

**SENATE . . . . . No. 195**

---

**The Commonwealth of Massachusetts**

PRESENTED BY:

***Marc R. Pacheco***

*To the Honorable Senate and House of Representatives of the Commonwealth of Massachusetts in General Court assembled:*

The undersigned legislators and/or citizens respectfully petition for the adoption of the accompanying bill:

An Act to clarify and enhance privacy protections for electronic health records.

PETITION OF:

NAME:	DISTRICT/ADDRESS:	
<i>Marc R. Pacheco</i>	<i>First Plymouth and Bristol</i>	
<i>Sal N. DiDomenico</i>	<i>Middlesex and Suffolk</i>	<i>2/2/2017</i>
<i>Michael D. Brady</i>	<i>Second Plymouth and Bristol</i>	<i>2/3/2017</i>

**SENATE . . . . . No. 195**

---

---

By Mr. Pacheco, a petition (accompanied by bill, Senate, No. 195) of Marc R. Pacheco, Sal N. DiDomenico and Michael D. Brady for legislation to clarify and enhance privacy protections for electronic health records. Economic Development and Emerging Technologies.

---

---

[SIMILAR MATTER FILED IN PREVIOUS SESSION  
SEE SENATE, NO. 226 OF 2015-2016.]

**The Commonwealth of Massachusetts**

—————  
**In the One Hundred and Ninetieth General Court  
(2017-2018)**  
—————

An Act to clarify and enhance privacy protections for electronic health records.

*Be it enacted by the Senate and House of Representatives in General Court assembled, and by the authority of the same, as follows:*

1           SECTION 1. The third paragraph of subsection (d) of section 6D of chapter 40J of the  
2 General Laws is hereby amended by striking clause (v) and inserting in place thereof the  
3 following clause:—

4           (v) give patients the option of allowing only designated health care providers to  
5 disseminate their individually identifiable health information to any statewide interoperable  
6 electronic health records network or statewide health information exchange;

7           SECTION 2. Section 6F of chapter 40J of the General Laws is hereby amended by  
8 striking the first paragraph and inserting in place thereof the following paragraph:—

9 Any plan for a statewide interoperable electronic health records network or statewide  
10 health information exchange approved by the health information technology council and every  
11 grantee and implementing organization that receives monies for the adoption of health  
12 information technology from the E-Health Institute Fund or pursuant to this chapter shall:

13 SECTION 3. Said section 6F of chapter 40J of the General Laws, as appearing in section  
14 4 of chapter 305 of the acts of 2014, is hereby further amended by inserting after the  
15 word “accessed”, in line 396, the following words:— ; and (5) require every grantee and  
16 implementing organization funded in whole or in part by the E-Health Institute Fund to conduct  
17 privacy and security audits of any and all interoperable electronic health records networks, health  
18 information exchanges, and participating entities that maintain electronic health records for  
19 potential and actual privacy and security breaches by July 1 of each year. Each grantee and  
20 implementing organization shall report the results of the annual audit to the health information  
21 technology council by July 1. The council shall report within 30 days to the Attorney General  
22 any audit result that indicates a violation of the rules and regulations adopted by the health  
23 information technology council or Department of Public Health pursuant to this chapter.

24 SECTION 4. Section 6G of said chapter 40J of the General Laws is hereby amended by  
25 inserting after the first paragraph the following paragraphs:—

26 For the purposes of this chapter, the health information technology council shall  
27 promulgate rules and regulations necessary for the administration and enforcement of this  
28 chapter, including but not limited to defining the following terms: “identifiable health  
29 information”, “unauthorized access” and “unauthorized disclosure.”

30 Any aggrieved individual claiming that any interoperable electronic health records  
31 network or health information exchange, its operators, contractors or agents, and participating  
32 entities that maintain electronic health records, funded in whole or in part by the E-Health  
33 Institute Fund failed to maintain the privacy and security protections required in Section 6F of  
34 this chapter or permitted an unauthorized access or disclosure as defined by the Health  
35 Information Technology Council pursuant to Section 6G of this chapter may bring a civil action  
36 in Superior Court.

37 The Attorney General may bring a civil action in Superior Court to enforce the privacy  
38 and data security obligations of health information network grantees, their operators, agents, and  
39 contractors, subject to GL Chapter 40J.

40 A court shall find a violation and order relief if it determines that any of the following  
41 circumstances has occurred:

42 any interoperable electronic health records network or health information exchange, its  
43 operators, contractors, or agents, and participating entities that maintain electronic health  
44 records, funded in whole or in part by the E-Health Institute Fund, failed to maintain safeguards  
45 for the confidentiality and security of protected health information in violation of this chapter or  
46 any rule or regulation promulgated by the health information technology council pursuant to this  
47 chapter; or

48 any interoperable electronic health records network or health information exchange, its  
49 operators, contractors, or agents, and participating entities that maintain electronic health  
50 records, funded in whole or in part by the E-Health Institute Fund, disclosed without

51 authorization identifiable health information as defined by any rule or regulation promulgated by  
52 the health information technology advisory council pursuant to this chapter; or

53 any interoperable electronic health records network or health information exchange, its  
54 operators, contractors, or agents, and participating entities that maintain electronic health  
55 records, funded in whole or in part by the E-Health Institute Fund, failed to provide notice of an  
56 unauthorized access or disclosure as required by Section 6G of Chapter 40J.

57 The court may order any interoperable electronic health records network or health  
58 information exchange, its operators, contractors or agents, or any participating entity or  
59 individual, to comply with this chapter and may order any other appropriate civil or equitable  
60 relief, including an injunction to prevent non-compliance. If the court determines that there has  
61 been a violation of this chapter, the aggrieved person is entitled to recover damages for losses  
62 sustained as a result of this violation.

63 The measure of damages shall be the greater of the aggrieved person's actual damages, or  
64 liquidated damages of \$1,000 for each violation, except that the total amount imposed on the  
65 offending party for all violations of an identical requirement or prohibition during a calendar  
66 year may not exceed \$100,000. If the court determines that there has been a violation of this  
67 chapter that results from willful or grossly negligent conduct, the aggrieved person may recover  
68 punitive damages not to exceed \$10,000, exclusive of any other loss, for each violation, except  
69 that the total amount imposed on the offending party for all violations of an identical requirement  
70 or prohibition during a calendar year may not exceed \$500,000 from the offending party.

71 If the aggrieved person prevails, the court shall assess reasonable attorney's fees and all  
72 other expenses reasonably incurred in the litigation against the non-prevailing parties.

73 Responsible parties are jointly and severally liable for any compensatory damages, attorney's  
74 fees or other costs awarded. Any action under this section is barred unless the action is  
75 commenced within three years after the cause of action accrues or was or should reasonably have  
76 been discovered by the aggrieved person or the person's lawful representative.

77 No employee shall be terminated, discharged, or retaliated against because he does any of  
78 the following based on a reasonable belief that an activity, policy or practice of the employer or  
79 another entity with whom the employer has a relationship violates this chapter or any rule or  
80 regulation promulgated pursuant to this chapter:

81 (1) objects to or refuses to participate in any such activity, policy or practice;

82 (2) discloses or threatens to disclose such activity, policy or practice to a supervisor,  
83 manager, public official, public body, or other entity; or

84 (3) provides information to or testifies before anybody conducting an investigation,  
85 hearing or inquiry into any violation of this chapter, or rule or regulation promulgated pursuant  
86 to this chapter.