

**LABOR & EMPLOYMENT ALERT**

---

**NEW AMENDMENTS TO MASSACHUSETTS DATA PRIVACY REGULATIONS: COMPLIANCE DATE POSTPONED TO MARCH 1, 2010**

On August 17, 2009, the Massachusetts Office of Consumer Affairs and Business Regulation (OCABR) modified its *Standards for the Protection of Personal Information of Residents of the Commonwealth*, 201 CMR 17.00, *et seq.* (the “Standards”). For simplicity’s sake, I refer to the old, superseded *Standards* as the “Old Regulations” and the new, amended *Standards* as the “New Regulations.” OCABR has also issued a “Frequently Asked Questions”<sup>1</sup> (“FAQ”) and a press release<sup>2</sup> (“Press Release”) assisting navigation of the New Regulations.

The *Standards* impact all individuals, corporations, associations, partnerships and other legal entities “owning or licensing”<sup>3</sup> Massachusetts residents’ “Personal Information”,<sup>4</sup> irrespective of where they are located. I refer to all such individuals or entities as “Holders” for purposes of this article. Generally speaking, the *Standards* employ two primary safeguards to protect Personal Information: (1) each Holder must adopt a comprehensive written information security plan (a “WISP”); and (2) each Holder must comply with certain minimum computer system security requirements for systems storing or transmitting Personal Information.

The New Regulations are the latest in a series of changes to 201 CMR 17.00 since the *Standards* were first proposed during 2007.<sup>5</sup> The New Regulations successfully file the sharpest edges off some of the provisions that were vehemently opposed by business interests and stakeholders. In at least one critical area, however, OCABR has re-inserted a slightly-diluted version of a requirement that had been previously excised from the *Standards*. The following summarizes the most significant changes incorporated within the New Regulations:

---

<sup>1</sup> Frequently Asked Question Regarding 201 CMR 17.00,  
<http://www.mass.gov/Eoca/docs/idtheft/201CMR17faqs.pdf>

<sup>2</sup> OCABR Press Release, August 17, 2009,  
[http://www.mass.gov/?pageID=ocapressrelease&L=1&L0=Home&sid=Eoca&b=pressrelease&f=20090817\\_idtheftregs&csid=Eoca](http://www.mass.gov/?pageID=ocapressrelease&L=1&L0=Home&sid=Eoca&b=pressrelease&f=20090817_idtheftregs&csid=Eoca)

<sup>3</sup> OCABR’s new definition for the term is provided below in the main body of this article.

<sup>4</sup> Essentially meaning a resident’s name used in connection with an identification or account number, “personal information” is defined, in M.G.L. 93H and in the *Standards*, as “a Massachusetts resident’s first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver’s license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident’s financial account; provided, however, that “Personal information” shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.”

<sup>5</sup> The process is not over; there will be a public hearing on the changes on September 22, 2009.

## LABOR & EMPLOYMENT ALERT

---

- **COMPLIANCE TIMELINE DELAYED.** OCABR changed the required compliance date from January 1, 2010 to March 1, 2010, a delay of two months.<sup>6</sup> Moreover, a new contract provision discussed below provides some latitude for contracts dated before March 1, 2010.
- **AMENDED PURPOSE CLAUSE.** Minor changes to the “Purpose” clause set forth in Section 17.01(1) do not have a material impact on the substance of the *Standards*. Importantly, however, these changes mirror the enabling language of M.G.L. Ch. 93H, and thereby signal OCABR’s intention to follow the legislature’s statutory mandate more closely than it had with the Old Regulations.
- **DEFINITION LIMITS “HOLDERS” SUBJECT TO STANDARDS.** OCABR’s introduction of a new definition for the phrase “owns or licenses,” which is used prominently in Section 17.03(1), narrows the class of Holders to which the *Standards* will apply. “Owns or licenses” now means: “receives, maintains, processes, or otherwise has access to personal information in connection with the provision of goods or services or in connection with employment.” As explained in the FAQ, this language clarifies that the *Standards* will not apply “to natural persons who are not in commerce.” Specifically, if Personal Information is unrelated to employment and/or providing goods or services, then the *Standards* do not apply. However, since most Personal Information *is* connected to employment or providing goods or services, this clarification may have little practical impact, exempting only incidental Personal Information access.
- **“SERVICE PROVIDER” DEFINED.** The New Regulations define “service provider” as “any person that receives, maintains, processes, or otherwise is permitted access to personal information through its provision of services directly to a person that is subject to this regulation.”<sup>7</sup> Importantly, the definition provides two limits on potential classification as a “service provider;” specifically, a potential “service provider” must: (i) have some access to Personal Information; and (ii) directly provide services to a Holder.
- **FACTORS FOR RISK-BASED APPROACH.** Responding to criticisms that the Old Regulations permitted situation-specific analysis only as part of after-the-fact enforcement proceedings, OCABR restated its WISP requirement.<sup>8</sup> Old Regulations’ Section 17.03(2) required that a WISP be *evaluated* taking into account the following factors:
  - (a) the size, scope and type of business of the person obligated to safeguard the personal information under a WISP; (b) the amount of resources available to such person; (c) the amount of stored data; and (d) the need for security and confidentiality of the stored information.In the New Regulations, these factors are now hard-wired into the up-front WISP requirements.<sup>9</sup> This change permits those drafting a WISP to employ discretion that was formerly reserved for

---

<sup>6</sup> 201 CMR 17.05.

<sup>7</sup> OCABR’s definition also provides that “‘service provider’ shall not include the U.S. Postal Service.”

<sup>8</sup> As stated in the Press Release, such changes “make clear the regulations are risk-based in implementation, not just in enforcement as had been the case in earlier versions of the regulations.”

<sup>9</sup> In addition, Section 17.03(1) now provides that the WISP may be “written in one or more readily accessible parts.”

## LABOR & EMPLOYMENT ALERT

---

OCABR (or the Massachusetts Attorney General's office) in evaluating a WISP's compliance. Under the New Regulations, WISP safeguards must be appropriate in light of all the specified factors:<sup>10</sup>

“Whether it's a small amount of employee paperwork, or a large amount of consumer information kept on an electronic database, each requires its own appropriate level of security and protection....”<sup>11</sup>

- **TREATMENT OF SERVICE PROVIDERS.** A *Standards* version pre-dating the Old Regulations required that Holders negotiate contract provisions regarding *Standards* compliance with, and obtain a certification of compliance from, service providers.<sup>12</sup> In February 2009, OCABR eliminated the contract and certification requirements. OCABR has essentially re-inserted the contract requirement within New Regulations Section 17.03(2)(f)(2) (albeit with a somewhat different approach modeled after the FTC's Safeguards Rule<sup>13</sup>).<sup>14</sup> Holders are now required to “oversee service providers” by

(1) “taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such personal information consistent with these regulations and any applicable federal regulations”<sup>15</sup> and

(2) “requiring such third-party service providers by contract to implement and maintain such appropriate security measures for personal information....”

This re-inserted contract requirement contrasts with the New Regulations' predominantly less prescriptive approach and may impose new transactional costs on Holders and service providers alike.

- **LIMITED EXEMPTION TO CONTRACT REQUIREMENT.** Though not a model of clarity, the following Section 17.03(2)(f)(2) proviso appears to provide a compliance ramp-up period, exempting from compliance contracts entered into before March 1, 2010; the exemption sunsets March 1, 2012:

“... provided, however, that any contract a person has entered into with a third-party service provider prior to March 1, 2012, shall be deemed to be in compliance herewith, notwithstanding the absence in any such contract of a requirement that the service provider maintain such protective security measures, so long as the contract was entered into before March 1, 2010.”

Section 17.03(2)(f)(2) has been structured in this way to: (1) avoid requiring contract amendments by March 1, 2010 before the *Standards* take effect; and (2) prevent Holders' side-stepping the *Standards*' goals by entering into long-term contracts before March 1, 2010. Except as noted, the contract requirement is absolute for all Holders.

---

<sup>10</sup> The need for security and confidentiality of “stored information” has been revised to “both consumer and employee information” in the New Regulations.

<sup>11</sup> See the Press Release, quoting OCABR Undersecretary Barbara Anthony.

<sup>12</sup> The *Standards*' old contract and certification requirement (201 C.M.R. 17.03(f) dated November 14, 2008) stated as follows: “[WISPs shall include ... Taking reasonable steps to verify that third-party service providers with access to personal information have the capacity to protect such personal information, including (i) selecting and retaining service providers that are capable of maintaining safeguards for personal information; and (ii) contractually requiring service providers to maintain such safeguards. Prior to permitting third-party service providers access to personal information, the person permitting such access shall obtain from the third-party service provider a written certification that such service provider has a written, comprehensive security program that is in compliance with the provisions of these regulations.”

<sup>13</sup> 16 CFR Part 314.

<sup>14</sup> See the FAQ.

<sup>15</sup> OCABR has clarified that the exhaustive “all reasonable steps” seemingly required by the Old Regulations are not required under the New Regulations – only reasonable steps.

## LABOR & EMPLOYMENT ALERT

---

- ***GOOD BUSINESS PRACTICES NO LONGER REGULATED.*** As OCABR points out in its FAQ, the Old Regulations’ “good business practice” requirements have been omitted from the *Standards*. Among others, Old Regulations Sections 17.03(7) (limiting information collection and retention) and 17.03(8) (requiring Personal Information inventory) have been deleted. Since identifying Personal Information subject to the *Standards* and minimizing Holders’ Personal Information inventory are obvious compliance steps, OCABR has reconsidered mandating them, noting they “will be used as a form of guidance only.”<sup>16</sup>
- ***“TECHNICALLY FEASIBLE” LIMITATION.*** OCABR left the *Standards*’ Section 17.04 computer system security requirements generally untouched – with one exception: the New Regulations move the “to the extent technically feasible” caveat to a more Holder-friendly location. Specifically, this caveat, which was formerly linked to the narrow transmittal encryption requirement,<sup>17</sup> now stands as an overarching technical feasibility limitation for computer system security. The FAQ defines this feasibility concept:

“Technically feasible” means that if there is a reasonable means through technology to accomplish a required result, then that reasonable means must be used.”

Technical requirements for establishing and maintaining *Standards*-compliant security for Holders’ computer systems remain substantially the same; the “technically feasible” limitation effectively and sensibly provides that if the technology is not reasonably available for use, then Holders are not required to implement it. Personal Information security, however, must be maintained irrespective of the feasibility of a particular technology. The FAQ stresses that protecting Personal Information may require that Holders apply alternative “best practices” approaches that *are* technically feasible (or are not “technical” at all).<sup>18</sup>
- ***“ENCRYPTION” REDEFINED.*** Changes to the definition of “encrypted” now permit Holders to use a wider array of defensive technologies. While the Old Regulations required an algorithmic encryption process, the New Regulations require only that data be altered to a state “in which meaning cannot be assigned without the use of a confidential process or key.”<sup>19</sup> Although a confidential process or key is still required, the New Regulations do not mandate an algorithmic lock. By broadening the encryption standard, OCABR has significantly eased the encryption requirements in the Old Regulations, making them, (per the FAQ):

“technology neutral so that as encryption technology evolves and new standards are developed, this regulation will not impede the adoption of new technologies.”

Despite the change, equating “encrypted” with “password-protected” remains ill-advised since password protection does not alter the underlying data but only restricts access to it.

The New Regulations generally retreat from the more formal and prescriptive provisions of the Old Regulations. The New Regulations impose a regulatory burden upon Holders that is more consistent with

---

<sup>16</sup> *Id.*

<sup>17</sup> 201 CMR 17.04(3).

<sup>18</sup> The FAQ counsels that the *Standards* require “encryption of portable devices where it is reasonable and technically feasible” and notes that Section 17.04 “should be construed in accordance with the risk-based approach” used in the *Standards*.

<sup>19</sup> 201 CMR 17.02.

## LABOR & EMPLOYMENT ALERT

---

that originally sought by the Massachusetts legislature; specifically, M.G.L. 93H's original statutory language is more closely tracked; Holders are now permitted flexibility for *Standards* compliance; and various technical security and encryption requirements are more realistically limited.

Nevertheless, Holders still must be vigilant! The new compliance deadline of March 1, 2010 looms in the not-too-distant future and requires Holders' full compliance with all except the "service provider" contract requirement (which, as discussed previously, operates prospectively for contracts entered into on March 1, 2010 and beyond).

*For more information, contact Michael C. Hackett at [mhackett@eckertseamans.com](mailto:mhackett@eckertseamans.com) or 617-342-6835. Mr. Hackett is a corporate attorney in the Business Division of Eckert Seamans Cherin & Mellott, LLC's Boston office. In addition, you may contact any other Eckert Seamans Cherin & Mellott, LLC attorney with whom you have been working.*

NOTE: The information in this Alert is for general, educational purposes. It is not intended to be, and should not be considered, legal advice with respect to any particular situation.

© Eckert Seamans Cherin & Mellott, LLC, 2009, all rights reserved.