C.F.R. § 164.306(a).

[5] 45 C.F.R. § 164.304 (emphasis added).

[6] In 2016, the U.S. Department of Health & Human Services established the Health Care Industry Cybersecurity Task Force pursuant to Cybersecurity Act of 2015. *See* H.R. 2029, 114th Cong. (2015), at Sec. 405(c).

[7] HCIC Task Force, *Report on Improving Cybersecurity in the Health Care Industry* (2017 HCIC Report), *available at* https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf.

[8] *Id.* at p. 40.

[9] *Id.* at p. 35. ("The health care industry must increase outreach for cybersecurity across all members of the health care workforce through ongoing workshops, meetings, conferences, and tabletop exercises.")

[10] Tara Siegel Bernard and Stacy Cowly, *Equifax Breach Caused by Lone Employee's Error, Former C.E.O. Says,* NY Times (Oct. 3, 2017), *available at* https://www.nytimes.com/2017/10/03/business/equifax-congress-data-breach.html.

[11] According to the U.S. Department of Human Services, Office for Civil Rights, "[a] covered entity's workforce is its frontline not only in patient care and patient service, but also in safeguarding the privacy and security of its patients' protected health information (PHI)." OCR Cyber Awareness Newsletter, *Train Your Workforce, so They Don't Get Caught by a Phish!* (July 2017), *available at* https://www.hhs.gov/sites/default/files/july-2017-ocr-cyber-newsletter.pdf.

[12] OCR's so called online "wall of shame" publically lists all breaches reported within the last 24 months that are currently under investigation by OCR: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

[13] Think Equifax. Kelly Phillips Erb, *After Pressure Over Security Concerns, IRS Suspends Equifax Contract,* Forbes (Oct. 13, 2017), *available at* https://www.forbes.com/sites/kellyphillipserb/2017/10/13/after-pressure-security-concerns-irs-suspends-equifax-contract/#6e08f74c36b6. Most states require businesses to notify their "customers" as soon as possible if there has been a data security breach. For SL/LTC employers, "customers" are likely their residents. This means, that if SL/LTC employees somehow cause a breach of "personal information" (residents' names, bank information, credit card information, health data and care needs, and so on), the employer likely must notify residents or others potentially affected by the breach. Depending on the scope of the breach, the SL/LTC employer may also be required to notify the state's attorney general. Needless to say, residents, prospective residents, their family members, and others may find a breach notification concerning.

[14] Where a SL/LTC employee's employment-related conduct infringes someone's privacy, it is possible the employer could be named as a defendant in a lawsuit brought by the person whose privacy (or employment right) was infringed.

[15] "[F]or the health care industry, cybersecurity issues are, at their heart, patient safety issues." 2017 HCIC Report, at p. iii.

[16] Sadly, pun intended.

[17] This employee-focused risk assessment is likely a subset of the broader privacy and data security assessment that all SL/LTC employers should undertake.

[18] However, each SL/LTC employer should modify its employee-focused risk assessment to best fit its particular circumstances.

[19] *See* National Labor Relations Act (NLRA) § 7 (29 U.S.C. § 157). Because the National Labor Relations Board continues to issue decisions regarding social media issues impacting the NLRA, SL/LTC providers should make sure their employee social media policies are based on the NLRB's current position and decisions. The NLRB offers some general guidance here: https://www.nlrb.gov/news-outreach/fact-sheets/nlrb-and-social-media.

[20] Stephen Baer, *Why you Should Gamify Your Cybersecurity Training,* Forbes (Oct. 4, 2017), *available at* https://www.forbes.com/sites/forbesagencycouncil/2017/10/04/why-you-should-gamify-your-cybersecurity-training/#2777266f6271.

[21] OCR has prepared a handy checklist entitled, *My entity just experienced a cyber-attack! What do we do now?* SL/LTC employers should reference OCR's checklist when considering how best to incorporate breach response as part of employee-related policies and training. The checklist is *available at* https://www.hhs.gov/sites/default/files/cyber-attack-checklist-06-2017.pdf.