



Commonwealth of Massachusetts  
Office of the State Auditor  
Suzanne M. Bump

*Making government work better*

Official Audit Report – Issued July 1, 2014

---

## Board of Registration in Medicine

For the period July 1, 2010 through June 30, 2012





Commonwealth of Massachusetts  
Office of the State Auditor  
Suzanne M. Bump

*Making government work better*

July 1, 2014

Barbara Piselli, Acting Executive Director  
Board of Registration in Medicine  
200 Harvard Mill Square, Suite 330  
Wakefield, MA 01880

Dear Ms. Piselli:

I am pleased to provide this performance audit of the Board of Registration in Medicine. This report details the audit objectives, scope, methodology, findings, and recommendations for the audit period, July 1, 2010 through June 30, 2012. My audit staff discussed the contents of this report with management of the agency, and their comments are reflected in this report.

I would also like to express my appreciation to the Board of Registration in Medicine for the cooperation and assistance provided to my staff during the audit.

Sincerely,

A handwritten signature in blue ink, appearing to read "SMB", written in a cursive style.

Suzanne M. Bump  
Auditor of the Commonwealth

**TABLE OF CONTENTS**

<b>EXECUTIVE SUMMARY .....</b>	<b>1</b>
<b>OVERVIEW OF AUDITED AGENCY .....</b>	<b>5</b>
<b>AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY .....</b>	<b>6</b>
<b>DETAILED AUDIT RESULTS AND FINDINGS WITH AUDITEE’S RESPONSE .....</b>	<b>10</b>
1. Collection of information regarding physician criminal activity is ineffective.....	10
2. The Board should improve its website to enhance access to physician information. ....	16
3. The Board has no record of an information security program, electronic security plan, or Self-Assessment Questionnaire. ....	19
4. The Board did not comply with the Payment Card Industry Data Security Standard. ....	21
5. Prior audit result partially resolved—The Board has developed a business continuity plan but has not updated it. ....	23
<b>APPENDIX A .....</b>	<b>25</b>
<b>APPENDIX B .....</b>	<b>27</b>
<b>APPENDIX C .....</b>	<b>28</b>
<b>APPENDIX D .....</b>	<b>29</b>
<b>APPENDIX E .....</b>	<b>32</b>
<b>APPENDIX F .....</b>	<b>33</b>
<b>APPENDIX G .....</b>	<b>34</b>
<b>APPENDIX H .....</b>	<b>35</b>
<b>APPENDIX I .....</b>	<b>38</b>
<b>APPENDIX J .....</b>	<b>40</b>

## EXECUTIVE SUMMARY

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws, the Office of the State Auditor has conducted a performance audit of certain activities of the Board of Registration in Medicine (the Board) for the period July 1, 2010 through June 30, 2012. For our objective regarding the processing of mandated reports, we extended our audit period to January 1, 2002 through December 31, 2012. The objectives of our audit were to review and evaluate the Board's internal controls and its compliance with applicable laws, regulations, policies, and procedures in the following areas: (1) physician licensing, physician online profiles, investigation of complaints, hearings, and sanctions for misconduct; (2) the processing of mandated reports received on physician misconduct, disciplinary actions, and medical-malpractice matters; (3) physician training on how to report suspected child abuse; (4) the sharing of physician information with other states and the federal government as required by 243 Code of Massachusetts Regulations 1.02(11); (5) system access controls over the Consolidated Licensing and Regulation Information System and the OnBase application system; (6) controls over the processing of credit-card transactions; (7) expenditures for contract services related to information technology (IT); (8) employee background Criminal Offender Record Information (CORI) checks; (9) safeguarding of IT-related equipment; and (10) whether the Board implemented the necessary corrective actions to address the issues raised in our previous audit report (No. 2008-0117-4T).

### *Summary of Findings*

- The Board did not collect from the trial courts and report all physician criminal activity in accordance with Chapter 112, Section 5, of the General Laws. As a result, the Board cannot be certain that its online individual physician profiles are complete and accurate, which could affect the public's ability to make informed decisions about physicians they are considering using as healthcare providers. The absence of complete criminal activity information hinders the Board's ability to discern any patterns of improper behavior among physicians and may preclude it from taking disciplinary actions.
- Information on the Board's website, which is the Board's primary means of disseminating information on disciplinary and/or criminal actions to the public, needs to be enhanced to ensure that the public will have complete and relevant information on which to base decisions about physicians. Otherwise, information about disciplinary actions taken by the Board may not be available to the public.
- During our audit period, the Board had not completed the 2011 and 2012 annual Self-Assessment Questionnaires to report the results of the self-audit required by the Commonwealth's Executive Office for Administration and Finance (EOAF). Further, the Board

had not submitted an information security program (ISP) or an electronic security plan as required in Sections 3 and 4 of Commonwealth Executive Order 504 (EO504). Without completing these documents, the Board cannot be certain that it has taken the measures necessary to reasonably ensure the security, confidentiality, and integrity of personal information residing on its application systems.

- The Board did not meet certain requirements for compliance with the Payment Card Industry Data Security Standard (PCI DSS), according to a November 2011 report prepared by Compass IT Compliance, LLC, a certified Qualified Security Assessor (QSA). Although the Board does not store cardholder data once transactions are completed, not meeting the PCI DSS requirements risks a security breach during the processing of transactions, including the fraudulent use of cardholder data. Further, a security breach of cardholder data under federal law could expose the Board to potential fines and penalties as well as adverse publicity.
- Our prior audit report (No. 2008-0117-4T) revealed that the Board did not have a formal business continuity plan (BCP) as required by Executive Order 490. Accordingly, we recommended that the Board work with the Commonwealth's Information Technology Division (ITD) to develop formal approved business continuity and disaster recovery plans that are tested at least annually. Our current audit indicated that the Board implemented our prior audit recommendation to develop a BCP; however, the Board has not updated its BCP since 2009. The absence of an updated BCP could hinder or prevent the Board from restoring computer operations in the event of unforeseen interruptions in business operations. Specifically, the lack of a BCP may cause delays in processing physician licenses and in updating physician profiles with disciplinary actions taken by the Board. Further, the Board may not be able to ensure continuity and sustainability of its operations without an up-to-date BCP.

### ***Recommendations***

- The Board should collaborate with the Executive Office of the Trial Court (EOTC) in order for EOTC to devise and implement a reporting system and develop related policies, procedures, and internal controls to ensure that court-mandated reports on physician criminal activity are routinely collected and reported to the Board. The Board should use the information it receives from EOTC to make timely updates to individual physician profiles for the public's use in accordance with Chapter 112, Section 5, of the General Laws. The development and implementation of a reporting system that provides for the consistent reporting of physician criminal activity should enable the Board to better ensure the public's safety and welfare by docketing complaints against physicians who have engaged in misconduct and by taking appropriate disciplinary action.
- To ensure that the Board has a complete record of physician criminal activity, the Board should conduct a CORI check when a physician submits his or her initial application for a license to practice medicine in the Commonwealth. By conducting this CORI check, the Board could identify any criminal activity before granting an individual a physician's license.
- The Board should update and periodically review its website to ensure consistency in the reporting of license status and disciplinary actions.

- The Board should ensure the consistent reporting of information between the Disciplinary and Other Board Actions sections of its website and related comments within the online physician profile. The physician profile should include an appropriate description of any disciplinary action or other action taken by the Board.
- The Board should correct the initial lookup section of its website to ensure that physicians with a license status of Active (Subject to Restrictions) appear correctly in the initial lookup screen rather than displaying the misleading status of Active.
- When reviewing allegations against a physician, the Board should modify its generic description of Profile Is in the Process of Being Updated to include language that better informs the public that there could be an issue with the status of the physician's license.
- The Board's information security officer (ISO), in conjunction with the Department of Public Health (DPH), should immediately begin an annual review of all IT-related security controls in place and file all required reports with ITD. If the Board needs guidance in this area, the ISO should consider reviewing EOAF's "Instructions for Completing and Submitting Agency Executive Order 504 Information Security Program (ISP) and Electronic Security Plan (ESP)." If necessary, the Board and ISO should seek assistance from ITD to assist in the completion of the required reports.
- The Board should develop policies and procedures and related internal controls to ensure compliance with PCI DSS. Completion of the EO504 ISP should help with this compliance.
- The Board should work with ITD to ensure that all requirements and protections identified in its risk assessment are addressed and tested by the QSA.
- The Board should annually test the controls it has established to track and monitor all access to network resources and cardholder data, regularly test security systems and processes, and regularly review and update its policies and procedures in this area as necessary.
- In collaboration with DPH, the Board should update its BCP to include all changes to its technology environment as well as changes to the emergency contact list since its prior plan. To that end, the Board should assess the extent to which it is dependent upon the continued availability of information systems for all required computer processing and operational needs and should develop its recovery plans based on the critical aspects of its information systems. The plan should be tested and the results incorporated into the current plan.
- The Board should identify an emergency relocation site to use should the Board's offices be rendered inaccessible by an unforeseen event.

### ***Agency Progress***

- As a result of an amendment to Chapter 112, Section 5(c), of the General Laws contained in Outside Section 115 of the fiscal year 2013 budget, the Board no longer purges its database of disciplinary actions 10 or more years old taken by healthcare facilities against physicians. During our audit, the Board added the date of any disciplinary action to the physician's profile, which

will enable the public to cross-reference and more easily locate actions taken by the Board in the Disciplinary and Other Board Actions section of its website. The Board has also taken corrective action to add the missing archived disciplinary actions to the Disciplinary and Other Board Actions section of its website for the period 2002 through 2009.

- During our examination of controls over logical access security and personally identifiable information, we confirmed that the Board has addressed the issues of developing and maintaining secure system applications, restricting physical access to cardholder data, and establishing a unique ID for each person with computer access.
- Since the completion of our audit, the Board has updated its BCP, continuity-of-operations plan, and emergency contact list as of November 2012; however, the updated plans do not include an emergency relocation site.

## OVERVIEW OF AUDITED AGENCY

### *Background*

The Board of Registration in Medicine (the Board) is a state agency that, under its enabling statute (Chapter 13, Section 10, of the Massachusetts General Laws), is responsible for licensing physicians and acupuncturists (collectively referred to here as physicians) within the Commonwealth. The Board was established in 1894 and resides administratively within the Department of Public Health, but retains a high level of statutorily mandated autonomy. The Board has five major divisions: the Licensing Division, the Enforcement Division, the Division of Law and Policy, the Quality and Patient Safety Division, and the Operations Division.

The Board's mission is to help ensure that only qualified and competent physicians are licensed to practice in the Commonwealth and to foster an atmosphere that provides the highest-quality health care. According to the Board's page on the Commonwealth's Executive Office of Health and Human Services (EOHHS) website,

*The Board of Registration in Medicine's mission is to ensure that only qualified physicians are licensed to practice in the Commonwealth of Massachusetts and that those physicians and health care institutions in which they practice provide to their patients a high standard of care, and support an environment that maximizes the high quality of health care in Massachusetts.*

The Board is overseen by a seven-member board appointed by the Governor. Pursuant to Chapter 112, Section 2, of the General Laws, the Board is responsible for the registration of physicians; alien applicants;<sup>1</sup> examinations; license renewals; monitoring of required professional malpractice liability insurance; and collection of associated fees such as license verification and lapsed license fees. EOHHS's Information Technology department is ultimately responsible for managing all of the Board's technology requirements, including support services. The Board has two mission-critical applications: Consolidated Licensing and Regulation Information System (CLARIS) and OnBase. CLARIS provides access to comprehensive physician licensure information, and OnBase contains scanned copies of supporting documentation. In addition, the Board maintains a website that provides the public with physician profile information including any disciplinary actions. The website also allows physicians to renew their licenses and update address information.

---

<sup>1</sup> An alien applicant is an applicant who has received, from a medical school legally chartered in a sovereign state other than the United States, the commonwealth of Puerto Rico, or Canada, a degree of Doctor of Medicine or its equivalent.



## **AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY**

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws, the Office of the State Auditor (OSA) has conducted a performance audit of certain activities of the Board of Registration in Medicine (the Board) for the period July 1, 2010 through June 30, 2012. It was necessary to extend our audit period to January 1, 2002 through December 31, 2012 in order to meet our audit objective regarding mandated reports.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The objectives of our audit were to review and evaluate the Board's internal controls and its compliance with applicable laws, regulations, policies, and procedures in the following areas: (1) physician licensing, physician online profiles, investigation of complaints, hearings, and sanctions for misconduct; (2) the processing of mandated reports received on physician misconduct, disciplinary actions, and medical-malpractice matters; (3) physician training on how to report suspected child abuse; (4) the sharing of physician information with other states and the federal government as required by 243 Code of Massachusetts Regulations (CMR) 1.02(11); (5) system access controls over the Consolidated Licensing and Regulation Information System (CLARIS) and the OnBase application system; (6) controls over the processing of credit-card transactions; (7) expenditures for contract services related to information technology (IT); (8) employee background Criminal Offender Record Information (CORI) checks; (9) safeguarding of IT-related equipment; and (10) whether the Board implemented the necessary corrective actions to address the issues raised in our previous audit report (No. 2008-0117-4I). To achieve our audit objectives, we performed the following audit procedures:

- We conducted interviews with Board management and reviewed various records to determine to what extent management had addressed the concerns that OSA identified during our prior audit of the agency.
- We examined the Board's process for issuing full licenses to physicians, as well as timely handling of mandated reporting and the sharing of physician-related information with other states and the federal government. To accomplish this, we interviewed management, obtained

and reviewed copies of licensing and disciplinary-action policies and procedures, reviewed physician profiles and reports of disciplinary actions on the Board's website, verified information stored in CLARIS, and obtained and reviewed documentation scanned into OnBase, as well as taking the following actions:

- (1) To assess the Board's physician licensing process, we used audit command language (ACL) software to generate a sample of 47 physicians out of a total population of 16,063 in order to obtain and review copies of the initial or renewal physician license applications to compare with the minimum requirements for licensure identified in the General Laws.
  - (2) We generated a sample of 217 out of a population of 4,846 mandated reports for our audit period to test whether mandated reports<sup>2</sup> were received by the Board and whether the Board investigated them in a timely manner by reviewing the physician profiles to verify that the Malpractice and/or Massachusetts Criminal Actions sections on its website included the appropriate comments.
  - (3) To verify the accuracy of the Board's physician profile database with regard to criminal activity, we compared the total population of physicians reported by the Department of Criminal Justice Information Services as having either a conviction or a continuation without a finding<sup>3</sup> to the information on the Board's website. During our audit period, Board practice was to purge certain profile information that was 10 or more years old. In order to effectively test protocols for mandated court reporting of criminal activity by physicians as well as to capture all available data, we modified our audit period in this area to include the period January 1, 2002 through December 31, 2012.
  - (4) We selected and tested a judgmental sample of 20 out of a total population of 192 complaints included in mandated reports to determine the timeliness of the Board's response by comparing the referral memo date<sup>4</sup> on the mandated claim report to the date of the Board's initial review to determine the number of days before the Board took action.
  - (5) We selected and tested a judgmental sample of 20 physicians listed in the Board's disciplinary action report for the period July 1, 2010 through June 30, 2012 from a total population of 137 to verify that the Board is sharing information regarding disciplinary actions with other states and the federal government in accordance with 243 CMR 1.02(11). Our testing included obtaining and reviewing copies of report forms filed with the Federation of State Medical Boards and the U.S. Department of Health and Human Services' Data Bank.
  - (6) We interviewed senior management and reviewed available documentation to identify requirements that physicians take specific training to identify and report suspected cases of child abuse to the appropriate agency as a condition for licensure.
- We gained an understanding of the Board's policies and procedures related to the collection of physician license fees paid by either check or credit card. We used ACL software to generate a

---

<sup>2</sup> Mandated reports include peer reports, reports of healthcare-facility privileges, reports of disciplinary actions, and annual summaries of disciplinary reports.

<sup>3</sup> A court order, following a formal submission and acceptance of a plea of guilty or an admission to sufficient facts, whereby a criminal case is continued to another date without the formal entry of a guilty finding.

<sup>4</sup> The date a claim is submitted to the Board for investigation.

statistical sample of 94 transactions (47 checks and 47 credit cards) from a total population of 26,083 to ensure that adequate controls were in place for (1) processing of checks received for new license applications and (2) compliance with payment card industry (PCI) standards related to credit-card renewals of existing licenses.

- We reviewed and analyzed IT-related contracts / statements of work and compared deliverables to hours billed on approved timesheets to determine whether expenditures were allowable.
- To determine whether the inventory system of record for computer equipment was current, accurate, and complete, we used ACL software to select a non-statistical sample of 54 desktops, monitors, and printers out of a total population of 295 items. We also reviewed the total population of 43 laptops and 13 tablets to determine whether they were included on the inventory list and had the appropriate acknowledgment form signed by the assigned user. To evaluate the accuracy of the inventory system of record, we verified the locations, descriptions, inventory tags, and serial numbers of the hardware items listed on the inventory record by observing the actual computer equipment. To verify the integrity and completeness of the Board's system of record for computer equipment, we randomly selected 52 additional computer hardware items in locations adjacent to our original inventory sample and determined whether they were properly recorded on the Board's inventory list. Finally, to determine whether the Board was in compliance with Chapter 647 of the Acts of 1989's reporting requirements,<sup>5</sup> we reviewed incident reports for missing or stolen IT equipment for the audit period and determined whether these incidents were reported to OSA.
- To determine whether logical access security controls were in place and in effect, we reviewed and verified the administration of login IDs, passwords, and selected control practices regarding logical access to network resources. To assess whether all users with active privileges were current employees, we obtained system-generated user lists of individuals granted access privileges to CLARIS and OnBase and compared those lists to the Board's list of current employees and outsourced staff. Furthermore, we reviewed password configuration policies and determined whether all persons authorized to access information system resources were required to change their passwords periodically and, if so, how often these changes occurred.
- To determine the Board's ability to comply with PCI standards, we reviewed industry data security policies and interviewed management to determine whether the Board used an authorized financial institution for the processing of credit-card transactions. We also verified that the Board obtained the services of Compass IT Compliance, LLC, a certified Qualified Security Assessor, to validate its annual PCI compliance activity on an ongoing basis.
- To determine the Board's compliance with respect to the handling of personally identifiable information (PII), we reviewed Commonwealth Executive Order 504 and Chapter 93H of the General Laws to identify state agencies' responsibilities regarding protection of PII and notification of confidentiality breaches. We reviewed internal policies and procedures and conducted a walkthrough of various storage locations to determine whether the Board maintained controls to protect the integrity and confidentiality of electronic and hardcopy PII.

---

<sup>5</sup> Chapter 647 of the Acts of 1989, An Act Relative to Improving the Internal Controls within State Agencies, requires agencies to file a report with OSA if they find any "unaccounted for variances, losses, shortages or thefts of funds or property."

With regard to the protection of PII, we interviewed senior management to verify compliance with the Commonwealth's requirement of completing an information security program, electronic security plan, and Self-Assessment Questionnaire.

- We gained an understanding of 803 CMR and Executive Order 495 regarding the requirement of performing a CORI check as a condition of either employment or changes in job responsibilities. To determine the Board's compliance with this requirement, we interviewed senior management and reviewed the Board's procedures and control practices. We tested a non-statistical sample of 24 employees, obtained with the ACL data analysis software, to determine whether a CORI check was performed in compliance with the Board's policies and procedures.

We assessed the reliability of the CLARIS and OnBase application systems' data by reviewing existing controls related to the protection of data and the system that produced them and interviewed senior management knowledgeable about the data. Our assessment was based on the recommended security controls identified in the National Institute of Standards and Technology Special Publication 800-53, Revision 3. We determined that the data were sufficiently reliable for the purposes of this report.

Based on our audit, we have concluded that, for the period July 1, 2010 through June 30, 2012, except for the issues addressed in the Detailed Audit Results and Findings section of this report, the Board maintained adequate internal controls and complied with applicable laws, rules, and regulations in the areas tested.

## DETAILED AUDIT RESULTS AND FINDINGS WITH AUDITEE'S RESPONSE

### 1. Collection of information regarding physician criminal activity is ineffective.

During our audit period, the Board of Registration in Medicine (the Board) did not collect from the Executive Office of the Trial Court (EOTC)<sup>6</sup> and report all physician criminal activity in accordance with Chapter 112, Section 5, of the Massachusetts General Laws. As a result, the Board cannot be certain that its online individual physician profiles are complete and accurate, which could affect the public's ability to make informed decisions about physicians they are considering using as healthcare providers. The absence of complete criminal activity information hinders the Board's ability to discern any patterns of improper behavior among physicians and may preclude it from taking disciplinary actions.

The Board is responsible for collecting information reported to it and providing the public with a description of any physician criminal convictions for felonies, serious misdemeanors, and continuations without a finding (CWOs) through its online physician profile database. The Board is dependent on the Commonwealth's trial courts in order to receive criminal activity reports listing this information. Our audit revealed that the Board received only two court reports of criminal activity for physicians with active licenses during the period 2002 through 2012. However, our Criminal Offender Record Information (CORI) check with the Department of Criminal Justice Information Services (DCJIS) for the same period showed that there was a total of 82 physicians with active full licenses with either a conviction for a felony or serious misdemeanor or a CWO that the individual trial courts had not reported to the Board. For example, DCJIS CORI data included one physician who had a CWO in 2004 for assault and battery and another physician who had a CWO in 2006 for illegal possession of a controlled substance. This information should have been reported to and/or collected by the Board so that it could conduct an investigation and, if necessary, take appropriate disciplinary action and update physician profiles accordingly.

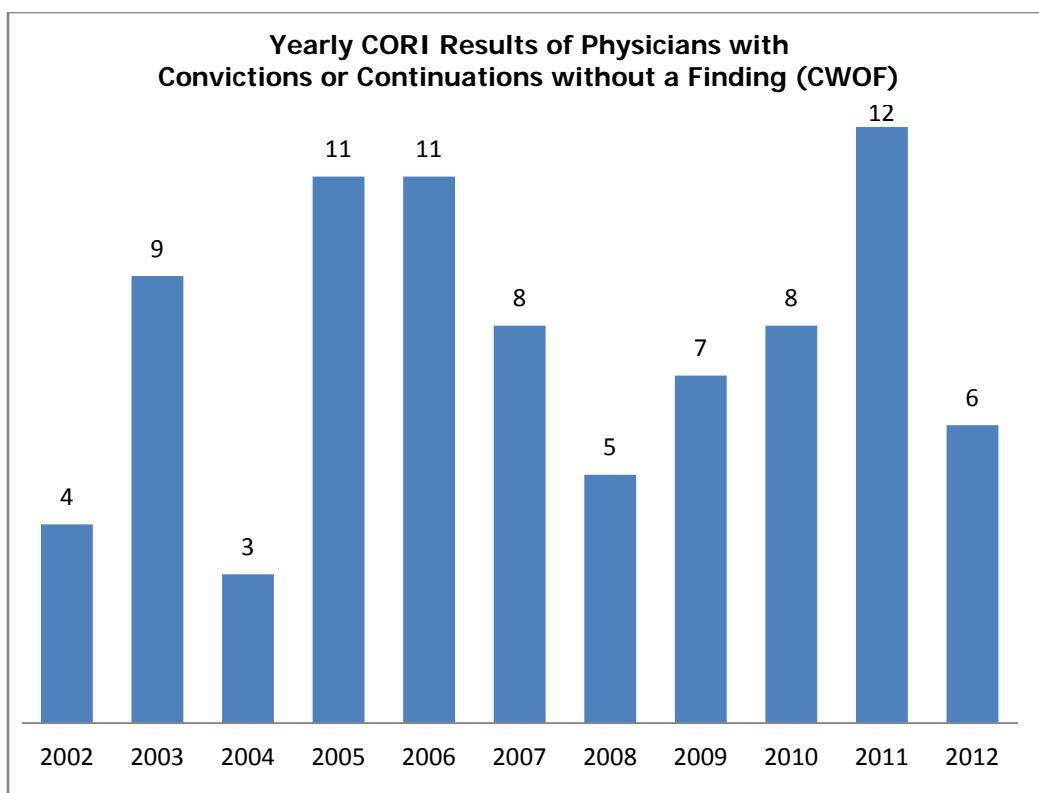
Our review of these 82 physicians identified by DCJIS also noted other offenses that included criminal activity such as conspiracy to file false insurance claims and operating under the influence (OUI). In the Commonwealth, the first and second offenses of OUI are considered misdemeanors and therefore are not reported on a physician's profile unless, as determined by the Board, the

---

<sup>6</sup> The Executive Office of the Trial Court comprises an Office of Court Management and an Office of the Chief Justice of the Trial Court; together, these offices support trial-court operations.

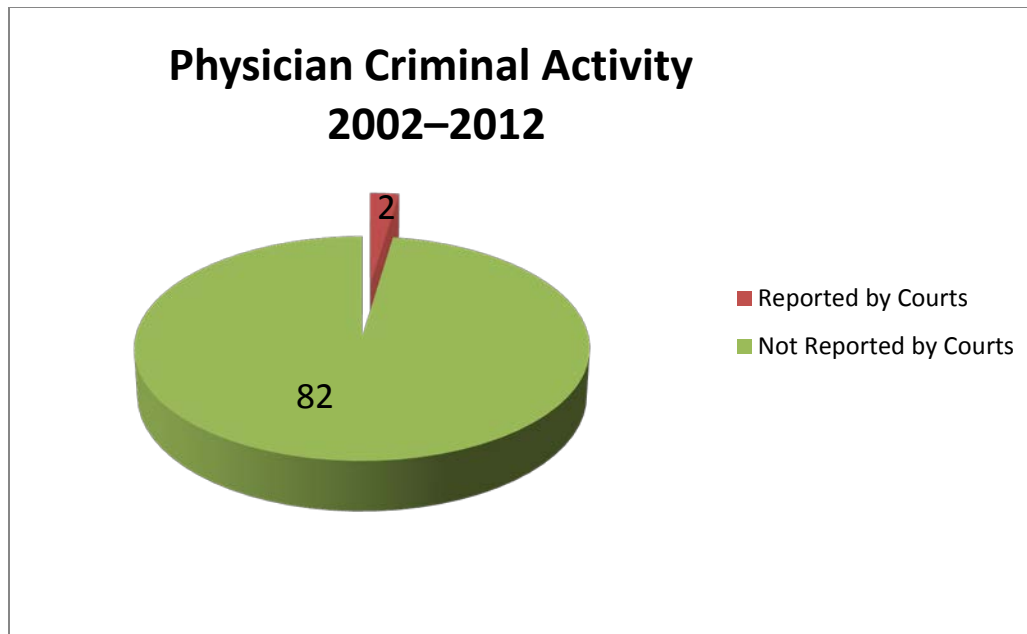
physician's continued practice of medicine would pose a threat to the public. However, if the courts do not provide the Board with reports of OUI offenses, the Board will not be able to establish any patterns of improper behavior that could threaten public safety.

The chart below displays the CORI results from DCJIS for both convictions and CWOFS for Commonwealth physicians with active licenses during calendar years 2002 through 2012.



During our examination, we determined that of the 82 physicians with CORI results showing a conviction or CWO not reported by the courts to the Board, 5 were identified by the Board via public resources (e.g., news media and/or the Internet). In all five instances, the Board took appropriate and timely action and updated each physician profile. Criminal activity in these five cases included such offenses as fraudulently obtaining controlled substances, distribution of drugs, and indecent assault and battery.

The chart below represents the 84 physicians who had either a conviction or a CWO during the calendar years 2002 through 2012. Of these 84, only 2 were reported by the courts to the Board.



With regard to the remaining 77 physicians not reported by the courts (82 less the 5 uncovered by the Board), we determined that 8 had misdemeanor convictions that did not warrant action by the Board, 55 had CWOs that consisted of either OUI or negligent operation of a vehicle, and 14 had CWOs that consisted of charges that were dismissed. The Board only reports misdemeanor convictions and CWOs of a serious nature. Nonetheless, these results show that the Board was not ensuring that it collected the necessary information and investigating it in order to post it on physicians' profiles where necessary.

### ***Authoritative Guidance***

Chapter 112, Section 5, of the General Laws states, in part,

*The board shall collect the following information reported to it to create individual profiles on licensees and former licensees in a format created by the board that shall be available for dissemination to the public: (a) a description of any criminal convictions for felonies and serious misdemeanors as determined by the board; provided, however, that for the purposes of this clause, a person shall be considered to be convicted of a crime if the person pleaded guilty or was found or adjudged guilty by a court of competent jurisdiction; (b) a description of any charges for felonies and serious misdemeanors as determined by the board to which a physician pleads nolo contendere or where sufficient facts of guilt were found and the matter was continued without a finding by a court of competent jurisdiction. . . .*

Chapter 221, Section 26, of the General Laws states, in part,

*The clerk of any court in which a physician registered in the commonwealth is convicted of any crime or in which an unregistered practitioner is convicted of holding himself out as a practitioner*

*of medicine or of practicing medicine shall, within one week thereafter, report the same to the board of registration in medicine together with a copy of the court proceedings in the case. For the purposes of this section, a person shall be deemed to be convicted of a crime if he pleaded guilty or was found or adjudged guilty by a court of competent jurisdiction.*

*In the instance where a physician pleads nolo contendere to charges or where sufficient facts of guilt were found and the matter was continued without a finding by a court of competent jurisdiction, such clerk shall, within one week thereafter, report the same to the board of registration in medicine together with a copy of the court proceedings in the case.*

### ***Reasons for Ineffective Collection and Reporting of Physician Criminal Activity***

The Board and the EOTC had not collaborated to devise and implement a reporting and collection system to ensure that all physician criminal activity was available for dissemination to the public. Board management stated that the Board had mailed letters in March 2012 (no prior mailings had taken place) to all Clerk-Magistrates and Chief Probation Officers throughout the Commonwealth, reinforcing the critical importance and statutory obligations regarding reporting criminal activity of any Commonwealth-licensed physician to the Board. The Board also said that it had periodically conducted informal discussions with various Clerk-Magistrates to communicate their reporting responsibilities. However, the Board was not able to provide any evidence of these occurrences or the frequency of these discussions; we found no evidence of any follow-up meetings or any other correspondence between the Board and the individual trial courts or EOTC regarding developing the necessary reporting mechanisms to ensure that the Board received the required reports.

No formal line of communication has been established between the Board and EOTC. EOTC officials told us that if it had been made aware of the Board's request for this information, it could have issued a directive to the trial courts to support the Board's need for information about physician criminal activity. At present, EOTC has not established formal policies and procedures for the electronic or manual reporting of criminal activity by physicians to the Board.

Lastly, even though the Board recognized that court-mandated reports were not being provided, it did not establish and implement an effective collection system and related policies and procedures, including internal controls that ensured the collection of the information in these reports as required by the General Laws. For instance, it did not use alternative procedures such as obtaining access to CORI data even though access to CORI data is granted to the Board under 243 Code of



Massachusetts Regulations 2.04(8).<sup>7</sup> However, before we finished our fieldwork, Board management advised us that it had obtained approval to create a position that would perform CORI checks on all new physician license applications.

### ***Recommendations***

The Board should collaborate with EOTC in order for EOTC to devise and implement a reporting system and develop related policies, procedures, and internal controls to ensure that court-mandated reports on physician criminal activity are routinely collected and reported to the Board. The Board should use the information it receives from EOTC to make timely updates to individual physician profiles for the public's use in accordance with Chapter 112, Section 5, of the General Laws. The development and implementation of a reporting system that provides for the consistent reporting of physician criminal activity should enable the Board to better ensure the public's safety and welfare by docketing complaints against physicians who have engaged in misconduct and by taking appropriate disciplinary action.

To ensure that the Board has a complete record of physician criminal activity, the Board should conduct a CORI check when a physician submits his or her initial application for a license to practice medicine in the Commonwealth. By conducting this CORI check, the Board could identify any criminal activity before granting an individual a physician's license.

### ***Auditee's Response***

*While the Board accepts the Audit Team recommendations for increased collaboration with the Executive Office of the Trial Court (EOTC), the Board does not have jurisdiction over the EOTC and cannot enforce their compliance with M.G.L. c. 221, § 26. . . .*

*When a physician is convicted of any crime, the statute requires the clerk of the court to report the conviction to the Board within a week of the conviction. . . . The statute further requires the clerk to report to the Board any nolo contendere plea or finding of sufficient facts of guilt when the matter is continued without a finding (CWO). The statutory obligation lies with each clerk of courts and is not, and should not be, dependent on a request from the Board. However, to promote an improved awareness, the Board will enhance ongoing outreach efforts with the courts to facilitate their reporting of physician criminal activity.*

*The Board has discussed this recommendation and the need for a corrective action plan with the Court Administrator of the Massachusetts Trial Court. Initially, he is seeking to determine if there is a more reliable reporting method that the courts would implement, preferably one that is automated. We have offered to participate and assist in any way that would be beneficial.*

---

<sup>7</sup> 243 Code of Massachusetts Regulations 2.04(8): "Each applicant for licensure or renewal shall authorize the Board to access information held by the Massachusetts Criminal History Systems Board [currently the Department of Criminal Justice Information Services] and other law enforcement agencies."

*Further discussions will occur between the Court Administrator and the Board in this regard in mid-June. In the interim, the Board will send letters to the Chief Justices of the Trial, District and Superior Courts and to the Chief Clerk Magistrates in all the courts reminding them of their statutory reporting obligation and offering assistance with any questions.*

*The Board has proactive and collaborative relationships with many law enforcement entities such as the Drug Enforcement Agency, the Attorney General's Office and various police departments. Additionally, physicians and applicants are required to self-report criminal activity on initial and renewal applications. When there is a self-report, the Licensing and Enforcement Divisions of the Board follow up as necessary, including reviewing the relevant court documents and conducting investigations.*

*The draft Audit Report refers to two examples of convictions that the court had not reported to the Board. One physician had a CWOFF in 2004 for assault and battery and another had a CWOFF in 2006 for illegal possession of a controlled substance. Although not reported by the courts, both were reported to the Board by the physicians, as required, on their renewal applications. One of them was also reported by the police department at the time of the initial arrest. Both physicians were investigated by the Enforcement Division.*

*The draft Audit Report references 84 physicians between 2002 and 2012 with either a conviction or a CWOFF and that only 2 were reported by the court. The premise that the failure of the courts to follow the law has resulted in the Board not having necessary information both as a basis for investigating physicians and to post information on Profiles is not supported by an analysis of the CORI information. Of the 84 instances noted in the draft Audit Report, nine were not physicians at the time of their criminal conduct. Furthermore, the Board was aware of the majority of these misdemeanor convictions/CWOFFs from another source, primarily through self-report by the physicians themselves on initial or renewal applications. The overwhelming majority of the 84 convictions/CWOFFs were for one time driving related crimes, which are not posted on Profiles and are investigated depending on the circumstance. Therefore, the assertion that the Trial Courts' failure to report this information has impacted the Board's ability to protect the public or to inform the public on the Profiles site is not accurate.*

*Finally, the Board is developing and implementing a process to CORI all license applicants. Due to the sensitive nature of this information, we continue to seek guidance from legal counsel at the Criminal Justice Information Systems Board to ensure legal compliance. We anticipate being able to CORI initial full applicants in July 2014. The Board then expects to phase in CORI checks for the other categories of licensees, including limited and renewals.*

### **Auditor's Reply**

Our report does not suggest that the Board should have to request information from EOTC on any criminal activity involving licensed physicians. Rather, we point out that both EOTC and the Board have a responsibility to collaborate to devise and implement a reporting system to ensure that all physician criminal activity is available for dissemination to the public as required by Chapter 112, Section 5, of the General Laws. In its response, the Board states that of the 2 out of 82 physicians cited as examples with a conviction for a felony, a serious misdemeanor, or a CWOFF that the individual trial courts had not reported to the Board, both were reported to the Board by the physicians on their initial or license renewal applications; one of them was also reported by the

police department at the time of the initial arrest; and both were investigated by the Board's Enforcement Division.

While we do not doubt the accuracy of the Board's supplemental information, the opinion of the Office of the State Auditor (OSA) is that this represents the breakdown in communication between the Board and EOTC described in our report. Also, waiting for physicians to report criminal activity during the license renewal process that takes place every two years does not ensure the timely reporting of this information to the public. More importantly, even though this information may have been reported to, and investigated by, the Board, it was not made available to the public, where applicable, on individual physician profiles as required by statute.

With respect to the Board's statement that EOTC's not reporting 82 instances of criminal activity to the Board did not affect the latter's ability to protect the public or to inform the public on its Profiles site, we maintain that without such pertinent information, the Board cannot be certain that its online individual physician profiles are complete and accurate and that, when necessary, appropriate disciplinary action is taken and reported on a physician's profile. This could affect the public's ability to make informed decisions. While we agree with the Board that the majority (59) of the unreported instances of criminal activity were for driving-related offenses, including OUI, leaving the scene of an accident, and operating negligently, our CORI analysis also identified 9 instances of assault and battery; 4 instances of fraud; and other offenses such as distributing a class D substance, malicious destruction of property, threatening a person, and larceny. The Board needs this information to determine whether any instances of criminal activity warrant immediate disciplinary action and to inform the public of any such activity that could affect healthcare decisions. Therefore, in OSA's opinion, the absence of that information hampers the Board's ability to properly protect the public or inform the public regarding this kind of criminal activity.

Notwithstanding these facts, based on its response, the Board is taking measures to address our concerns in this area.

## **2. The Board should improve its website to enhance access to physician information.**

Information on the Board's website, which is the Board's primary means of disseminating information on disciplinary and/or criminal actions to the public, needs to be enhanced to ensure that the public will have complete and relevant information on which to base decisions about

physicians. We found that in certain situations, physicians' online profiles were not available to the public; instead, the website gave generic descriptions of physicians' license statuses (Appendix A). In these situations, there may have been information about disciplinary actions taken by the Board that was not available to the public.

During our audit, we identified the following problems with the Board's online physician profiles:

- In some instances, information about disciplinary actions was posted on the Board's webpages for Disciplinary and Other Board Actions and/or News and Updates, but was not shown on the physicians' online profiles, or was listed under generic terms that could be misleading to the public. For instance, disciplinary actions were missing or described generically in the following cases:
  - The Board had taken disciplinary action against one physician who had been charged with OUI, negligent operation of a motor vehicle, and two counts of assault and battery against a police officer and had been placed on probation. However, the physician's online profile only showed the physician's license status as "suspension," with no further explanation other than a link to click to get a definition of the term "suspension" (Appendix B). When questioned, the Board did not see a problem with its use of generic terms.
  - One physician's license status was listed as Active with a comment that the physician's profile was being updated. Our test sample revealed that the physician had been convicted of obtaining a controlled substance by fraud and of filing a false healthcare claim (Appendix C). Since the generic description does not mention the reason for the update, the public may be under the impression that the Active license status indicates that there are no pending issues, when in fact the physician may pose a threat to public safety.
  - The Board had disciplined one physician, whose license was inactive, for sexual misconduct; however, the license status shown on the physician's profile was Revoked, with a link to a generic description that did not refer to the disciplinary action. This information was not easily discernible on the Board's website, though it had been posted on the National Sex Offender Public Website and the Florida Department of Law Enforcement—Sexual Offender website (Appendix D).
- On its website, the Board did not post archived information about disciplinary actions against 780 physicians for the period 2002 through 2009. According to Board management, this information was inadvertently omitted during the website's development. As a result of this unnoticed error, the public was not made aware of any disciplinary action that the Board may have taken against Commonwealth-licensed physicians during this period. As a result of our audit, the Board promptly posted the missing archived information to its website.
- The Board website was inconsistent in reporting the license status of physicians. For example, during an initial search of a physician's profile, we identified the status of a license as Active; however, by double-clicking on the License Status heading, we found that the actual license status in the physician's profile was Active (Subject to Restrictions), with no explanation. If

website visitors only rely on an initial lookup to determine a physician's license status, they may not be aware of restrictions imposed by the Board as a result of disciplinary actions or other actions (Appendix E).

- The Physician Profiles section of the Board's website did not always show disciplinary actions or other actions taken by the Board for physicians with inactive licenses. For example, for one physician who was convicted of sexual misconduct, the misconduct was not reflected on the physician profile. Although the Board reported the sexual misconduct conviction to the Data Bank,<sup>8</sup> the conviction was not reflected on the Board's website (Appendix F).

### ***Authoritative Guidance***

Chapter 112, Section 5, of the General Laws requires the Board to disclose disciplinary actions and/or Massachusetts criminal actions to the public with regard to physician licensure information. Since the Board's website is its primary means of communicating licensure information to the public, the website must be clear, accurate, and consistent in its reporting of that information.

### ***Reasons for Inadequate Public Access to Information on the Board's Website***

We found that the issues with the Board's website resulted from a lack of integration between the online physician profiles and the Disciplinary and Other Board Actions section of the site. Since the inception of its website, the Board has not conducted periodic reviews of the information on various pages to ensure consistency in the reporting of license status and disciplinary actions to the public.

### ***Recommendations***

We recommend that the Board take the following actions:

- Update and periodically review its website to ensure consistency in the reporting of license status and disciplinary actions.
- Ensure the consistent reporting of information between the Disciplinary and Other Board Actions sections of its website and related comments within the online physician profile. The physician profile should include an appropriate description of any disciplinary action or other action taken by the Board.
- Correct the initial lookup section of its website to ensure that physicians with a license status of Active (Subject to Restrictions) appear correctly in the initial lookup screen rather than displaying the misleading status of Active.

---

<sup>8</sup> A national repository for information regarding physicians who have had disciplinary action taken by a state board of medicine.

- When reviewing allegations against a physician, modify its generic description of Profile Is in the Process of Being Updated to include language that better informs the public that there could be an issue with the status of the physician's license.

***Auditee's Response***

*The Board appreciates the Audit Team's recommendations regarding enhancements to the Board's Profiles site. The draft Audit Report correctly points out that if a physician's license has restrictions that information is not apparent from the list of names that appears when a search is done on the Profiles site. It does appear when an individual physician's full Profile is accessed. We are making a change to our Profiles search function to make this information readily available on the initial lookup page and expect this to be in operation by the end of June 2014.*

*Additionally, the Audit Team informed us during their site work that the 2002–2009 disciplinary action list was missing from our website. We appreciate this inadvertent omission being brought to our attention. It occurred during the migration of our website to Mass.gov and was immediately reposted. However, this website omission only affected the chronological listing of disciplinary actions that is maintained on the Board's website. It did not affect the inclusion of the disciplinary action on each individual physician's Profile when appropriate, making it readily available to the public.*

*The Profiles site maintained by the Board on its website is mandated by M.G.L. c. 112 §5, which enumerates exactly what information is included on a physician's Profile. The purpose of the Profile is to inform the public about physicians from whom they may seek treatment. The statute is quite precise about exactly what details shall appear on a Profile. For instance, pursuant to statute, open complaints and investigations are confidential and never available on a Profile. Legislative changes have resulted in corresponding changes to the Profiles site, including the posting of full Profiles for inactive licensees.*

*Because it is crucial that adverse information on a Profile be accurate, the Board affords a physician the opportunity to review his Profile before it is posted. During the review period only certain information is available on the Profile site. More comprehensive information is always readily available by contacting the Board.*

***Auditor's Reply***

We agree that the Board should not disclose information that it is required to keep confidential, such as information on open complaints and investigations. However, when disciplinary actions or convictions have taken place, the Board should add that information to a physician's profile as soon as the physician has had a chance to review it.

**3. The Board has no record of an information security program, electronic security plan, or Self-Assessment Questionnaire.**

During our audit period, the Board had not completed the 2011 and 2012 annual Self-Assessment Questionnaires (SAQs) to report the results of the self-audit required by the Commonwealth's Executive Office for Administration and Finance (EOAF). Further, the Board had not submitted an information security program (ISP) or an electronic security plan (ESP) as required in Sections 3

and 4 of Commonwealth Executive Order 504 (EO504). These documents help agencies identify all personal information residing on each of their application systems and the security controls in effect to protect this information from unauthorized access and use. Without completing them, the Board cannot be certain that it has taken the measures necessary to reasonably ensure the security, confidentiality, and integrity of personal information collected.

### ***Authoritative Guidance***

Sections 3 and 4 of EO504 include the following:

*Section 3. All state agencies shall develop, implement and maintain written information security programs governing their collection, use, dissemination, storage, retention and destruction of personal information. . . .*

*Section 4. Each agency's written information security program shall include provisions that relate to the protection of information stored or maintained in electronic form (hereafter, "electronic security plans").*

In addition, on April 1, 2009, EOAF issued the Enterprise Information Security Policy, Issue #2, which implemented the provisions of EO504. This policy requires agencies to implement requirements that include "results of self-audits required by [the Commonwealth's Information Technology Division, or ITD] upon request and at a minimum annually." ITD developed the SAQ for agencies to use for submitting self-audit results.

### ***Reasons for Noncompliance with Security-Plan Requirements***

Because of reorganizations of information technology (IT) departments in executive agencies required by Executive Order 510<sup>9</sup> (EO510), the Board, as part of the Department of Public Health (DPH), did not work with DPH to ensure that the ISP, ESP, and SAQ were completed, reviewed, and submitted to ITD. Board senior management told us that IT consolidation at the Secretariat level changed the lines of reporting for Board IT personnel. Specifically, EO510 required that IT personnel be transferred from the Board and consolidated with the Executive Office of Health and Human Services (EOHHS). This transfer affected the ability of the Board, in conjunction with DPH, to direct the actions of its staff members to prepare and submit the ISP, ESP, and SAQ. In

---

<sup>9</sup> On February 19, 2009, the Governor issued EO510, Enhancing the Efficiency and Effectiveness of the Executive Department's Information Technology Systems, for the purpose of achieving greater efficiency and cost-effectiveness by centralizing the management and operation of IT systems across the state's Executive Department agencies (Secretariats).

addition, we found no documentation to indicate that the Board sought assistance from ITD to help in the preparation of the EO504 filings.

### ***Recommendations***

The Board's information security officer (ISO), in conjunction with DPH, should immediately begin an annual review of all IT-related security controls in place and file all required reports with ITD. If the Board needs guidance in this area, the ISO should consider reviewing EOAF's "Instructions for Completing and Submitting Agency Executive Order 504 Information Security Program (ISP) and Electronic Security Plan (ESP)." If necessary, the Board and ISO should seek assistance from ITD to assist in the completion of the required reports.

### ***Auditee's Response***

*The Board accepts the Audit Team's recommendation regarding the lack of an information security program (ISP), electronic security plan (ESP), or self-assessment questionnaire for 2011 and 2012. The Board is now in full compliance. The Acting Executive Director and the Director of Operations attended training at [EOHHS] / Information Technology Division in June 2013 and successfully submitted the 2013 SAQ and ISP/ESP on November 27, 2013. The Board will continue to submit the SAQ and ISP/ESP as required. The Board is committed to protecting the security, confidentiality, and integrity of personal information collected.*

### ***Auditor's Reply***

Based on its response, the Board is taking measures to address our concerns in this area.

## **4. The Board did not comply with the Payment Card Industry Data Security Standard.**

The Board did not meet certain requirements<sup>10</sup> for compliance with the Payment Card Industry Data Security Standard (PCI DSS), according to a November 2011 report prepared by Compass IT Compliance, LLC, a certified Qualified Security Assessor (QSA). Although the Board does not store cardholder data once transactions are completed, not meeting the PCI DSS requirements risks a security breach during the processing of transactions, including the fraudulent use of cardholder data. Further, a security breach of cardholder data under federal law could expose the Board to potential fines and penalties as well as adverse publicity.

We determined that the Board processed 39,855 credit-card transactions associated with online physician license renewals, totaling \$20.1 million dollars, for the period July 1, 2010 through June 30, 2012.

---

<sup>10</sup> We have omitted specific PCI DSS deficiency information from this report because of security concerns.



***Authoritative Guidance***

PCI DSS was initiated by the major credit-card brands, including American Express, MasterCard, Visa, and Discover, in order to secure credit-card data in a globally consistent manner (Appendix G). In addition to PCI DSS, the Office of the State Comptroller (OSC) and ITD require all departments (in any branch of state government) that currently accept credit- or debit-card payments, or payments through other collection options, to validate data security compliance with standards set by the Payment Card Industry Council. OSC procedure "FY 2010-26: Payment Card Industry (PCI) Data Security Standard Compliance," issued May 13, 2010, states, in part,

*PCI compliance must be validated by a Qualified Security Assessor (QSA) prior to implementing any new application or program that will accept credit card payments or that processes, stores or transfers credit cardholder data, and any applications connected to networks that process or transmit credit cardholder data.*

The Board has complied with OSC's requirement to obtain the services of a QSA to perform a detailed risk assessment associated with the 12 PCI DSS requirements. It also has controls in place to give only authorized users access to credit-card data and does not store any credit-card data after completion of a transaction. However, the Board has not fully met all PCI DSS requirements.

***Reasons for Noncompliance with PCI DSS***

The Board's noncompliance with PCI DSS was due primarily to a lack of documented policies and procedures for industry requirements and related internal controls. Since ITD has overall responsibility for the processing of all its credit-card transactions conducted over the Internet and had not implemented PCI-compliant controls at the time of our audit, the Board was unable to comply with this requirement.

***Recommendations***

We recommend that the Board take the following actions:

- Develop policies and procedures and related internal controls to ensure compliance with PCI DSS. Completion of the EO504 ISP should help with this compliance.
- Work with ITD to ensure that all requirements and protections identified in the risk assessment are addressed and tested by the QSA.

- Annually test the controls it has established to track and monitor all access to network resources and cardholder data, regularly test security systems and processes, and regularly review and update its policies and procedures in this area as necessary.

***Auditee's Response***

*The Board is committed to protecting the personal information of all individuals and will take appropriate steps in remediating findings. The Board is implementing a new credit card processing solution that will be in place by the end of June 2014 that will allow us to meet and maintain our compliance requirements. The Board is working with [EOHHS] and ITD to update PCI related documentation as required.*

***Auditor's Reply***

Based on its response, the Board is taking measures to address our concerns in this area.

**5. Prior audit result partially resolved—The Board has developed a business continuity plan but has not updated it.**

Our prior audit report (No. 2008-0117-4T) revealed that the Board did not have a formal business continuity plan (BCP) as required by Executive Order 490.<sup>11</sup> Accordingly, we recommended that the Board work with ITD to develop formal approved business continuity and disaster recovery plans that are tested at least annually.

Our current audit indicated that the Board implemented our prior audit recommendation to develop a BCP; however, the Board has not updated its BCP since 2009. The absence of an updated BCP could hinder or prevent the Board from restoring computer operations in the event of unforeseen interruptions in business operations. Specifically, the lack of a BCP may cause delays in processing physician licenses and in updating physician profiles with disciplinary actions taken by the Board. Further, the Board may not be able to ensure continuity and sustainability of its operations without an up-to-date BCP.

The Board has controls in place for daily and weekly incremental backup of data that are maintained in both on- and off-site secured locations. In addition, the Board has plans in place for system restoration at its on-site IT server room. However, we found that the plans did not include an emergency relocation site to be used if the Board cannot continue operations at its headquarters. In

---

<sup>11</sup> Executive Order 490 requires agencies to develop continuity plans “establishing emergency operating procedures, delegating specific emergency authority to key personnel, establishing reliable, interoperable communications, and providing for the safekeeping of critical systems, records, and databases.”

addition, the Board's Memorandum of Agreement with Middlesex Community College expired November 14, 2011, leaving the Board without an emergency relocation site.

Executive Order 490 requires the Board to have a continuity-of-operations plan including an ongoing business continuity planning process that assesses the relative criticality of information systems as well as maintaining appropriate contingency and recovery plans.

### ***Recommendations***

In collaboration with DPH, the Board should update its BCP to include all changes to its technology environment as well as changes to the emergency contact list since its prior plan. To that end, the Board should assess the extent to which it is dependent upon the continued availability of information systems for all required computer processing and operational needs and should develop its recovery plans based on the critical aspects of its information systems. The plan should be tested and the results incorporated into the current plan. The Board should also identify an emergency relocation site to use should the Board's offices be rendered inaccessible by an unforeseen event.

### ***Auditee's Response***

*The Board accepts the Audit Team's finding regarding updating its business continuity plan (BCP). As of March 2014, the Board updated its BCP with all changes to its technology environment as well as [its] emergency contact list. The BCP lists temporary accommodations in the event that the Board's building becomes hazardous or unusable. The Board recognizes that it needs to identify a new relocation site and has reached out to discuss options with the [EOHHS] Regional Manager.*

### ***Auditor's Reply***

Based on its response, the Board is taking measures to address our concerns in this area.

## APPENDIX A

### Generic Terms for License Status Actions Taken by the Board of Registration in Medicine<sup>12</sup>

*License statuses include the following:*

**Profile is Being Updated**—The Board may place an administrative hold on a physician's profile prior to release to the public to ensure that the profile is factually accurate.

**Profile is Being Updated and Will be Available at a Later Date**—The Board is required to provide physicians with copies of their profiles prior to release to the public. The physician is given 30 days to review the profile and correct factual inaccuracies that appear in the profile.

**Active License Status**—A physician with an active status may prescribe medications and must complete the Board's continuing medical education requirements. In addition, physicians with an active status must have malpractice liability insurance coverage, unless they are not providing direct or indirect patient care.

**Active License Status (Subject to Restrictions)**—The Board may place restrictions on the license of a physician with an active status. A physician with an active status (subject to restrictions) must complete the Board's continuing medical education requirements. In addition, physicians with an active status (subject to restrictions) must have malpractice liability insurance coverage, unless they are not providing direct or indirect patient care.

**Voluntary Agreement Not to Practice License Status**—An agreement between the physician and the Board, or the Complaint Committee, that the physician will not practice medicine during the Board's investigation of allegations against the physician.

**Resigned License Status**—Under the Board's regulations, a physician who is under investigation or named in a complaint by the Board may choose to submit a resignation and terminate the investigation.

**Suspension License Status**—As the result of a disciplinary action, the Board may suspend a physician for an indefinite or limited term. This suspension may be stayed upon compliance with specific conditions imposed by the Board.

**Summary Suspension License Status**—The Board may summarily suspend a physician's license. If the Board determines, based on affidavits and other documentary evidence, that a physician represents a serious threat to the public health, safety or welfare, the Board may suspend the license pending a hearing on the merits.

**Revoked License Status**—A revocation is permanent and removes all privileges of practice. The physician may not apply for reinstatement of licensure for at least five years from the date of imposition of the action, unless the Board permits a shorter period in its final decision.

**Inactive License Status**—A physician who is inactive is exempt from the Board's requirements regarding continuing medical education credits and malpractice liability insurance coverage. In addition, a physician on inactive status may not provide patient care or prescribe medications.

---

<sup>12</sup> Source: Board of Registration in Medicine website.


***Lapsed License Status***—*The physician has not renewed his or her license prior to the license expiration date and therefore does not currently have a valid license to practice medicine in Massachusetts.*

***Deceased Status***—*The physician is deceased.*

## APPENDIX B

### Notice of Disciplinary Action Posted on the Board of Registration in Medicine's Website but Not Posted on Physician Profile

The link to Complaints and Disciplinary Actions on the Board of Registration in Medicine (Board) website leads to this document:



**DEVAL L. PATRICK**  
Governor

**TIMOTHY P. MURRAY**  
Lieutenant Governor

*The Commonwealth of Massachusetts*  
Board of Registration in Medicine  
200 Harvard Mill Square, Suite 330  
Wakefield, MA 01880  
(781) 876-8200  
[www.mass.gov/massmedboard](http://www.mass.gov/massmedboard)

**STANCEL M. RILEY, Jr., M.D.**  
Executive Director

**FOR IMMEDIATE RELEASE:**  
Wednesday, [REDACTED]


**CONTACT:**  
Russell Aims  
(781) 876-8267

**STATE BOARD OF MEDICINE TAKES DISCIPLINARY ACTION**

**WAKEFIELD:** At its meeting today the state Board of Registration in Medicine took disciplinary action against the medical licenses of [REDACTED] M.D.

The Board found that Dr. [REDACTED] was charged with Operating Under the Influence of Liquor, Negligent Operation of a Motor Vehicle and two counts of Assault & Battery on a police officer, and subsequently admitted to sufficient facts, and was placed on probation. Dr. [REDACTED] was also found to have failed to respond to the Board. Today the Board indefinitely suspended her right to renew her license. She may petition for a stay of suspension upon demonstration of her fitness to practice medicine. Dr. [REDACTED] is a 1986 graduate of the University of Medicine and Dentistry in New Jersey. She is board certified in Internal Medicine and was first licensed in Massachusetts in 1989.

This physician's profile on the Board website has no reference to the specific disciplinary action:



Commonwealth of Massachusetts

**BOARD OF REGISTRATION IN MEDICINE**



Accessibility

[Home](#)
[Help](#)

[Back to Search Results](#)

### Physician Profile

[Disclaimer](#)

[Printer Friendly](#)

**Physician Information**

License Number	[REDACTED]
License Status	Suspension (What does this mean?)
License Issue Date	[REDACTED]
License Expiration Date	3/8/2012
License Suspension Date	9/19/2012

Both The Joint Commission and the National Committee on Quality Assurance consider the Massachusetts Board of Registration to be a primary source provider for license status information.

---

Instructions for obtaining public information about a physician are available at [our public information page](#). Questions about a physician's Profile may be submitted to [ma\\_profiles@state.ma.us](mailto:ma_profiles@state.ma.us). You may also contact the Massachusetts Board of Registration in Medicine, 200 Harvard Mill Square, Suite 330, Wakefield, MA 01880. Phone 781-876-8200 or public information about a physician or questions about a physician's Profile.

**Suspension License Status** – As the result of a disciplinary action, the Board may suspend a physician for an indefinite or limited term. This suspension may be stayed upon compliance with specific conditions imposed by the Board.

## APPENDIX C

### Physician Profile with Generic Terms Rather Than Information on Specific Convictions

Below is an example of physician profile maintained by the Board of Registration in Medicine indicating that a physician's profile "is being updated" even though the physician, based on our Criminal Offender Record Information analysis, had been convicted of obtaining a controlled substance by fraud and of filing a false healthcare claim. The listing of generic terms like the one used below could be misleading to the public.

Commonwealth of Massachusetts  
BOARD OF REGISTRATION IN MEDICINE

Home Help Mass.gov Accessibility

Back to Search Results Printer Friendly

### Physician Profile

[Redacted], M.D.

**This profile is being updated.**

[What does this mean?](#) ← Click for generic definition.


License Number [Redacted]  
License Status **Active** ← License shows as active  
License Renewal Date 2/5/2015  
NPI Number [Redacted]

Instructions for obtaining public information about a physician are available at [our public information page](#). Questions about a physician's Profile may be submitted to [ma\\_profiles@state.ma.us](mailto:ma_profiles@state.ma.us). You may also contact the Massachusetts Board of Registration in Medicine, 200 Harvard Mill Square, Suite 330, Wakefield, MA 01880. Phone 781-876-8200 for public information about a physician or questions about a physician's Profile.


**Profile is Being Updated** – The Board may place an administrative hold on a physician's profile prior to release to the public to ensure that the profile is factually accurate.

## APPENDIX D

### Example of Physician's Conviction of Sexual Misconduct Not Posted on Physician Profile



Commonwealth of Massachusetts  
**BOARD OF REGISTRATION IN MEDICINE**

  
Accessibility

[Home](#)
[Help](#)

[Back to Search Results](#)

**Physician Profile**  

M.D.

[Disclaimer](#)

**Physician Information**  
Except for the License information, this information has been reported by Dr.

License Number
License Status
License Issue Date

Revoked (What does this mean?)

Both The Joint Commission and the National Committee on Quality Assurance consider the Massachusetts Board of Registration to be a primary source provider for license status information.

Instructions for obtaining public information about a physician are available at [our public information page](#). Questions about a physician's Profile may be submitted to [ma\\_profiles@state.ma.us](mailto:ma_profiles@state.ma.us). You may also contact the Massachusetts Board of Registration in Medicine, 200 Harvard Mill Square, Suite 330, Wakefield, MA 01880. Phone 781-876-8200 for public information about a physician or questions about a physician's Profile.

“Revoked License Status—A revocation is permanent and removes all privileges of practice. The physician may not apply for reinstatement of licensure for at least five years from the date of imposition of the action, unless the Board permits a shorter period in its final decision.”

Disciplinary Action Notice on Board of Registration in Medicine website:

**September 19, 2007**

Name and Address	Date of Action(s)	Type of Action(s) Click link to view Board Order
<div></div>	09/19/2007	1. Revocation



Florida Department of Law Enforcement Sexual Offender / Predator Flyer reference to actual complaint:

Florida Department of Law Enforcement - Sexual Offender / Predator Flyer

[Click Here to Track this Offender](#)

Designation: Sexual Offender

Name: [REDACTED]

Status: Released - Required to Register

Department of Corrections #: Not Available  
[Search the Dept of Corrections Website](#)

Date of Birth: [REDACTED]

Race : White

Sex: Male

Hair: Grey

Eyes: Hazel

Height: 5'10"

Weight: 160 lbs

(Picture Removed)

[REDACTED] is registered as a Sexual Offender.  
Positive identification cannot be established unless a fingerprint comparison is made.

**Aliases**

[REDACTED]

**Scars, Marks & Tattoos**

Information temporarily unavailable

**Address Information**

Address	Address Source Information	Map Link
[REDACTED]	Source: Dept. of Highway Safety and Motor Vehicle Received: 06/19/2013 Type of Address: Permanent	<a href="#">Show Map</a>

**Crime Information - Qualifying Offenses**

Adjudication Date	Crime Description	Court Case Number	Jurisdiction & State	Adjudication
03/19/2007	SEX OFFENSE, OTHER STATE (9 COUNTS: INDECENT ASSAULT AND BATTERY ON PERSON 14 OR OLDER)	Not Available	PLYMOUTH, MA	Guilty/convict

**Victim Information**

Gender:Unknown Minor:No

THE U.S. DEPARTMENT OF JUSTICE

NSOPW

SMART Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking

HOMEABOUTSEARCHEDUCATION & PREVENTIONREGISTRY SITESFAQ

## National Sex Offender Search

### Results

[print view](#) [create new search](#)

1 record from a national search including all states, territories and Indian Country for First Name like [REDACTED] Last Name like [REDACTED]. To view a list of the jurisdictions included in this search, [click here](#).

Search performed 9/20/2013 3:22 PM EDT

OFFENDER	AGE	ADDRESS
[REDACTED]	[REDACTED]	[REDACTED] Residential

## APPENDIX E

### Example of License Status of Active Though the Physician Profile Displays the License Status as Active (Subject to Restrictions)

**Click 1**—Shows the license status as Active



Commonwealth of Massachusetts  
BOARD OF REGISTRATION IN MEDICINE

Home Help Mass.gov Accessibility

### List of Physicians that Match Your Search

**Search Criteria**  
License Number: [REDACTED]

**1 Physician Found**

Select a physician's profile by clicking on the last name. The list may be sorted by clicking on any column header.

[Back to Search](#) show 10 20 50 rows per page page 1

Last Name	First Name	Initial	Practice Specialties	License Status	Town / City	State
[REDACTED]	[REDACTED]	[REDACTED]	Addiction Medicine, Internal Medicine, Rheumatology	Active		

[Back to Search](#) show 10 20 50 rows per page page 1

**Click 2**—Shows the correct license status, Active (Subject to Restrictions)



Commonwealth of Massachusetts  
BOARD OF REGISTRATION IN MEDICINE

Home Help Mass.gov Accessibility

[Back to Search Results](#) **Physician Profile** [Printer Friendly](#)

[REDACTED]

[Disclaimer](#)

**Physician Information**  
Except for the License information, this information has been reported by Dr. [REDACTED]

License Number	[REDACTED]	Accepting New Patients	Yes
License Status	Active (Subject to Restrictions) *	Accepts Medicaid	Yes
License Issue Date	[REDACTED]	Translation Services Available	None Reported
License Renewal Date	8/24/2014	Insurance Plans Accepted	None Reported
Primary Work Setting	Private Office	Hospital Affiliations	None Reported
Business Address	None Reported	NPI Number	[REDACTED]
Business Telephone	None Reported		

\* Instructions for obtaining public information about this restriction are available at [our public information page](#).

Both The Joint Commission and the National Committee on Quality Assurance consider the Massachusetts Board of Registration to be a primary source provider for license status information.

## APPENDIX F

### Example of Physician Profile with a License Status of Suspension Compared to the Board of Registration in Medicine's Report to the National Data Bank of Sexual Misconduct

Physician profile on Board of Registration in Medicine website:

Commonwealth of Massachusetts  
BOARD OF REGISTRATION IN MEDICINE

Home Help

Mass.gov  
Accessibility

[Back to Search Results](#) **Physician Profile** [Printer Friendly](#)

██████████ M.D.

[Disclaimer](#)

**Physician Information**  
Except for the License information, this information has been reported by ██████████

License Number ██████████  
License Status **Suspension** (What does this mean?)  
License Issue Date ██████████  
License Suspension Date 10/1/2010

Both The Joint Commission and the National Committee on Quality Assurance consider the Massachusetts Board of Registration to be a primary source provider for license status information.

Screen shows Suspension and no reference to sexual misconduct.

National Database Report (OnBase Application):

the DataBank  
P.O. Box 10832  
Chantilly, VA 20153-0832  
http://www.npdb-hipdb.hrsa.gov

DCN 5500000080550925  
Process Date 03/04/2013  
Page 1 of 3  
For authorized use by  
MA BOARD OF REGISTRATION IN MEDICINE

██████████

MA BOARD OF REGISTRATION IN MEDICINE	
<b>CORRECTION TO STATE LICENSURE ACTION</b>	Date of Action 10/06/2010
<b>Initial Action</b>	<b>Basis for Initial Action</b>
- SUSPENSION OF LICENSE	- SEXUAL MISCONDUCT

**A REPORTING ENTITY**

Entity Name	MA BOARD OF REGISTRATION IN MEDICINE
Address	200 HARVARD HILL SQUARE SUITE 330
City State, Zip	WAKEFIELD, MA 01880
Country	
Name of Office	██████████ ESQ
Title or Department	ASSISTANT GENERAL COUNSEL
Telephone	██████████
Entity Internal Report Reference	
Type of Report	CORRECTION
Previous Report Number	5500000065309121 (Please destroy all copies of the previous report!)

Complaint of sexual misconduct reported to the national database.

## APPENDIX G

### Payment Card Industry Data Security Standard<sup>13</sup>

*The Payment Card Industry (PCI) Data Security Standard (DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data. PCI DSS applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data. PCI DSS comprises a minimum set of requirements for protecting cardholder data, and may be enhanced by additional controls and practices to further mitigate risks. Below is a high-level overview of the 12 PCI DSS requirements.*

#### PCI Data Security Standard – High Level Overview

<b>Build and Maintain a Secure Network</b>	<ol style="list-style-type: none"> <li>1. Install and maintain a firewall configuration to protect cardholder data</li> <li>2. Do not use vendor-supplied defaults for system passwords and other security parameters</li> </ol>
<b>Protect Cardholder Data</b>	<ol style="list-style-type: none"> <li>3. Protect stored cardholder data</li> <li>4. Encrypt transmission of cardholder data across open, public networks</li> </ol>
<b>Maintain a Vulnerability Management Program</b>	<ol style="list-style-type: none"> <li>5. Use and regularly update anti-virus software or programs</li> <li>6. Develop and maintain secure systems and applications</li> </ol>
<b>Implement Strong Access Control Measures</b>	<ol style="list-style-type: none"> <li>7. Restrict access to cardholder data by business need to know</li> <li>8. Assign a unique ID to each person with computer access</li> <li>9. Restrict physical access to cardholder data</li> </ol>
<b>Regularly Monitor and Test Networks</b>	<ol style="list-style-type: none"> <li>10. Track and monitor all access to network resources and cardholder data</li> <li>11. Regularly test security systems and processes.</li> </ol>
<b>Maintain an Information Security Policy</b>	<ol style="list-style-type: none"> <li>12. Maintain a policy that addresses information security for all personnel.</li> </ol>

<sup>13</sup> Source: PCI Security Standards Council LLC, *PCI DSS Requirements and Security Assessment Procedures, Version 2.0*, October 2010.

## APPENDIX H

### **Executive Order 504: Order Regarding the Security and Confidentiality of Personal Information (Revoking and Superseding Executive Order 412)**

*WHEREAS, identity theft is a serious crime that, according to current Federal Trade Commission statistics, affects as many as 9 million Americans each year and costs consumers and businesses approximately \$52 billion annually;*

*WHEREAS, the Commonwealth of Massachusetts has recognized the growing threat of identity theft and taken steps to safeguard the personal information of its residents by, among other things, enacting Massachusetts General Laws Chapter 93H ("Chapter 93H");*

*WHEREAS, pursuant to Chapter 93H, the Massachusetts Office of Consumer Affairs and Business Regulation has promulgated regulations, effective January 1, 2009, defining security standards that must be met by persons, other than state entities, who own, license, store or maintain personal information about residents of the Commonwealth;*

*WHEREAS, also pursuant to Chapter 93H, the Secretary of the Commonwealth, through his Supervisor of Public Records, is charged with establishing rules or regulations designed to safeguard personal information that is owned or licensed by state executive offices and authorities;*

*WHEREAS, the Executive Department recognizes the importance of developing and implementing uniform policies and standards across state government to safeguard the security, confidentiality and integrity of personal information maintained by state agencies; and*

*WHEREAS, the implementation of such policies and standards will further the objectives of Chapter 93H and will demonstrate the Commonwealth's commitment to adhere to standards equal to or higher than those that govern the private sector.*

*NOW, THEREFORE, I, Deval L. Patrick, Governor of the Commonwealth of Massachusetts, by virtue of the authority vested in me by the Constitution, Part 2, c. 2, § 1, Art. 1, do hereby revoke Executive Order 412 and order as follows:*

*Section 1. This Executive Order shall apply to all state agencies in the Executive Department. As used in this Order, "state agencies" (or "agencies") shall include all executive offices, boards, commissions, agencies, departments, divisions, councils, bureaus, and offices, now existing and hereafter established.*

*Section 2. It shall be the policy of the Executive Department of the Commonwealth of Massachusetts to adopt and implement the maximum feasible measures reasonably needed to ensure the security, confidentiality and integrity of personal information, as defined in Chapter 93H, and personal data, as defined in Massachusetts General Laws Chapter 66A, maintained by state agencies (hereafter, collectively, "personal information"). Each executive officer and agency head serving under the Governor, and all state employees, shall take immediate, affirmative steps to ensure compliance with this policy and with applicable federal and state privacy and information security laws and regulations.*

*Section 3. All state agencies shall develop, implement and maintain written information security programs governing their collection, use, dissemination, storage, retention and destruction of*

*personal information. The programs shall ensure that agencies collect the minimum quantity of personal information reasonably needed to accomplish the legitimate purpose for which the information is collected; securely store and protect the information against unauthorized access, destruction, use, modification, disclosure or loss; provide access to and disseminate the information only to those persons and entities who reasonably require the information to perform their duties; and destroy the information as soon as it is no longer needed or required to be maintained by state or federal record retention requirements. The security programs shall address, without limitation, administrative, technical and physical safeguards, and shall comply with all federal and state privacy and information security laws and regulations, including but not limited to all applicable rules and regulations issued by the Secretary of State's Supervisor of Public Records under Chapter 93H.*

*Section 4. Each agency's written information security program shall include provisions that relate to the protection of information stored or maintained in electronic form (hereafter, "electronic security plans"). The Commonwealth's Chief Information Officer ("CIO") shall have the authority to:*

- Issue detailed guidelines, standards, and policies governing agencies' development, implementation and maintenance of electronic security plans;*
- Require that agencies submit their electronic security plans to ITD for review, following which ITD shall either approve the plans, return them for amendment, or reject them and mandate the preparation of a new plan;*
- Issue guidelines specifying when agencies will be required to prepare and submit supplemental or updated electronic security plans to ITD for approval;*
- Establish periodic reporting requirements pursuant to which all agencies shall conduct and submit self-audits to ITD no less than annually, assessing the state of their implementation and compliance with their electronic security plans, with all guidelines, standards, and policies issued by ITD, and with all applicable federal and state privacy and information security laws and regulations;*
- Conduct reviews to assess agency compliance with the governing plans, guidelines, standards, policies, laws and regulations. At the discretion of ITD, reviews may be conducted on site or electronically, and may be announced or unannounced;*
- Issue policies requiring that incidents involving a breach of security or unauthorized acquisition or use of personal information be immediately reported to ITD and to such other entities as required by the notice provisions of Chapter 93H; and*
- Where necessary and appropriate, and with the approval of the Secretary for Administration and Finance, determine and implement remedial courses of action to assist non-compliant agencies in achieving compliance with the governing plans, guidelines, standards, policies, laws and regulations. Such actions may include, without limitation, the imposition of terms and conditions relating to an agency's information technology ("IT")-related expenditures and use of IT capital funding.*

*Section 5. Each agency shall appoint an Information Security Officer ("ISO"), who may also hold another position within the agency. ISOs shall report directly to their respective Agency heads and shall coordinate their agency's compliance with the requirements of this Order, applicable federal and state laws and regulations, and ITD security standards and policies. All agency security programs, plans, self-audits, and reports required by this Order shall contain*



*certifications signed by the responsible ISO and the responsible agency head attesting to the accuracy and completeness of the submissions.*

*Section 6. All agency heads, managers, supervisors, and employees (including contract employees) shall attend mandatory information security training within one year of the effective date of this Order. For future employees, such training shall be part of the standardized orientation provided at the time they commence work. Such training shall include, without limitation, guidance to employees regarding how to identify, maintain and safeguard records and data that contain personal information.*

*Section 7. The Enterprise Security Board ("ESB"), as presently established, shall advise the CIO in developing the guidelines, standards, and policies required by Section 4 of this Order. Consistent with the ESB's current framework, the precise members and make-up of the ESB shall be determined by the CIO, but its membership shall be drawn from state employees across the Executive Department with knowledge and experience in the fields of information technology, privacy and security, together with such additional representatives from the Judicial and Legislative Branches, other constitutional offices, and quasi-public authorities who accept an invitation from the CIO to participate. The ESB shall function as a consultative body to advise the CIO in developing and promulgating guidelines, standards, and policies that reflect best practices to ensure the security, confidentiality and integrity of the electronic personal information collected, stored, used, and disseminated by the Commonwealth's IT resources.*

*Section 8. The CIO shall develop mandatory standards and procedures for agencies to follow before entering into contracts that will provide third parties with access to electronic personal information or information technology systems containing such information. Such standards must require that appropriate measures be taken to verify the competency and integrity of contractors and subcontractors, minimize the data and systems to which they will be given access, and ensure the security, confidentiality and integrity of such data and systems.*

*Section 9. All contracts entered into by state agencies after January 1, 2009 shall contain provisions requiring contractors to certify that they have read this Executive Order, that they have reviewed and will comply with all information security programs, plans, guidelines, standards and policies that apply to the work they will be performing for their contracting agency, that they will communicate these provisions to and enforce them against their subcontractors, and that they will implement and maintain any other reasonable and appropriate security procedures and practices necessary to protect personal information to which they are given access as part of the contract from unauthorized access, destruction, use, modification, disclosure or loss. The foregoing contractual provisions shall be drafted by ITD, the Office of the Comptroller, and the Operational Services Division, which shall develop and implement uniform language to be incorporated into all contracts that are executed by state agencies. The provisions shall be enforced through the contracting agency and the Operational Services Division. Any breach shall be regarded as a material breach of the contract that may subject the contractor to appropriate sanctions.*

*Section 10. In performing their responsibilities under this Order, ITD, the CIO and the Operational Services Division shall have the full cooperation of all state agencies, including compliance with all requests for information.*

*Section 11. This Executive Order shall take effect immediately and shall continue in effect until amended, superseded or revoked by subsequent Executive Order.*



## APPENDIX I

### Executive Order 490 (Revoking and Superseding Executive Order 475)

*WHEREAS, the security and well-being of the people of the Commonwealth depend on our ability to ensure continuity of government;*

*WHEREAS, effective preparedness planning requires the identification of functions that must be performed during an emergency and the assignment of responsibility for developing and implementing plans for performing those functions;*

*WHEREAS, to accomplish these aims each secretariat within the executive department was directed to develop a Continuity of Government plan identifying an official line of succession for vital positions, prioritizing essential functions, designating alternate command sites, and establishing procedures for safeguarding personnel and resources; and each secretariat and agency within the executive department was directed to develop a Continuity of Operations Plan establishing emergency operating procedures, delegating specific emergency authority to key personnel, establishing reliable, interoperable communications, and providing for the safekeeping of critical systems, records, and databases;*

*WHEREAS, Continuity of Government and Continuity of Operations plans have been developed by the Office of the Governor and every secretariat and agency within the executive department and all one hundred and two of these plans are currently stored in paper form at the Massachusetts Emergency Management Agency;*

*WHEREAS, to achieve a maximum state of readiness, these plans should be incorporated into the daily operations of every secretariat and agency in the executive department, and should be reviewed on a regular basis and, with respect to agencies supplying services critical in times of emergency, exercised regularly;*

*WHEREAS, to allow greater access to these plans, ensure their security and sustainability, and encourage more active participation and review by the secretariats and agencies, they should be maintained on a secure online database; and*

*WHEREAS, the Executive Office of Public Safety and Security and Massachusetts Emergency Management Agency are collaborating with the Information Technology Department to develop an online tool and database to maintain these Continuity of Government and Continuity of Operations plans;*

*NOW, THEREFORE, I, Deval L. Patrick, Governor of the Commonwealth of Massachusetts, by virtue of the authority vested in me by the Constitution, Part 2, c. 2, § 1, Art. 1, do hereby revoke Executive Order 475 and order as follows:*

*Section 1. Each secretariat and agency within the executive department shall continue to consider emergency preparedness functions in the conduct of its regular operations, particularly those functions which would be critical in a time of emergency.*

*Section 2. The Secretary of Public Safety and Security (hereinafter, "the Secretary"), in his discretion, shall designate secretariats and agencies as either critical or non-critical for the purpose of determining the detail, frequency of submission, and testing of Continuity of Government and Continuity of Operations plans.*

*Section 3. The Secretary shall notify all secretariats and agencies of the completion of the online Continuity of Operation / Continuity of Government tool and database (hereinafter, "the online tool"). Within 120 days of notification of completion of the online tool, each secretariat and agency shall submit, via the online tool, the appropriate Continuity of Government plan and/or Continuity of Operations plan based upon its critical or non-critical designation.*

*Section 4. If the Secretary designates a secretariat or agency as critical, then that secretariat or agency shall regularly, and in no event less than once per calendar year, conduct trainings and exercises to put into practice its submitted Continuity of Government and Continuity of Operations plans.*

*Section 5. These trainings and exercises shall be designed to simulate emergency situations which may arise, and shall be designed to test the effectiveness of the various components of the Continuity of Government and Continuity of Operations plans. These exercises must, at a minimum, include transfer of command functions to an emergency relocation site and the use of emergency communication systems.*

*Section 6. Each designated critical secretariat within the executive department shall incorporate findings from these trainings and exercises into its Continuity of Government and Continuity of Operations plans, and based on these findings, shall regularly, and in no event less than once per calendar year, update these plans using the online tool. Likewise, each designated critical agency within the executive department shall incorporate findings from these trainings and exercises into its Continuity of Operations plan, and based on these findings, shall regularly, and in no event less than once per calendar year, update its Continuity of Operations plan using the online tool. In addition, each critical secretariat and agency shall submit an annual report to the Executive Office of Public Safety and Security detailing the trainings and exercises conducted and the actions taken to incorporate the findings of such trainings and exercises into updated Continuity of Government and Continuity of Operations plans.*

*Section 7. Each non-critical agency within the executive department shall conduct activities on an annual basis that support the implementation of its Continuity of Operations plan, including but not limited to ensuring that the plan is current and viable, and shall regularly, and in no event less than once per calendar year, update these plans using the online tool. In addition, each non-critical agency shall submit an annual report to the Executive Office of Public Safety and Security detailing the actions taken to implement such plan.*

*Section 8. The Executive Office of Public Safety and Security shall submit an annual report to the Office of the Governor regarding the status of the Continuity of Government plan of each secretariat within the executive department, and the status of the Continuity of Operations plan of each secretariat and agency within the executive department.*

*Section 9. This Executive Order shall continue in effect until amended, superseded, or revoked by subsequent Executive Order.*

## APPENDIX J

### Abbreviations

audit command language	ACL
Board of Registration in Medicine	the Board
business continuity plan	BCP
Code of Massachusetts Regulations	CMR
Consolidated Licensing and Regulation Information System	CLARIS
continuation without a finding	CWOF
Criminal Offender Record Information	CORI
Department of Criminal Justice Information Services	DCJIS
Department of Public Health	DPH
electronic security plan	ESP
Executive Office for Administration and Finance	EOAF
Executive Office of Health and Human Services	EOHHS
Executive Office of the Trial Court	EOTC
Executive Order 504	EO504
Executive Order 510	EO510
information security officer	ISO
information security program	ISP
information technology	IT
Information Technology Division	ITD
Office of the State Auditor	OSA
Office of the State Comptroller	OSC
operating under the influence	OUI
payment card industry	PCI
Payment Card Industry Data Security Standard	PCI DSS
personally identifiable information	PII
Qualified Security Assessor	QSA
Self-Assessment Questionnaire	SAQ