

## **Ten Things Massachusetts Non-Profit Employers Should Know About the New CORI Regulations**

by

David C. Henderson and Sarah D. Kohrs

New Criminal Offender Record Information (CORI) regulations will take effect on May 4, 2012. Many non-profit employers, especially those in the human and youth services, educational and health care fields, are highly reliant on CORI information in making employment decisions. Portions of the regulations most relevant to Massachusetts employers explain (a) a new, secure, web-based service for obtaining criminal offender information; (b) restrictions on that use of information; and (c) penalties of using the information illegally. Key points to remember are these:

### **1. Employers or their agents must register for an iCORI account in order to obtain CORI.**

The new, secure, web-based service for obtaining criminal offender information is named iCORI. Any employer desiring to screen employees or applicants based on CORI must register for an iCORI account. To register, the employer must (a) provide information that identifies the individual user and the organization or business; (b) provide information regarding the purpose for requesting CORI; (c) pay a registration fee;<sup>1</sup> and (d) designate an individual to access the account. The designated individual must undergo training and agree to iCORI terms and conditions. 803 CMR 2.04(2).

The iCORI account will expire after one year. For information after that, the employer must renew its registration. 803 CMR 2.04(6).

### **2. All employers will have at least “Standard Access” to CORI, allowing them to access more information than the general public. Certain employers authorized to receive CORI by a statute, regulation or accreditation requirement will have even greater access to CORI.**

All employers receive “standard access” to applicant or employee CORI and thus will have access to (a) all pending criminal charges; (b) all misdemeanor convictions from the past five years; (c) all felony convictions from the past ten years; and (d) all convictions for murder, voluntary manslaughter, involuntary manslaughter, and sex offenses. 803 CMR 2.05(4)(a).

Juvenile, civil, sealed, and non-incarcerable convictions, as well as offenses for which the subject was not convicted, are not included under “standard access,” but are included under “required access.” Employers that are authorized to receive CORI by a statute, regulation, or accreditation requirement are entitled to “required access.” 803 CMR 2.05.

---

<sup>1</sup> The Department of Criminal Justice Information Systems (DCJIS) is charged with implementing the new CORI law. Although the Regulations say that an employer “may” be required to pay a registration fee, DCJIS states on its website that a fee will be required.

**3. Employers must document notifying the current or prospective employee before obtaining CORI and must retain the documentation.**

Before submitting a CORI request, the employer must (a) submit a CORI Acknowledgement Form for each subject to be checked; (b) verify the identity of the subject; (c) obtain the subject's signature on the CORI Acknowledgement Form; and (d) sign and date the CORI Acknowledgement Form certifying that the subject was properly identified. 803 CMR 2.09(1).

CORI Acknowledgement Forms are valid for one year, or until the conclusion of the subject's employment, whichever comes first. 803 CMR 2.09(9).

An Acknowledgement Form must be retained for one year after the subject signs it. 803 CMR 2.09(12).

An employer may submit a new request for CORI as long as (a) the CORI Acknowledgement Form is still valid; (b) the employer provides the subject with 24 hours written notice; and (c) the subject does not object to the request. If the subject objects, the Acknowledgement Form becomes invalid. 803 CMR 2.09(9)(a) and (c). But the employer is permitted to make an adverse employment decision on the basis of a subject's objection to a request for CORI information. 803 CMR 2.09(10).

Verification of the subject's identity must be accomplished by examining government-issued identification, such as a state-issued driver's license, a state-issued identification card with a photograph, a passport, or a military identification. 803 CMR 2.09(3).

After verifying identity, the employer will input into the iCORI system the subject's name, date of birth, and the last six digits of the subject's social security number. 803 CMR 2.09(6). The system will not return CORI unless the submitted information matches information already in the iCORI system. 803 CMR 2.09(7).

**4. CORI usually will be delivered electronically.**

Where possible, CORI information will be provided electronically through the requestor's iCORI account. 803 CMR 2.10. Where electronic information is not available, a manual search will be conducted and a response will be mailed upon completion of the search. 803 CMR 2.10.

**5. CORI must be stored and destroyed in a way that ensures confidentiality.**

Hard copies of CORI must be stored in a separate locked and secure location. Electronic copies must be password-protected and encrypted. Only those employees who have been approved by the employer may have access to the CORI records. 803 CMR 2.11(1) and (2).

CORI may not be retained for longer than seven years from date of employment or date of the employer's final decision regarding the subject. 803 CMR 2.11(3).

Employers must destroy hard copies of CORI by shredding or otherwise , and must destroy electronic copies of CORI by deleting them from the hard drive on which they are stored and from any back-up system. 803 CMR 2.12(1) and (2).

**6. Employers may disseminate CORI only in limited circumstances and must keep a log if there is dissemination outside the employer's organization.**

Employers generally are prohibited from disseminating CORI. The three limited exceptions to that rule are (a) when disseminating to the subject, (b) when the employer is sued as a result of a decision based on CORI (allowing dissemination only to the court or administrative agency involved), and (c) to the employer's staff members authorized to review the information for purposes of evaluating the subject's application for employment. 803 CMR 2.14.

If the employer disseminates CORI outside its own organization, it must record the dissemination in a log containing (a) the subject's name and date of birth; (b) the date and time of dissemination; (c) the name of the person or entity to whom the information was disseminated; and (d) the specific reason for dissemination. 803 CMR 2.16(1) and (2).

The log may be electronic or on paper, and it must be maintained for at least one year. 803 CMR 2.16(3)-(5).

**7. An employer that bases an adverse employment decision on CORI or other criminal history information must comply with additional procedures.**

When an employer makes an adverse employment decision based on CORI or other criminal history information, it must (a) comply with all applicable law; (b) notify the applicant<sup>2</sup> of the potential adverse action; (c) provide the applicant with a copy of the CORI or criminal history information; (d) provide the applicant with a copy of the employer's CORI policy, if applicable; (e) provide the employment applicant with the opportunity to dispute the accuracy of the information; (f) provide the applicant with a copy of the Department of Criminal Justice Information System's process for correcting CORI or criminal records; and (g) document all steps taken to comply with these requirements.

**8. There are additional procedural requirements when a consumer reporting agency obtains CORI for an employer.**

If an employer uses a consumer reporting agency to obtain CORI, it must notify the applicant and obtain the applicant's written consent. 803 CMR 2.21(1)(a).

Also, the employer must certify to the agency that (a) the employer is in compliance with the Federal Fair Credit Reporting Act; (b) the employer will not use the information obtained illegally; and (c) the employer has provided accurate information about the subject. 803 CMR 2.21(1)(b).

---

<sup>2</sup> The Regulations use the word "applicant"; it is not clear whether the requirements of this section would apply if the employer is making an adverse employment decision regarding a current employee.

Further, before making an adverse decision based on information obtained from a consumer reporting agency, the employer must follow steps similar to those it would follow if it had obtained the information directly. 803 CMR 2.21(2) and (3).

9. **Requests for CORI may be audited by the Department of Criminal Justice Information Services.**

The new regulations empower DCJIS to audit all CORI requests. 803 CMR 2.22(1). Failure to cooperate with, or respond to, an audit may result in revocation of CORI access. 803 CMR 2.22(2). During an audit, DCJIS is entitled to inspect CORI Acknowledgement Forms, secondary dissemination logs, the organization's CORI policy, and documentation of adverse employment decisions based on CORI. 803 CMR 2.22(3). Audit results may be published. 803 CMR 2.22(5). Additionally, the DCJIS may file a complaint against a non-complying entity, or refer the results of the audit to law enforcement for criminal investigation. 803 CMR 2.22(6) and (7).

10. **The new regulations establish a Criminal Records Review Board empowered to investigate and punish CORI violations.**

The Criminal Records Review Board (CRRB) has authority to hear or dismiss a complaint brought by DCJIS against an entity allegedly violating CORI law. 803 CMR 2.27(5)(a) and (h). The CRRB also may (a) revoke access to CORI; (b) impose civil fines of up to \$5000 for each knowing CORI violation; and (c) refer any complaint to state or federal criminal justice agencies for criminal investigation. 803 CMR 2.27(5)(j), (k), and (l).<sup>3</sup>

---

*This article was prepared by David C. Henderson and Sarah D. Kohrs. Both David and Sarah are members of the Labor, Employment and Benefits practice group at Nutter McClennen & Fish LLP. For more information, please contact David at 617.439.2345 and [dhenderson@nutter.com](mailto:dhenderson@nutter.com) or Sarah at 617.439.2725 and [skohrs@nutter.com](mailto:skohrs@nutter.com).*

2101957.1  
2104991.1

---

<sup>3</sup> If criminal charges are brought, penalties that can be imposed by a court include "imprisonment in a jail or house of correction for not more than 1 year or by a fine of not more than \$5,000 or by both such fine and imprisonment, and in the case of an entity that is not a natural person, the amount of the fine may not be more than \$50,000 for each violation." M.G.L. c. 6, § 178.