

AN ACT

1 Amending the act of December 22, 2005 (P.L.474, No.94), entitled
2 "An act providing for the notification of residents whose
3 personal information data was or may have been disclosed due
4 to a security system breach; and imposing penalties," further
5 providing for notification of breach.

6 The General Assembly of the Commonwealth of Pennsylvania
7 hereby enacts as follows:

8 Section 1. Section 3 of the act of December 22, 2005
9 (P.L.474, No.94), known as the Breach of Personal Information
10 Notification Act, is amended by adding subsections to read:

11 Section 3. Notification of breach.

12 * * *

13 (a.1) Notification by State agency.--If a State agency is
14 the subject of a breach of security of the system, the State
15 agency shall provide notice of the breach of security of the
16 system required under subsection (a) within seven days following
17 discovery of the breach. Notification shall be provided to the
18 Office of Attorney General within three business days following
19 discovery of the breach. A State agency under the Governor's

1 jurisdiction shall also provide notice of a breach of its
2 security system to the Governor's Office of Administration
3 within three business days following the discovery of the
4 breach. Notification shall occur regardless of the existence of
5 procedures and policies under section 7.

6 (a.2) Notification by county, school district or
7 municipality.--If a county, school district or municipality is
8 the subject of a breach of security of the system, the county,
9 school district or municipality shall provide notice of the
10 breach of security of the system required under subsection (a)
11 within seven days following discovery of the breach.
12 Notification shall be provided to the district attorney in the
13 county in which the breach occurred within three business days
14 following discovery of the breach. Notification shall occur
15 regardless of the existence of procedures and policies under
16 section 7.

17 (a.3) Storage policy.--

18 (1) The Office of Administration shall develop a policy
19 to govern the proper storage by State agencies of data which
20 includes personally identifiable information. The policy
21 shall address identifying, collecting, maintaining,
22 displaying and transferring personally identifiable
23 information, using personally identifiable information in
24 test environments, remediating personally identifiable
25 information stored on legacy systems and other relevant
26 issues. A goal of the policy shall be to reduce the risk of
27 future breaches of security of the system.

28 (2) In developing the policy under paragraph (1), the
29 Office of Administration shall consider similar existing
30 policies in other states, best practices identified by other

1 states and relevant studies and other sources as appropriate.
2 The policy shall be reviewed at least annually and updated as
3 necessary.

4 * * *

5 Section 2. This act shall take effect in 60 days.