











IN THIS ISSUE

- 2  [Our Authors](#)
- 3  [General Data Protection Regulation Update](#) by Alan Meneghetti, Natasha Ahmed and Philippa Townley
- 3  [Vermont Passes Additional Privacy Protections in Light of Changing Technologies](#) by Bart Huffman and Charles Salmon
- 3  [No Pictures, Please! Workplace Anti-Recording Policies and the NLRA](#) by Sean Killian
- 4  [Charge! Coverage Disputes Over Credit Card Issuer Assessments and Bank Lawsuits](#) by Molly McGinnis Stine and John F. Kloecker
- 5  [Illinois Simplifies Cumbersome Insurer Record Retention and Destruction Requirements](#) by Karen Booth
- 5  [Recent UK Information Commissioner's Office \(ICO\) Fines and Investigations](#) by Alan Meneghetti, Natasha Ahmed and Philippa Townley
- 6  [U.S.-EU Privacy Shield Update](#) by Alan Meneghetti, Natasha Ahmed and Philippa Townley
- 6  [EEOC Update: New Wellness Program Regulations Create New Employer Obligations](#) by Charles Salmon and Sean Killian
- 7  [Increasing Necessity for a HIPAA Compliant "Business Associate Agreement" Within the Technology Industry](#) by Ashley Wheelock

Locke Lord's Privacy & Cybersecurity Newsletter provides topical snapshots of recent developments in the fast-changing world of privacy, data protection and cyber risk management. For further information on any of the subjects covered in the newsletter, please contact one of the members of our privacy and cybersecurity team.

OUR AUTHORS:



Natasha Ahmed
Associate
London
+44 (0) 20 7861 9048
nahmed@lockelord.com



Molly McGinnis Stine
Partner
Chicago
312-443-0327
mmstine@lockelord.com



Karen L. Booth
Associate
Hartford
860-541-7714
karen.booth@lockelord.com



Alan D. Meneghetti
Partner
London
+44 (0) 20 7861 9024
ameneghetti@lockelord.com



Bart W. Huffman
Partner
Austin
512-305-4746
bhuffman@lockelord.com



Charles M. Salmon
Associate
Austin
512-305-4722
csalmon@lockelord.com



Sean Kilian
Associate
Dallas
214-740-8560
skilian@lockelord.com



Philippa Townley
Associate
London
+44 (0) 20 7861 9041
ptownley@lockelord.com



John F. Kloecker
Of Counsel
Chicago
312-443-0235
jkloecker@lockelord.com



Ashley Wheelock
Associate
Austin
512-305-4860
ashley.wheelock@lockelord.com

General Data Protection Regulation Update

As [reported](#) in the April Locke Lord Privacy & Cybersecurity Newsletter, the European Parliament gave the final approval to the General Data Protection Regulation (GDPR) on April 14, 2016.

The final text of the GDPR was published in the Official Journal of the European Union on May 4, 2016, and the GDPR will come into force in all EU Member States two years and 20 days after its publication, that is on May 24, 2018. The final text of the legislation can be accessed on the website of the European Commission [here](#), and a summary of the key features of the GDPR are set out in a recently published Locke Lord article, accessible [here](#) on the Locke Lord website.

Although the GDPR will not apply to Member States for another two years, there are a number of steps that organisations can, and indeed should, be taking now in order to ensure that they are compliant when the time comes, including the 12 steps outlined in the UK Information Commissioner's Office (ICO) publication "[Preparing for the General Data Protection Regulation \(GDPR\): 12 Steps to Take Now](#)." The note from the ICO emphasises (amongst other things) the importance of an organisation understanding what personal data it holds, where it came from and who it is shared with; ensuring that it has the appropriate consents for obtaining and using personal data; and ensuring that appropriate procedures are in place for the secure storage of, and timely deletion of, personal data. As the ICO points out, many of the obligations in the GDPR are substantially the same as those in the UK Data Protection Act 1998, and so organisations that are already compliant with the current data protection law should be well placed to ensure compliance with the GDPR.

The ICO has [stated](#) that it will continue to publish further guidance over the coming months, and we will keep our clients posted on this as and when this is made available. In light of the UK's vote to leave the EU on June 24, 2016 ("Brexit"), the GDPR and the ICO's guidance remains relevant to the UK. A formal process must be followed in order for a country to leave the EU, commencing with the activation of Article 50 of the 2009 Lisbon Treaty. Once this has taken place, the UK and the remaining members of the EU must negotiate the UK's exit. The UK will still be a member of the EU when the GDPR comes into force. Even if the UK chooses not to retain the GDPR (whether in whole or in part) once it leaves the EU, as the ICO has stated "The UK will continue to need clear and effective data protection laws, whether or not the country remains part of the EU."

Vermont Passes Additional Privacy Protections in Light of Changing Technologies

Vermont has recently enacted legislation to directly limit how information may be collected and used by government entities using drones, through access to electronic communications and through automated license plate recognition technology. Vermont Senate Bill [155](#) (SB 155).

With respect to drones, SB 155 provides that a Vermont law enforcement agency shall not "use a drone or information

acquired through the use of a drone for the purpose of investigating, detecting, or prosecuting crime" or "use a drone to gather or retain data on private citizens peacefully exercising their constitutional rights of free speech and assembly." The law does not prohibit use of drones by a law enforcement agency (i) for observational or public safety reasons, (ii) pursuant to a warrant or a judicially-recognized exception to a warrant requirement (such as exigent circumstances) or (iii) for purposes other than investigations (such as search and rescue and assessment of accidents). However, a law enforcement agency using a drone pursuant to a warrant must endeavor to limit observation and information collection to the target of the warrant, and an agency acting under exigent circumstances must try to obtain a warrant within 48 hours and immediately cease the drone use if the warrant is denied. Law enforcement agencies that use drones must provide an annual report to the Vermont Department of Public Safety addressing the volume, efficacy and cost of drone usage.

With respect to electronic communications, and in line with the federal [Electronic Communications Privacy Act](#), SB 155 prohibits law enforcement officers from "compell[ing] the production of or access to subscriber [communication contents] from [electronic communication] service provider[s]." Content may be properly collected via a warrant (which must be particularized and prohibit further disclosure of the collected information absent a court order) or a judicially-recognized exception to a warrant requirement or with the specific consent of a subscriber. Information other than content may be collected by law enforcement from electronic communications service providers pursuant to a subpoena issued based on reasonable cause and a reasonable calculation that the information sought will lead to evidence of an offense.

The new law amends existing Vermont law governing treatment of automated license plate recognition technology (ALPR). Under the new law, ALPR can be used for more serious crimes and circumstances (e.g., to locate missing persons) but not for general traffic and parking violations.

Technological advances continue to make it easier for the government (and private entities) to collect information traditionally considered to be private. Vermont's new law is the latest example of a state taking the initiative in the continuing development of use-based contours for privacy protection. Whether and to what extent it ultimately matters that the government or a non-governmental person or entity is collecting or using information remains to be seen.

No Pictures, Please! Workplace Anti-Recording Policies and the NLRA

Most people in modern workplaces carry high definition video cameras in their pockets. This can make employers uncomfortable for a variety of reasons, but any employer that wishes to regulate recording devices in the workplace must be careful not to infringe on employees' rights to engage in "protected concerted activity." Even though the National Labor Relations Act (NLRA) was signed in 1935 – roughly the same year the word "video" entered the English lexicon – the National Labor Relations Board (the Board) has found that the use of

recording devices in the workplace is often concerted activity protected by the NLRA.

In *Whole Foods Market, Inc.*, [363 NLRB No. 87](#) (Dec. 24, 2015), the issue for the Board was whether Whole Foods violated the NLRA by maintaining two anti-recording policies. One policy prohibited the recording any conversations or company meetings without management's approval or the consent of all parties to the conversation. Similarly, the second policy prohibited recording any conversations without management approval. The justifications for the policies were to encourage the free exchange of ideas at company meetings, and to eliminate the chilling effect that may exist when a person is concerned he or she is being recorded. Importantly, the scope of the policies was not qualified in any way, and there was evidence that the policies applied regardless of whether or not employees were engaged in protected concerted activity.

Under Board precedent, photography and audio or video recording in the workplace, as well as posting photos and recordings on social media, are protected concerted activities as long as employees are acting in concert for their mutual aid and protection, and no overriding employer interest is present. For example, recording images of unsafe working conditions or protected picketing, or documenting and publicizing discussions of terms and conditions of employment may all be protected concerted activities.

In its argument, Whole Foods relied on *Flagstaff Medical Center*, 357 NLRB No. 65 (2011). In that case, the Board held that a hospital's policy of prohibiting recording during work time on hospital property was justified in light of the privacy interests of the hospital's patients, and the hospital's HIPAA obligations to prevent wrongful disclosure of health information. Whole Foods argued that, like the hospital, its policies were justified by its desire to protect privacy interests, including information about its employees and the confidentiality of its trade secrets. Although the Board conceded these justifications were "not without merit," it held that such broad and unqualified policies violated the NLRA because they could be read to prohibit protected concerted activity. Further, it distinguished *Flagstaff Medical Center*, finding the hospital patients' privacy interests in that case far more compelling than the interests articulated by Whole Foods.

The takeaway for employers is that to maintain an anti-recording policy, there must be a strong business justification, which should be specified in the policy. As *Whole Foods* demonstrates, blanket restrictions are highly suspect, so policies should be narrowly tailored to those times and locations where they are necessary to protect the employer's valid business interests.

Charge! Coverage Disputes Over Credit Card Issuer Assessments and Bank Lawsuits

Costs commonly associated with retail data breaches include notification to affected consumers, third-party lawsuits by alleged victims, and reimbursements for fraudulent charges. After the press releases, notifications and third-party lawsuits, however, there are the issues or disputes involving the breached merchant, its credit card servicer, the credit card associations or

the bank issuing the credit cards. Case law is evolving regarding whether the fines, assessments or damages asserted by the servicers, the associations or the banks are covered by any of the merchant's cyber or other policies.

One court recently found that assessments imposed on an insured's credit card servicer were not covered under the insured's cyber policy. In *P.F. Chang's China Bistro, Inc. v. Federal Ins. Co.*, No. CV-15-01322 (D. Ariz. May 31, 2016), the court addressed P.F. Chang's demand for coverage of certain assessments under a cybersecurity policy. The policy covered "direct loss, legal liability, and consequential loss resulting from cyber security breaches." Following a 2014 breach, Chang's notified its insurer, which reimbursed Chang's for costs of a forensic investigation and third party lawsuits by customers. Chang's credit card servicer performed its services pursuant to contracts with credit card associations such as MasterCard and Visa. As a result of the breach, MasterCard imposed \$1.7 million in assessments on the credit card servicer. The servicer paid and then received reimbursement for those assessments from Chang's under the agreement between the servicer and Chang's. Chang's submitted a claim to its insurer for the payment. After the insurer denied coverage, Chang's sued.

The court granted the insurer's summary judgment motion, finding no coverage for the reimbursed assessments. First, the court held that Chang's servicer did not sustain an injury as defined in Chang's policy, because the servicer was not the party that was breached. Therefore, the assessments were not an injury sustained by the insured. Had the servicer itself been the victim of the breach, coverage may have been triggered because the servicer was a "Third Party Servicer Provider" under the policy. Chang's argued it was immaterial that the assessments were first passed through its servicer which in turned charged Chang's, i.e., because a "Privacy Injury" occurred and Chang's was responsible for the resulting assessments, it should not matter which party suffered the injury. The court rejected this argument, holding that the plain language of the policy provided that only the party that was breached suffers a "Privacy Injury." Because the servicer's records were not breached, the assessments imposed on it were not covered.

Second, although the court found that the assessments qualified as "Privacy Notification Expenses" and "Extra Expenses" arising from a breach, certain exclusions barred coverage. The court found that exclusions for losses arising from a "contract or agreement" and for costs "incurred to perform any obligation assumed by, on behalf of, or with the consent" of the insured applied. The court thus dismissed Chang's complaint.

In a slightly different scenario, a Texas liquor store chain is seeking coverage under a liability policy for litigation costs incurred in attempting to recover \$4.2 million withheld by its credit card servicer. The servicer kept the funds to pay for assessments imposed on it by MasterCard and Visa following two breaches of Spec's computer network. *Spec's Family Partners, LTD v. The Hanover Ins. Co.*, No. 4:16-cv-438 (S.D. Tex.) (filed Feb. 19, 2016). Spec's sued the servicer to recover the withheld funds and sought coverage from its insurer for its affirmative litigation fees. The insurer denied coverage on grounds that that Spec's incurred the fees solely in connection with the lawsuit filed by Spec's against the servicer. This litigation is ongoing.

Another recent decision involves coverage for the defense of a lawsuit brought by a bank in connection with its reimbursement of fraudulent charges relating to the insured's data breach. [RVST Holdings, LLC v. Main Street Assurance Co.](#), No. 52419 (NY App. Div. Feb. 18, 2016). The bank alleged that the insured failed to exercise reasonable care in safeguarding cardholder information. The insured sought coverage for defense and indemnification as to the bank's action. The insurer declined coverage, asserting an exclusion that barred coverage for claims arising from loss of electronic data. The trial court granted summary judgment in the insured's favor, holding that the insurer had a duty to defend the underlying action. The appellate court reversed in favor of the insurer, relying on the electronic data exclusion and the tangible property definition.

The universe of those affected by a data breach expands to a range of parties beyond those most commonly thought of as the victims – the holder of the information (the merchant) and the persons whose information is stolen (the customers). The above cases illustrate the types of other players in the stream of commerce that are often affected as a result of retailer data breaches. These include banks, credit card issuers and servicers, and credit card associations that have authority to impose or seek reimbursement for significant assessments, fines and other fees. Each type of entity may potentially seek coverage for such damages under its own policies or those of the breached entity, a process which is often complicated by the contractual obligations among them.

Illinois Simplifies Cumbersome Insurer Record Retention and Destruction Requirements

The Illinois Department of Insurance (IL DOI) has amended its record disposal and destruction regulation effective May 23, 2016, significantly reducing reporting, book-keeping and retention obligations for Illinois domestic insurers, as well as any principal U.S. office of a foreign or alien insurer located in Illinois. The amendment to Title 50, Section 901.20 of the Illinois Administrative Code, available [here](#), eliminates a cumbersome requirement that, prior to destruction, insurers submit to the IL DOI an affidavit signed by the company president and secretary listing records in their custody that are no longer needed for specified purposes, and request IL DOI authorization to destroy such records.

The amendment eliminates the reporting and approval requirements, and instead provides insurers with the authority to dispose of records that do not have sufficient administrative, legal or fiscal value to warrant their further preservation and are not needed: (a) in the transaction of current business; (b) for the final settlement or disposition of an insurance claim, except that these records must be maintained for the current year plus five years; or (c) to determine the financial condition of the company since the date of the last examination report, except that these records must be maintained for at least the current year plus five years. The adopted amendment tracks the IL DOI's previous proposed amendment, reported [here](#), except that the adopted amendment reduces the required retention period from seven to five years.

In its Notice of Adopted Amendment, the IL DOI states, "The Department recognized that the process outlined by this rule

was outdated, unnecessary, and not in line with other states' requirements." We would add that the adopted amendment is in furtherance of significant privacy and data protection goals: by streamlining insurers' ability to destroy claims files and other documents containing sensitive personal information, the amendment reduces the risk of unauthorized access to or acquisition of such information.

Insurance companies domiciled in Illinois, as well as any principal U.S. office of a foreign or alien insurer located in Illinois, should review and revise their record retention policies accordingly.

Recent UK Information Commissioner's Office (ICO) Fines and Investigations

Illegal sale of personal data

On June 8, 2016, the ICO raided a house in Sheffield in the belief that residents of the property were illegally selling personal data to marketing companies, which then use the personal data to make nuisance calls. The raid was made on the basis of information which the ICO had received through complaints from individuals and businesses about emails advertising databases of personal data for sale. The ICO investigation identified a business at the house in Sheffield as being the source of the emails. The ICO will not reveal the identity of the business whilst the investigation is on-going.

The ICO has emphasised that it is not illegal to sell lists of personal data, provided that the personal data was obtained lawfully and the owner of the list has the right to sell it (which is likely to mean, in practice, that it has the consent of the relevant data subjects to transfer their personal data to buyers of the list).

Leave.EU campaign group fined

Ahead of the June 23 vote concerning whether the U.K. would remain part of the EU, Better for the Country Ltd (also known as Leave.EU), the anti-European Union campaign group, was fined £50,000 by the ICO in May 2016 for sending more than 500,000 text messages urging individuals to vote for the UK to leave the EU, without the consent of the individuals to whom the messages were sent. The campaign group told the ICO that they had obtained the list of phone numbers from a third party. During the ICO investigation, it transpired that the individuals who were on the list had consented to receiving text messages about areas including leisure, home improvements and insurance – but had not consented to receiving text messages in relation to the campaign for the UK to leave the EU.

Before purchasing lists of personal data, companies must ensure that the third parties from whom they purchase the lists obtained the personal data lawfully in accordance with data protection legislation, that they have consent to sell the personal data, and that consent has been obtained allowing the purchaser to use the personal data for its specific purposes required after the purchase. Ideally, purchasers of these lists should obtain a corresponding indemnity from the seller.

Stephen Eckersley, the Head of Enforcement at the ICO, has [stated](#) that "Political parties and campaign groups must follow the same rules as anyone else. That means they must have people's permission before sending them text messages." (Emphasis added.)

U.S.-EU Privacy Shield Update

In the February Locke Lord Privacy & Cybersecurity Newsletter, we [reported](#) on the announcement of the new U.S.-EU Privacy Shield by the EU authorities and the U.S. Federal Trade Commission on February 2, 2016 and on the [publication](#) by the European Commission of the draft “adequacy decision” and draft texts intended to constitute the Privacy Shield.

On April 13, 2016, the Article 29 Working Party (a committee composed of representatives of each of the European Union Member States) adopted its [Opinion](#) on the draft text of the Privacy Shield, noting that the Working Party had “strong concerns” on both the commercial aspects of the text as well as on the rights of access granted to public authorities to personal data transferred under the Privacy Shield. The Working Party also advised that a further review of the text should take place after the entry into application of the General Data Protection Regulation (GDPR) in 2018. In concluding, the Working Party urged the European Commission to take its comments into consideration and to “improve” the draft adequacy decision to ensure that it provides protection to the same level as that offered by EU law.

On May 25, 2016, in a plenary session of the European Parliament, Members of European Parliament (MEPs) debated the draft adequacy decision, and on the following day they passed a non-binding resolution (passed by 501 votes to 119 with 31 abstentions) on the matter. In the resolution, MEPs voiced their concerns about the draft adequacy decision, such concerns mirroring those outlined by the Article 29 Working Party. Also in line with the Working Party’s recommendation was the MEPs’ recommendation that the European Commission should continue to review and negotiate the draft adequacy decision with U.S. authorities to ensure adequate protection of personal data under the Privacy Shield.

On May 30, 2016, the European Data Protection Supervisor (EDPS), Giovanni Buttarelli, published his [Opinion](#) on the Privacy Shield, which echoes the Article 29 Working Party’s concerns about the draft adequacy decision. Mr Buttarelli has [said](#):

“I appreciate the efforts made to develop a solution to replace Safe Harbor, but the Privacy Shield as it stands is not robust enough to withstand future legal scrutiny before the Court [of Justice of the EU]. Significant improvements are needed should the European Commission wish to adopt an adequacy decision, to respect the essence of key data protection principles with particular regard to necessity, proportionality and redress mechanisms. Moreover, it’s time to develop a longer term solution in the transatlantic dialogue.”

If the European Commission chooses to make further amendments as a result of the above views, this may well delay the final adoption of the adequacy decision. In order for the adequacy decision to be adopted, Article 31 Committee (which is comprised of representatives of the Member States and is chaired by the Commission) must give its approval before the decision can finally be adopted by the College of the EU Commission.

EEOC Update: New Wellness Program Regulations Create New Employer Obligations

New technologies and increased awareness of health-related costs continue to drive growing use of employee wellness programs, which can provide significant benefits to employers and employees alike. Accordingly, employers have long awaited the Equal Employment Opportunity Commission’s (EEOC) recently released regulations and guidance under the Genetic Information Nondiscrimination Act (GINA, regulation [here](#)) and Americans with Disabilities Act (ADA, regulation [here](#)), which help clarify how genetic and disability information may be collected and used in connection with employee wellness programs.

The ADA prohibits employment discrimination based on disability, and generally also prohibits asking employees about their medical conditions and requiring medical examinations. General prohibitions notwithstanding, the ADA historically permitted such inquiries so long as they were part of “voluntary” wellness programs. However, until now, the EEOC has not provided clear guidance as to what makes a wellness program voluntary. The new regulations fill this gap.

The regulations set forth the following four-part test for determining whether a wellness program is voluntary:

1. The program must not require employees to participate.
2. The program must not deny coverage under a group health plan for employees who do not participate.
3. Employers must not take adverse action, retaliate against, or coerce employees who do not participate.
4. Employers must provide notice regarding what medical information will be obtained, how it will be used, who will receive it, how its disclosure will be restricted, and how improper disclosure will be prevented.

In addition to the new standard for voluntariness, the regulations provide employees various other protections. An employer may only receive information collected by a wellness program in aggregate form, such that the employer cannot identify a particular individual associated with such information, except as necessary to administer a health plan. Additionally, employees generally cannot be required to waive confidentiality rights with respect to further sale, exchange, sharing, or other transfer in order to participate in the wellness program or receive an incentive for participation. Information about employees remains subject to the requirements of other laws that might govern its treatment, such as HIPAA. Finally, the regulations clarify that in order to maintain “voluntary” status, the financial incentives for participation in wellness programs generally cannot exceed 30% of what would be the total cost of self-only coverage (including both the employee’s and the employer’s contribution).

Wellness programs are likely to maintain their popularity with both employees and employers. As such, employers making use of those programs should be careful to ensure compliance with the new regulatory requirements and make provision for appropriate handling of employee information.

Increasing Necessity for a HIPAA Compliant “Business Associate Agreement” Within the Technology Industry

In recent years, the scope of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and implementing regulations has expanded dramatically, presenting new privacy and information security challenges to technology businesses intersecting with health care. Under HIPAA, companies providing domestic data storage services (including cloud service providers), e-prescribing gateways, and software or equipment used by a covered entity for the provision of healthcare services (including telemedicine / telehealth) fall within the scope of a “business associate” (BA), even if the company merely “maintains” protected health information (PHI) and does not personally view it. The definition of a BA also captures a BA’s downstream subcontractors that create, receive, maintain, or transmit PHI on its behalf. BAs are increasingly at risk of potential federal enforcement actions for noncompliance, specifically for the failure to enter into a business associate agreement (BAA) ensuring it will appropriately safeguard PHI (technical requirements for which are set forth under 45 C.F.R. § 164.504(e)).

The U.S. Department of Health and Human Services Office of Civil Rights’ (OCR) recent enforcement actions signal a BA’s failure to enter into a BAA may result in substantial monetary penalties. The OCR has recently reported three large settlements involving the failure to enter into BAAs:

- In April 2016 OCR [announced a \\$750,000 settlement](#) with a North Carolina orthopedic practice resulting from the failure to execute a BAA prior to providing PHI of 17,300 patients to a third party entity that promised to transfer the images to electronic media in exchange for harvesting the silver from the x-ray films. OCR initiated its investigation of the practice following its receipt of a breach report from the practice itself. Interestingly, the “breach” at issue was merely the fact that the covered entity released the information to the third party prior to executing a written BAA. OCR specifically stressed that “the lack of a business associate agreement left this sensitive health information without safeguards and vulnerable to misuse or improper disclosure.”
- In March 2016 OCR [announced a \\$1.55 million settlement](#) with a Minnesota healthcare system following its investigation of a breach report involving an unencrypted, password-protected laptop stolen from a BA’s employee’s locked vehicle, impacting the electronic PHI of 9,497 individuals. The covered entity failed to enter into a BAA with BA performing certain payment activities on its behalf. OCR’s

investigation revealed that from March 21, 2011 to October 14, 2011, the covered entity impermissibly disclosed the PHI of at least 289,904 individuals to the BA without obtaining satisfactory privacy and security assurances in the form of a written BAA. OCR further concluded that the covered entity failed to perform a risk assessment of all applications, software, databases, servers, workstations, mobile devices and electronic media, network administration and security devices, and associated business processes.

- In November 2015 OCR entered into a \$3.5 million [settlement against](#) an insurance holding company in San Juan, Puerto Rico. This settlement was the result of the covered entity’s self-reported multiple data breaches. One of the breaches involved the covered entity’s discovery that a vendor impermissibly disclosed its beneficiaries’ PHI (including the beneficiary’s names, mailing addresses, and Health Insurance Claim Number) on the outside of a pamphlet mailed to the beneficiaries. The covered entity, OCR alleged, did not have an appropriate BAA with the vendor and failed to conduct an accurate and thorough risk analysis incorporating all IT equipment, applications, and data systems utilizing electronic PHI (ePHI).

Although these settlements subjected the covered entity to punishment, future enforcement actions will likely target BAs. Indeed, OCR [expressed a particular interest](#) in BAs and BAAs through its release of new audit questions for 2016.

The OCR settlements provide two main lessons for BAs. First, as evidenced by the April 2016 settlement, the mere release of PHI to a third party prior to entering into a BAA constitutes a “breach” subject to potential civil liability. Second, internal security risk assessments are imperative. OCR implies appropriate risk assessments could have prevented the above-mentioned data breaches. HIPAA requires BAs to conduct thorough assessments of potential risks and vulnerabilities with the respect to the confidentiality, integrity, and availability of electronic PHI.

Accordingly, technology companies should be mindful of whether they are a BA and, if so, scrupulously adhere to HIPAA. When determining whether an entity is a BA, the key inquiries are (1) what services does the organization carry out for a covered entity and (2) what kind of data does the organization create, receive, maintain, or transmit. If a company’s services to the covered entity involve *anything* to do with PHI, it is likely a BA and must enter into a written BAA with the covered entity and also with downstream subcontractors involved in handling PHI. BAs should carefully scrutinize the terms of the BAA as many impose further heightened privacy and security requirements than HIPAA. When negotiating a BAA, a BA should be particularly attentive to provisions addressing the parties’ agency status, burdensome breach notification requirements and reporting deadlines, cost allocation of breach notification or investigation, and indemnification.



Practical Wisdom, Trusted Advice.

www.lockelord.com

Atlanta | Austin | Boston | Chicago | Cincinnati | Dallas | Hartford | Hong Kong | Houston | Istanbul | London | Los Angeles | Miami
Morristown | New Orleans | New York | Providence | Sacramento | San Francisco | Stamford | Tokyo | Washington DC | West Palm Beach

Locke Lord LLP disclaims all liability whatsoever in relation to any materials or information provided. This piece is provided solely for educational and informational purposes. It is not intended to constitute legal advice or to create an attorney-client relationship. If you wish to secure legal advice specific to your enterprise and circumstances in connection with any of the topics addressed, we encourage you to engage counsel of your choice. If you would like to be removed from our mailing list, please contact us at either unsubscribe@lockelord.com or Locke Lord LLP, 111 South Wacker Drive, Chicago, Illinois 60606, Attention: Marketing. If we are not so advised, you will continue to receive similar mailings. (070516)

Attorney Advertising © 2016 Locke Lord LLP