

# HOUSE BILL 716

P1

9lr0130

---

By: **Chair, Health and Government Operations Committee (By Request – Departmental – Information Technology)**

Introduced and read first time: February 7, 2019

Assigned to: Health and Government Operations

---

Committee Report: Favorable with amendments

House action: Adopted

Read second time: March 13, 2019

---

## CHAPTER \_\_\_\_\_

1 AN ACT concerning

2 **State Government – Protection of Information – Revisions**  
3 **(Maryland Data Privacy Act)**

4 FOR the purpose of requiring certain units of State government to comply with certain  
5 standards and guidelines to ensure that the security of all information systems and  
6 applications are managed through a certain framework; requiring certain units of  
7 State government to undertake activities comprising collection, processing, and  
8 sharing of personally identifiable information in good faith and in accordance with a  
9 certain provision of this Act; requiring the units to identify and document certain  
10 legal authority, describe a certain purpose and make certain notifications, adopt a  
11 certain privacy governance and risk management program, implement certain  
12 security measures, establish certain privacy requirements and incorporate the  
13 requirements into certain agreements, take certain steps, implement certain  
14 processes, and establish certain notice provisions; requiring the units to advise  
15 certain individuals whether certain information is required to be provided by law or  
16 whether the provision is voluntary and subject to certain discretion; requiring the  
17 units to provide an individual with certain means to access certain information and  
18 certain third parties; requiring the units to include certain means in certain notices  
19 and provide certain notices to individuals at or before the point of sharing personally  
20 identifiable information; requiring the units to provide an individual with a certain  
21 process and the means to opt out of sharing information with third parties under  
22 certain circumstances; establishing that certain provisions of law do not apply to the  
23 Office of the Attorney General or the University System of Maryland; providing for  
24 the application of certain provisions of law; defining certain terms; repealing certain

---

EXPLANATION: CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.

[Brackets] indicate matter deleted from existing law.

Underlining indicates amendments to bill.

~~Strike out~~ indicates matter stricken from the bill by amendment or deleted from the law by amendment.



1 definitions; making conforming changes; providing for the effective date of certain  
2 provisions of this Act; providing for the termination of certain provisions of this Act;  
3 and generally relating to the protection of personally identifiable information by  
4 government agencies.

5 BY repealing and reenacting, with amendments,

6 Article – State Government

7 Section 10–1301 through 10–1304 and 10–1305(a), (b)(1) and (2), (c)(1), (g)(1), (h)(2),  
8 and (j)

9 Annotated Code of Maryland

10 (2014 Replacement Volume and 2018 Supplement)

11 BY adding to

12 Article – State Government

13 Section 10–13A–01 through 10–13A–08 to be under the new subtitle “Subtitle 13A.  
14 Protection of Information by the University System of Maryland”

15 Annotated Code of Maryland

16 (2014 Replacement Volume and 2018 Supplement)

17 BY repealing and reenacting, with amendments,

18 Article – State Government

19 Section 10–1302(c)

20 Annotated Code of Maryland

21 (2014 Replacement Volume and 2018 Supplement)

22 (As enacted by Section 1 of this Act)

23 SECTION 1. BE IT ENACTED BY THE GENERAL ASSEMBLY OF MARYLAND,

24 That the Laws of Maryland read as follows:

25 **Article – State Government**

26 10–1301.

27 (a) In this subtitle the following words have the meanings indicated.

28 (b) “Encryption” means the protection of data in electronic or optical form, in  
29 storage or in transit, using a technology that:

30 (1) is certified to meet or exceed the level that has been adopted by the  
31 Federal Information Processing Standards issued by the National Institute of Standards  
32 and Technology; and

33 (2) renders such data indecipherable without an associated cryptographic  
34 key necessary to enable decryption of such data.

1 [(c) (1) “Personal information” means an individual’s first name or first initial  
2 and last name, personal mark, or unique biometric or genetic print or image, in combination  
3 with one or more of the following data elements:

4 (i) a Social Security number;

5 (ii) a driver’s license number, state identification card number, or  
6 other individual identification number issued by a unit;

7 (iii) a passport number or other identification number issued by the  
8 United States government;

9 (iv) an Individual Taxpayer Identification Number; or

10 (v) a financial or other account number, a credit card number, or a  
11 debit card number that, in combination with any required security code, access code, or  
12 password, would permit access to an individual’s account.

13 (2) “Personal information” does not include a voter registration number.

14 (d) “Reasonable security procedures and practices” means data security  
15 procedures and practices developed, in good faith, and set forth in a written information  
16 security policy.]

17 (C) “INDIVIDUAL” MEANS AN INDIVIDUAL WHO INTERACTS WITH A UNIT.

18 (D) (1) “PERSONALLY IDENTIFIABLE INFORMATION” MEANS  
19 INFORMATION THAT CAN BE USED TO DISTINGUISH OR TRACE AN INDIVIDUAL’S  
20 IDENTITY, EITHER ALONE OR WHEN COMBINED WITH OTHER INFORMATION  
21 ASSOCIATED WITH A PARTICULAR INDIVIDUAL, INCLUDING:

22 (I) UNIQUE PERSONAL IDENTIFIERS, INCLUDING:

23 1. A FULL NAME;

24 2. A FIRST INITIAL AND LAST NAME;

25 3. A SOCIAL SECURITY NUMBER;

26 4. A DRIVER’S LICENSE NUMBER, A STATE  
27 IDENTIFICATION NUMBER, OR ANY OTHER IDENTIFICATION NUMBER ISSUED BY A  
28 UNIT; AND

29 5. A PASSPORT NUMBER;

1 (II) CHARACTERISTICS OF CLASSIFICATIONS PROTECTED  
2 UNDER FEDERAL OR STATE LAW;

3 (III) BIOMETRIC INFORMATION INCLUDING AN INDIVIDUAL'S  
4 PHYSIOLOGICAL, BIOLOGICAL, OR BEHAVIORAL CHARACTERISTICS, INCLUDING AN  
5 INDIVIDUAL'S DEOXYRIBONUCLEIC ACID (DNA), THAT CAN BE USED, SINGLY OR IN  
6 COMBINATION WITH EACH OTHER OR WITH OTHER IDENTIFYING DATA, TO  
7 ESTABLISH INDIVIDUAL IDENTITY;

8 (IV) GEOLOCATION DATA;

9 (V) INTERNET OR OTHER ELECTRONIC NETWORK ACTIVITY  
10 INFORMATION, INCLUDING BROWSING HISTORY, SEARCH HISTORY, AND  
11 INFORMATION REGARDING AN INDIVIDUAL'S INTERACTION WITH AN INTERNET  
12 WEBSITE, APPLICATION, OR ADVERTISEMENT;

13 (VI) INFORMATION FROM MULTIPLE SOURCES THAT WHEN USED  
14 IN COMBINATION WITH EACH OTHER OR OTHER IDENTIFYING INFORMATION CAN BE  
15 USED TO ESTABLISH INDIVIDUAL IDENTITY; AND

16 (VII) A FINANCIAL OR OTHER ACCOUNT NUMBER, A CREDIT CARD  
17 NUMBER, OR A DEBIT CARD NUMBER THAT, IN COMBINATION WITH ANY REQUIRED  
18 SECURITY CODE, ACCESS CODE, OR PASSWORD, WOULD PERMIT ACCESS TO AN  
19 INDIVIDUAL'S ACCOUNT.

20 (2) "PERSONALLY IDENTIFIABLE INFORMATION" DOES NOT  
21 INCLUDE:

22 (I) VOTER REGISTRATION INFORMATION;

23 (II) INFORMATION PUBLICLY DISCLOSED BY THE INDIVIDUAL  
24 WITHOUT BEING UNDER DURESS OR COERCION; OR

25 (III) DATA RENDERED ANONYMOUS THROUGH THE USE OF  
26 TECHNIQUES, INCLUDING OBFUSCATION, DELETION AND REDACTION, AND  
27 ENCRYPTION, SO THAT THE INDIVIDUAL IS NO LONGER IDENTIFIABLE.

28 (E) "REASONABLE SECURITY PROCEDURES AND PRACTICES" MEANS  
29 SECURITY PROTECTIONS THAT ALIGN WITH DEPARTMENT OF INFORMATION  
30 TECHNOLOGY POLICIES AND THE FEDERAL INFORMATION SECURITY  
31 MODERNIZATION ACT (FISMA) OF 2014.

32 [(e)] (F) "Records" means information that is inscribed on a tangible medium or  
33 that is stored in an electronic or other medium and is retrievable in perceivable form.

1            **[(f)] (G)**        “Unit” means:

2                    (1)     an executive agency, or a department, a board, a commission, an  
3 authority, a public institution of higher education, a unit or an instrumentality of the State;  
4 or

5                    (2)     a county, municipality, bi-county, regional, or multicounty agency,  
6 county board of education, public corporation or authority, or any other political subdivision  
7 of the State.

8 10–1302.

9            **(A) (1) SUBJECT TO PARAGRAPH (2) OF THIS SUBSECTION, THIS**  
10 **SUBTITLE APPLIES ONLY TO THE COLLECTION, PROCESSING, AND SHARING OF**  
11 **PERSONALLY IDENTIFIABLE INFORMATION BY A UNIT.**

12            **(2) THIS SUBTITLE DOES NOT APPLY TO THE COLLECTION,**  
13 **PROCESSING, OR SHARING OF PERSONALLY IDENTIFIABLE INFORMATION**  
14 **EXCLUSIVELY FOR PURPOSES OF:**

15                    **(I) PUBLIC HEALTH;**

16                    **(II) PUBLIC SAFETY;**

17                    **(III) STATE SECURITY; OR**

18                    **(IV) THE INVESTIGATION AND PROSECUTION OF CRIMINAL**  
19 **OFFENSES.**

20            **[(a)] (B)**        This subtitle does not apply to **[personal] PERSONALLY**  
21 **IDENTIFIABLE** information that:

22                    (1)     is publicly available information that is lawfully made available to the  
23 general public from federal, State, or local government records;

24                    (2)     an individual has consented to have publicly disseminated or listed;

25                    (3)     except for a medical record that a person is prohibited from redisclosing  
26 under § 4–302(d) of the Health – General Article, is disclosed in accordance with the federal  
27 Health Insurance Portability and Accountability Act; or

28                    (4)     is disclosed in accordance with the federal Family Educational Rights  
29 and Privacy Act.

1           **[(b)] (C)**       This subtitle does not apply to the Legislative or Judicial Branch of  
2 State government, **THE OFFICE OF THE ATTORNEY GENERAL, OR THE UNIVERSITY**  
3 **SYSTEM OF MARYLAND.**

4 10–1303.

5           When a unit is destroying records of an individual that contain [personal]  
6 **PERSONALLY IDENTIFIABLE** information of the individual, the unit shall take reasonable  
7 steps to protect against unauthorized access to or use of the [personal] **PERSONALLY**  
8 **IDENTIFIABLE** information, taking into account:

- 9           (1)     the sensitivity of the records;
- 10           (2)    the nature of the unit and its operations;
- 11           (3)    the costs and benefits of different destruction methods; and
- 12           (4)    available technology.

13 10–1304.

14           (a)    **(1)**    To protect [personal] **PERSONALLY IDENTIFIABLE** information from  
15 unauthorized access, use, modification, or disclosure **AND SUBJECT TO PARAGRAPH (2)**  
16 **OF THIS SUBSECTION**, a unit that collects [personal] **PERSONALLY IDENTIFIABLE**  
17 information of an individual shall implement and maintain reasonable security procedures  
18 and practices that are appropriate to the nature of the [personal] **PERSONALLY**  
19 **IDENTIFIABLE** information collected and the nature of the unit and its operations.

20           **(2)    THE UNIT SHALL COMPLY WITH STANDARDS AND GUIDELINES,**  
21 **INCLUDING FEDERAL INFORMATION PROCESSING STANDARDS (FIPS) 199, FIPS**  
22 **200, AND THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)**  
23 **SPECIAL PUBLICATION (SP) 800 SERIES, TO ENSURE THAT THE SECURITY OF ALL**  
24 **INFORMATION SYSTEMS AND APPLICATIONS IS MANAGED THROUGH THE NIST RISK**  
25 **MANAGEMENT FRAMEWORK ~~DEFINED IN NIST SP 800-37 REV 1~~, WHICH REQUIRES**  
26 **THAT:**

27                   **(I)    THE SYSTEM IS CATEGORIZED BASED ON A FIPS 199**  
28 **ANALYSIS;**

29                   **(II)   THE SECURITY CONTROLS ARE SELECTED BASED ON THE**  
30 **SECURITY CATEGORIZATION OF THE SYSTEM;**

31                   **(III) THE CONTROLS ARE IMPLEMENTED WITHIN THE**  
32 **INFORMATION SYSTEM OR APPLICATION;**

1 (IV) THE CONTROLS ARE ASSESSED BY A  
2 THIRD-PARTY ASSESSOR;

3 (V) THE SYSTEM IS AUTHORIZED TO OPERATE BY AN  
4 AUTHORIZING OFFICIAL WHO REVIEWS THE SECURITY AUTHORIZATION PACKAGE  
5 AND ACCEPTS THE RISKS IDENTIFIED;

6 (VI) THE IMPLEMENTED SECURITY CONTROLS ARE  
7 CONTINUOUSLY MONITORED FOR EFFECTIVENESS; AND

8 (VII) THE REASSESSMENT AND AUTHORIZATION OF SYSTEMS ARE  
9 TO BE COMPLETED ON AN ANNUAL BASIS.

10 (b) (1) This subsection shall apply to a written contract or agreement that is  
11 entered into on or after July 1, 2014.

12 (2) A unit that uses a nonaffiliated third party as a service provider to  
13 perform services for the unit and discloses [personal] PERSONALLY IDENTIFIABLE  
14 information about an individual under a written contract or agreement with the third party  
15 shall require by written contract or agreement that the third party implement and  
16 maintain reasonable security procedures and practices that:

17 (i) are appropriate to the nature of the [personal] PERSONALLY  
18 IDENTIFIABLE information disclosed to the nonaffiliated third party; and

19 (ii) are reasonably designed to help protect the [personal]  
20 PERSONALLY IDENTIFIABLE information from unauthorized access, use, modification,  
21 disclosure, or destruction.

22 (C) (1) EACH UNIT SHALL UNDERTAKE ACTIVITIES COMPRISING THE  
23 COLLECTION, PROCESSING, AND SHARING OF PERSONALLY IDENTIFIABLE  
24 INFORMATION IN GOOD FAITH AND IN ACCORDANCE WITH THE REQUIREMENTS  
25 UNDER PARAGRAPH (2) OF THIS SUBSECTION.

26 (2) EACH UNIT SHALL:

27 (I) IDENTIFY AND DOCUMENT THE LEGAL AUTHORITY FOR THE  
28 UNIT'S COLLECTION OF PERSONALLY IDENTIFIABLE INFORMATION;

29 (II) DESCRIBE THE PURPOSE OF THE PERSONALLY  
30 IDENTIFIABLE INFORMATION COLLECTION AND PROVIDE NOTICE OF THE  
31 PERSONALLY IDENTIFIABLE INFORMATION COLLECTION TO THE INDIVIDUAL AT  
32 THE TIME OF COLLECTION AND IN A PRIVACY NOTICE PROMINENTLY DISPLAYED ON  
33 THE UNIT'S WEBSITE;

1 (III) ADOPT A PRIVACY GOVERNANCE AND RISK MANAGEMENT  
2 PROGRAM AND IMPLEMENT REASONABLE SECURITY PROCEDURES AND PRACTICES,  
3 CONSISTENT WITH POLICIES AND STANDARDS ESTABLISHED BY THE DEPARTMENT  
4 OF INFORMATION TECHNOLOGY, TO ENSURE THAT CONFIDENTIALITY, INTEGRITY,  
5 AND AVAILABILITY OF ALL PERSONALLY IDENTIFIABLE INFORMATION IS  
6 MAINTAINED;

7 (IV) ESTABLISH PRIVACY REQUIREMENTS APPLICABLE TO  
8 CONTRACTORS, SERVICE PROVIDERS, AND OTHER THIRD PARTIES AND  
9 INCORPORATE THE REQUIREMENTS INTO AGREEMENTS ENTERED INTO WITH THE  
10 THIRD PARTIES;

11 (V) TAKE REASONABLE STEPS TO ENSURE THAT PERSONALLY  
12 IDENTIFIABLE INFORMATION COLLECTED IS ACCURATE, RELEVANT, TIMELY, AND  
13 COMPLETE;

14 (VI) TAKE REASONABLE STEPS TO IMPLEMENT MEANS TO  
15 MINIMIZE THE PERSONALLY IDENTIFIABLE INFORMATION COLLECTED TO  
16 INFORMATION RELEVANT AND NECESSARY TO ADDRESS THE LEGALLY AUTHORIZED  
17 PURPOSE OF THE COLLECTION;

18 (VII) IMPLEMENT PROCESSES TO PROVIDE AN INDIVIDUAL  
19 ACCESS TO THE INDIVIDUAL'S PERSONALLY IDENTIFIABLE INFORMATION AND TO  
20 ALLOW THE INDIVIDUAL TO CORRECT OR AMEND THE PERSONALLY IDENTIFIABLE  
21 INFORMATION PROCESSED BY THE UNIT; AND

22 (VIII) SUBJECT TO SUBSECTION (D) OF THIS SECTION, ESTABLISH  
23 CLEAR AND COMPREHENSIVE NOTICE PROVISIONS TO INFORM THE PUBLIC AND  
24 INDIVIDUALS OF UNIT PRACTICES AND ACTIVITIES REGARDING THE USE OF  
25 PERSONALLY IDENTIFIABLE INFORMATION.

26 (D) EACH UNIT SHALL:

27 (1) ADVISE AN INDIVIDUAL REQUESTED TO PROVIDE PERSONALLY  
28 IDENTIFIABLE INFORMATION WHETHER:

29 (I) THE PERSONALLY IDENTIFIABLE INFORMATION  
30 REQUESTED IS REQUIRED TO BE PROVIDED BY LAW; OR

31 (II) THE PROVISION OF THE PERSONALLY IDENTIFIABLE  
32 INFORMATION REQUESTED IS VOLUNTARY AND SUBJECT TO THE INDIVIDUAL'S  
33 DISCRETION TO REFUSE TO PROVIDE THE PERSONALLY IDENTIFIABLE  
34 INFORMATION;



1                   **(2) PROVIDE AN INDIVIDUAL WITH CLEAR AND CONSPICUOUS MEANS**  
2 **TO ACCESS:**

3                   **(I) THE TYPES OF PERSONALLY IDENTIFIABLE INFORMATION**  
4 **COLLECTED ABOUT THE INDIVIDUAL;**

5                   **(II) THE TYPES OF SOURCES FROM WHICH THE PERSONALLY**  
6 **IDENTIFIABLE INFORMATION WAS COLLECTED;**

7                   **(III) THE PURPOSE FOR COLLECTING THE PERSONALLY**  
8 **IDENTIFIABLE INFORMATION;**

9                   **(IV) THE THIRD PARTIES WITH WHOM THE PERSONALLY**  
10 **IDENTIFIABLE INFORMATION IS SHARED; AND**

11                   **(V) THE SPECIFIC PERSONALLY IDENTIFIABLE INFORMATION**  
12 **COLLECTED ABOUT THE INDIVIDUAL;**

13                   **(3) INCLUDE THE MEANS PROVIDED UNDER ITEM (2) OF THIS**  
14 **SUBSECTION IN THE NOTICES PROVIDED TO THE INDIVIDUAL REGARDING THE**  
15 **COLLECTION, PROCESSING, AND SHARING OF THE INDIVIDUAL'S PERSONALLY**  
16 **IDENTIFIABLE INFORMATION;**

17                   **(4) AT OR BEFORE THE POINT OF SHARING PERSONALLY**  
18 **IDENTIFIABLE INFORMATION, PROVIDE NOTICE TO AN INDIVIDUAL OF THE UNIT'S**  
19 **SHARING OF THE INDIVIDUAL'S PERSONALLY IDENTIFIABLE INFORMATION,**  
20 **INCLUDING:**

21                   **(I) THE NATURE AND SOURCES OF INFORMATION SHARED;**

22                   **(II) THE PURPOSE FOR WHICH THE INFORMATION IS SHARED;**

23                   **(III) THE RECIPIENTS OF THE SHARED INFORMATION;**

24                   **(IV) THE AUTHORITY UNDER WHICH THE INFORMATION IS**  
25 **SHARED;**

26                   **(V) ANY RIGHTS THE INDIVIDUAL HAS TO DECLINE THE UNIT'S**  
27 **SHARING OF PERSONALLY IDENTIFIABLE INFORMATION; AND**

28                   **(VI) THE INDIVIDUAL'S RIGHT AND MEANS TO OBTAIN AND**  
29 **REVIEW THE PERSONALLY IDENTIFIABLE INFORMATION SHARED BY THE UNIT;**

1           **(5) PROVIDE AN INDIVIDUAL A PROCESS TO DELETE OR CORRECT**  
2 **PERSONALLY IDENTIFIABLE INFORMATION SHARED WITH THIRD PARTIES IF THE**  
3 **SHARING OF THE INFORMATION IS NOT REQUIRED BY LAW; AND**

4           **(6) PROVIDE AN INDIVIDUAL THE MEANS TO OPT OUT OF SHARING**  
5 **INFORMATION WITH THIRD PARTIES IF THE SHARING OF THE INFORMATION IS NOT**  
6 **REQUIRED BY LAW.**

7 10-1305.

8           (a) (1) In this section, “breach of the security of a system” means the  
9 unauthorized acquisition of computerized data that compromises the security,  
10 confidentiality, or integrity of the [personal] **PERSONALLY IDENTIFIABLE** information  
11 maintained by a unit.

12           (2) “Breach of the security of a system” does not include the good faith  
13 acquisition of [personal] **PERSONALLY IDENTIFIABLE** information by an employee or  
14 agent of a unit for the purposes of the unit, provided that the [personal] **PERSONALLY**  
15 **IDENTIFIABLE** information is not used or subject to further unauthorized disclosure.

16           (b) (1) If a unit that collects computerized data that includes [personal]  
17 **PERSONALLY IDENTIFIABLE** information of an individual discovers or is notified of a  
18 breach of the security of a system, the unit shall conduct in good faith a reasonable and  
19 prompt investigation to determine whether the unauthorized acquisition of [personal]  
20 **PERSONALLY IDENTIFIABLE** information of the individual has resulted in or is likely to  
21 result in the misuse of the information.

22           (2) (i) Except as provided in subparagraph (ii) of this paragraph, if after  
23 the investigation is concluded, the unit determines that the misuse of the individual’s  
24 [personal] **PERSONALLY IDENTIFIABLE** information has occurred or is likely to occur, the  
25 unit or the nonaffiliated third party, if authorized under a written contract or agreement  
26 with the unit, shall notify the individual of the breach.

27           (ii) Unless the unit or nonaffiliated third party knows that the  
28 encryption key has been broken, a unit or the nonaffiliated third party is not required to  
29 notify an individual under subparagraph (i) of this paragraph if:

30                   1. the [personal] **PERSONALLY IDENTIFIABLE** information  
31 of the individual was secured by encryption or redacted; and

32                   2. the encryption key has not been compromised or disclosed.

33           (c) (1) A nonaffiliated third party that maintains computerized data that  
34 includes [personal] **PERSONALLY IDENTIFIABLE** information provided by a unit shall  
35 notify the unit of a breach of the security of a system if the unauthorized acquisition of the

1 individual's [personal] PERSONALLY IDENTIFIABLE information has occurred or is likely  
2 to occur.

3 (g) The notification required under subsection (b) of this section shall include:

4 (1) to the extent possible, a description of the categories of information that  
5 were, or are reasonably believed to have been, acquired by an unauthorized person,  
6 including which of the elements of [personal] PERSONALLY IDENTIFIABLE information  
7 were, or are reasonably believed to have been, acquired;

8 (h) (2) In addition to the notice required under paragraph (1) of this  
9 subsection, a unit, as defined in [§ 10–1301(f)(1)] § 10–1301(G)(1) of this subtitle, shall  
10 provide notice of a breach of security to the Department of Information Technology.

11 (j) Compliance with this section does not relieve a unit from a duty to comply  
12 with any other requirements of federal law relating to the protection and privacy of  
13 [personal] PERSONALLY IDENTIFIABLE information.

14 SECTION 2. AND BE IT FURTHER ENACTED, That the Laws of Maryland read  
15 as follows:

16 Article – State Government

17 TITLE 13A. PROTECTION OF INFORMATION BY THE UNIVERSITY SYSTEM OF  
18 MARYLAND.

19 10–13A–01.

20 (A) IN THIS SUBTITLE THE FOLLOWING WORDS HAVE THE MEANINGS  
21 INDICATED.

22 (B) “ENCRYPTION” MEANS THE PROTECTION OF DATA IN ELECTRONIC OR  
23 OPTICAL FORM, IN STORAGE OR IN TRANSIT, USING A TECHNOLOGY THAT:

24 (1) IS CERTIFIED TO MEET OR EXCEED THE LEVEL THAT HAS BEEN  
25 ADOPTED BY THE FEDERAL INFORMATION PROCESSING STANDARDS ISSUED BY  
26 THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY; AND

27 (2) RENDERS SUCH DATA INDECIPHERABLE WITHOUT AN  
28 ASSOCIATED CRYPTOGRAPHIC KEY NECESSARY TO ENABLE DECRYPTION OF SUCH  
29 DATA.

30 (C) (1) “PERSONAL INFORMATION” MEANS AN INDIVIDUAL’S FIRST NAME  
31 OR FIRST INITIAL AND LAST NAME, PERSONAL MARK, OR UNIQUE BIOMETRIC OR

1 GENETIC PRINT OR IMAGE, IN COMBINATION WITH ONE OR MORE OF THE  
2 FOLLOWING DATA ELEMENTS:

3 (I) A SOCIAL SECURITY NUMBER;

4 (II) A DRIVER'S LICENSE NUMBER, STATE IDENTIFICATION  
5 CARD NUMBER, OR OTHER INDIVIDUAL IDENTIFICATION NUMBER ISSUED BY THE  
6 UNIVERSITY SYSTEM OF MARYLAND;

7 (III) A PASSPORT NUMBER OR OTHER IDENTIFICATION NUMBER  
8 ISSUED BY THE UNITED STATES GOVERNMENT;

9 (IV) AN INDIVIDUAL TAXPAYER IDENTIFICATION NUMBER; OR

10 (V) A FINANCIAL OR OTHER ACCOUNT NUMBER, A CREDIT CARD  
11 NUMBER, OR A DEBIT CARD NUMBER THAT, IN COMBINATION WITH ANY REQUIRED  
12 SECURITY CODE, ACCESS CODE, OR PASSWORD, WOULD PERMIT ACCESS TO AN  
13 INDIVIDUAL'S ACCOUNT.

14 (2) "PERSONAL INFORMATION" DOES NOT INCLUDE A VOTER  
15 REGISTRATION NUMBER.

16 (D) "REASONABLE SECURITY PROCEDURES AND PRACTICES" MEANS DATA  
17 SECURITY PROCEDURES AND PRACTICES DEVELOPED, IN GOOD FAITH, AND SET  
18 FORTH IN A WRITTEN INFORMATION SECURITY POLICY.

19 (E) "RECORDS" MEANS INFORMATION THAT IS INSCRIBED ON A TANGIBLE  
20 MEDIUM OR STORED IN AN ELECTRONIC OR OTHER MEDIUM AND IS RETRIEVABLE  
21 IN PERCEIVABLE FORM.

22 10-13A-02.

23 (A) THIS SUBTITLE DOES NOT APPLY TO PERSONAL INFORMATION THAT:

24 (1) IS PUBLICLY AVAILABLE INFORMATION THAT IS LAWFULLY MADE  
25 AVAILABLE TO THE GENERAL PUBLIC FROM FEDERAL, STATE, OR LOCAL  
26 GOVERNMENT RECORDS;

27 (2) AN INDIVIDUAL HAS CONSENTED TO HAVE PUBLICLY  
28 DISSEMINATED OR LISTED;

29 (3) EXCEPT FOR A MEDICAL RECORD THAT A PERSON IS PROHIBITED  
30 FROM REDISCLOSING UNDER § 4-302(D) OF THE HEALTH - GENERAL ARTICLE, IS

1 DISCLOSED IN ACCORDANCE WITH THE FEDERAL HEALTH INSURANCE  
2 PORTABILITY AND ACCOUNTABILITY ACT; OR

3 (4) IS DISCLOSED IN ACCORDANCE WITH THE FEDERAL FAMILY  
4 EDUCATIONAL RIGHTS AND PRIVACY ACT.

5 (B) THIS SUBTITLE DOES NOT APPLY TO THE LEGISLATIVE BRANCH OR THE  
6 JUDICIAL BRANCH OF STATE GOVERNMENT.

7 10-13A-03.

8 WHEN THE UNIVERSITY SYSTEM OF MARYLAND IS DESTROYING RECORDS OF  
9 AN INDIVIDUAL THAT CONTAIN PERSONAL INFORMATION OF THE INDIVIDUAL, THE  
10 UNIVERSITY SYSTEM OF MARYLAND SHALL TAKE REASONABLE STEPS TO PROTECT  
11 AGAINST UNAUTHORIZED ACCESS TO OR USE OF THE PERSONAL INFORMATION,  
12 TAKING INTO ACCOUNT:

13 (1) THE SENSITIVITY OF THE RECORDS;

14 (2) THE NATURE OF THE UNIVERSITY SYSTEM OF MARYLAND AND ITS  
15 OPERATIONS;

16 (3) THE COSTS AND BENEFITS OF DIFFERENT DESTRUCTION  
17 METHODS; AND

18 (4) AVAILABLE TECHNOLOGY.

19 10-13A-04.

20 (A) TO PROTECT PERSONAL INFORMATION FROM UNAUTHORIZED ACCESS,  
21 USE, MODIFICATION, OR DISCLOSURE, THE UNIVERSITY SYSTEM OF MARYLAND  
22 INSTITUTION THAT COLLECTS PERSONAL INFORMATION OF AN INDIVIDUAL SHALL  
23 IMPLEMENT AND MAINTAIN REASONABLE SECURITY PROCEDURES AND PRACTICES  
24 THAT ARE APPROPRIATE TO THE NATURE OF THE PERSONAL INFORMATION  
25 COLLECTED AND THE NATURE OF THE UNIVERSITY SYSTEM OF MARYLAND AND ITS  
26 OPERATIONS.

27 (B) IF THE UNIVERSITY SYSTEM OF MARYLAND USES A NONAFFILIATED  
28 THIRD PARTY AS A SERVICE PROVIDER TO PERFORM SERVICES FOR THE  
29 UNIVERSITY SYSTEM OF MARYLAND AND DISCLOSES PERSONAL INFORMATION  
30 ABOUT AN INDIVIDUAL UNDER A WRITTEN CONTRACT OR AGREEMENT WITH THE  
31 THIRD PARTY SHALL REQUIRE BY WRITTEN CONTRACT OR AGREEMENT THAT THE  
32 THIRD PARTY IMPLEMENT AND MAINTAIN REASONABLE SECURITY PROCEDURES  
33 AND PRACTICES THAT:

1           (1) ARE APPROPRIATE TO THE NATURE OF THE PERSONAL  
2 INFORMATION DISCLOSED TO THE NONAFFILIATED THIRD PARTY; AND

3           (2) ARE REASONABLY DESIGNED TO HELP PROTECT THE PERSONAL  
4 INFORMATION FROM UNAUTHORIZED ACCESS, USE, MODIFICATION, DISCLOSURE,  
5 OR DESTRUCTION.

6 10-13A-05.

7           (A) (1) IN THIS SECTION, “BREACH OF THE SECURITY OF A SYSTEM”  
8 MEANS THE UNAUTHORIZED ACQUISITION OF COMPUTERIZED DATA THAT  
9 COMPROMISES THE SECURITY, CONFIDENTIALITY, OR INTEGRITY OF THE PERSONAL  
10 INFORMATION MAINTAINED BY THE UNIVERSITY SYSTEM OF MARYLAND.

11           (2) “BREACH OF THE SECURITY OF A SYSTEM” DOES NOT INCLUDE  
12 THE GOOD-FAITH ACQUISITION OF PERSONAL INFORMATION BY AN EMPLOYEE OR  
13 AGENT OF THE UNIVERSITY SYSTEM OF MARYLAND FOR THE PURPOSES OF THE  
14 UNIVERSITY SYSTEM OF MARYLAND, PROVIDED THAT THE PERSONAL  
15 INFORMATION IS NOT USED OR SUBJECT TO FURTHER UNAUTHORIZED DISCLOSURE.

16           (B) (1) IF THE UNIVERSITY SYSTEM OF MARYLAND INSTITUTION THAT  
17 COLLECTS COMPUTERIZED DATA THAT INCLUDES PERSONAL INFORMATION OF AN  
18 INDIVIDUAL DISCOVERS OR IS NOTIFIED OF A BREACH OF THE SECURITY OF A  
19 SYSTEM, THE UNIVERSITY SYSTEM OF MARYLAND SHALL CONDUCT IN GOOD FAITH  
20 A REASONABLE AND PROMPT INVESTIGATION TO DETERMINE WHETHER THE  
21 UNAUTHORIZED ACQUISITION OF PERSONAL INFORMATION OF THE INDIVIDUAL HAS  
22 RESULTED IN OR IS LIKELY TO RESULT IN THE MISUSE OF THE INFORMATION.

23           (2) (I) EXCEPT AS PROVIDED IN SUBPARAGRAPH (II) OF THIS  
24 PARAGRAPH, IF AFTER THE INVESTIGATION IS CONCLUDED, THE UNIVERSITY  
25 SYSTEM OF MARYLAND DETERMINES THAT THE MISUSE OF THE INDIVIDUAL’S  
26 PERSONAL INFORMATION HAS OCCURRED OR IS LIKELY TO OCCUR, THE  
27 UNIVERSITY SYSTEM OF MARYLAND OR THE NONAFFILIATED THIRD PARTY, IF  
28 AUTHORIZED UNDER A WRITTEN CONTRACT OR AGREEMENT WITH THE UNIVERSITY  
29 SYSTEM OF MARYLAND, SHALL NOTIFY THE INDIVIDUAL OF THE BREACH.

30           (II) UNLESS THE UNIVERSITY SYSTEM OF MARYLAND OR THE  
31 NONAFFILIATED THIRD PARTY KNOWS THAT THE ENCRYPTION KEY HAS BEEN  
32 BROKEN, THE UNIVERSITY SYSTEM OF MARYLAND OR THE NONAFFILIATED THIRD  
33 PARTY IS NOT REQUIRED TO NOTIFY AN INDIVIDUAL UNDER SUBPARAGRAPH (I) OF  
34 THIS PARAGRAPH IF:

1                   **1. THE PERSONAL INFORMATION OF THE INDIVIDUAL**  
2 **WAS SECURED BY ENCRYPTION OR REDACTED; AND**

3                   **2. THE ENCRYPTION KEY HAS NOT BEEN COMPROMISED**  
4 **OR DISCLOSED.**

5                   **(3) EXCEPT AS PROVIDED IN SUBSECTION (D) OF THIS SECTION, THE**  
6 **NOTIFICATION REQUIRED UNDER PARAGRAPH (2) OF THIS SUBSECTION SHALL BE**  
7 **GIVEN AS SOON AS REASONABLY PRACTICABLE AFTER THE UNIVERSITY SYSTEM OF**  
8 **MARYLAND CONDUCTS THE INVESTIGATION REQUIRED UNDER PARAGRAPH (1) OF**  
9 **THIS SUBSECTION.**

10                   **(4) IF, AFTER THE INVESTIGATION REQUIRED UNDER PARAGRAPH (1)**  
11 **OF THIS SUBSECTION IS CONCLUDED, THE UNIVERSITY SYSTEM OF MARYLAND**  
12 **DETERMINES THAT NOTIFICATION UNDER PARAGRAPH (2) OF THIS SUBSECTION IS**  
13 **NOT REQUIRED, THE UNIVERSITY SYSTEM OF MARYLAND SHALL MAINTAIN**  
14 **RECORDS THAT REFLECT ITS DETERMINATION FOR 3 YEARS AFTER THE**  
15 **DETERMINATION IS MADE.**

16                   **(C) (1) A NONAFFILIATED THIRD PARTY THAT MAINTAINS**  
17 **COMPUTERIZED DATA THAT INCLUDES PERSONAL INFORMATION PROVIDED BY THE**  
18 **UNIVERSITY SYSTEM OF MARYLAND SHALL NOTIFY THE UNIVERSITY SYSTEM OF**  
19 **MARYLAND OF A BREACH OF THE SECURITY OF A SYSTEM IF THE UNAUTHORIZED**  
20 **ACQUISITION OF THE INDIVIDUAL'S PERSONAL INFORMATION HAS OCCURRED OR IS**  
21 **LIKELY TO OCCUR.**

22                   **(2) EXCEPT AS PROVIDED IN SUBSECTION (D) OF THIS SECTION, THE**  
23 **NOTIFICATION REQUIRED UNDER PARAGRAPH (1) OF THIS SUBSECTION SHALL BE**  
24 **GIVEN AS SOON AS REASONABLY PRACTICABLE AFTER THE NONAFFILIATED THIRD**  
25 **PARTY DISCOVERS OR IS NOTIFIED OF THE BREACH OF THE SECURITY OF A SYSTEM.**

26                   **(3) A NONAFFILIATED THIRD PARTY THAT IS REQUIRED TO NOTIFY**  
27 **THE UNIVERSITY SYSTEM OF MARYLAND OF A BREACH OF THE SECURITY OF A**  
28 **SYSTEM UNDER PARAGRAPH (1) OF THIS SUBSECTION SHALL SHARE WITH THE**  
29 **UNIVERSITY SYSTEM OF MARYLAND INFORMATION RELATING TO THE BREACH.**

30                   **(D) (1) THE NOTIFICATION REQUIRED UNDER SUBSECTION (B) OF THIS**  
31 **SECTION MAY BE DELAYED:**

32                   **(I) IF A LAW ENFORCEMENT AGENCY DETERMINES THAT THE**  
33 **NOTIFICATION WILL IMPEDE A CRIMINAL INVESTIGATION OR JEOPARDIZE**  
34 **HOMELAND OR NATIONAL SECURITY; OR**

1                   (II) TO DETERMINE THE SCOPE OF THE BREACH OF THE  
2 SECURITY OF A SYSTEM, IDENTIFY THE INDIVIDUALS AFFECTED, OR RESTORE THE  
3 INTEGRITY OF THE SYSTEM.

4                   (2) IF NOTIFICATION IS DELAYED UNDER PARAGRAPH (1)(I) OF THIS  
5 SUBSECTION, NOTIFICATION SHALL BE GIVEN AS SOON AS REASONABLY  
6 PRACTICABLE AFTER THE LAW ENFORCEMENT AGENCY DETERMINES THAT THE  
7 NOTIFICATION WILL NOT IMPEDE A CRIMINAL INVESTIGATION AND WILL NOT  
8 JEOPARDIZE HOMELAND OR NATIONAL SECURITY.

9                   (E) THE NOTIFICATION REQUIRED UNDER SUBSECTION (B) OF THIS  
10 SECTION MAY BE GIVEN:

11                   (1) BY WRITTEN NOTICE SENT TO THE MOST RECENT ADDRESS OF THE  
12 INDIVIDUAL IN THE RECORDS OF THE UNIVERSITY SYSTEM OF MARYLAND;

13                   (2) BY E-MAIL TO THE MOST RECENT E-MAIL ADDRESS OF THE  
14 INDIVIDUAL IN THE RECORDS OF THE UNIVERSITY SYSTEM OF MARYLAND IF:

15                   (I) THE INDIVIDUAL HAS EXPRESSLY CONSENTED TO RECEIVE  
16 ELECTRONIC NOTICE; OR

17                   (II) THE UNIVERSITY SYSTEM OF MARYLAND CONDUCTS ITS  
18 DUTIES PRIMARILY THROUGH INTERNET ACCOUNT TRANSACTIONS OR THE  
19 INTERNET;

20                   (3) BY TELEPHONIC NOTICE, TO THE MOST RECENT TELEPHONE  
21 NUMBER OF THE INDIVIDUAL IN THE RECORDS OF THE UNIVERSITY SYSTEM OF  
22 MARYLAND; OR

23                   (4) BY SUBSTITUTE NOTICE AS PROVIDED IN SUBSECTION (F) OF THIS  
24 SECTION IF:

25                   (I) THE UNIVERSITY SYSTEM OF MARYLAND DEMONSTRATES  
26 THAT THE COST OF PROVIDING NOTICE WOULD EXCEED \$100,000 OR THAT THE  
27 AFFECTED CLASS OF INDIVIDUALS TO BE NOTIFIED EXCEEDS 175,000; OR

28                   (II) THE UNIVERSITY SYSTEM OF MARYLAND DOES NOT HAVE  
29 SUFFICIENT CONTACT INFORMATION TO GIVE NOTICE IN ACCORDANCE WITH ITEM  
30 (1), (2), OR (3) OF THIS SUBSECTION.

31                   (F) SUBSTITUTE NOTICE UNDER SUBSECTION (E)(4) OF THIS SECTION  
32 SHALL CONSIST OF:



1           (1) E-MAILING THE NOTICE TO AN INDIVIDUAL ENTITLED TO  
2 NOTIFICATION UNDER SUBSECTION (B) OF THIS SECTION IF THE UNIVERSITY  
3 SYSTEM OF MARYLAND HAS AN E-MAIL ADDRESS FOR THE INDIVIDUAL TO BE  
4 NOTIFIED;

5           (2) CONSPICUOUS POSTING OF THE NOTICE ON THE WEBSITE OF THE  
6 UNIVERSITY SYSTEM OF MARYLAND IF THE UNIVERSITY SYSTEM OF MARYLAND  
7 MAINTAINS A WEBSITE; AND

8           (3) NOTIFICATION TO APPROPRIATE MEDIA.

9           (G) THE NOTIFICATION REQUIRED UNDER SUBSECTION (B) OF THIS  
10 SECTION SHALL INCLUDE:

11           (1) TO THE EXTENT POSSIBLE, A DESCRIPTION OF THE CATEGORIES  
12 OF INFORMATION THAT WERE, OR ARE REASONABLY BELIEVED TO HAVE BEEN,  
13 ACQUIRED BY AN UNAUTHORIZED PERSON, INCLUDING WHICH OF THE ELEMENTS  
14 OF PERSONAL INFORMATION WERE, OR ARE REASONABLY BELIEVED TO HAVE BEEN,  
15 ACQUIRED;

16           (2) CONTACT INFORMATION FOR THE UNIVERSITY SYSTEM OF  
17 MARYLAND INSTITUTION MAKING THE NOTIFICATION, INCLUDING THE UNIVERSITY  
18 SYSTEM OF MARYLAND INSTITUTION'S ADDRESS, TELEPHONE NUMBER, AND  
19 TOLL-FREE TELEPHONE NUMBER IF ONE IS MAINTAINED;

20           (3) THE TOLL-FREE TELEPHONE NUMBERS AND ADDRESSES FOR THE  
21 MAJOR CONSUMER REPORTING AGENCIES; AND

22           (4) (I) THE TOLL-FREE TELEPHONE NUMBERS, ADDRESSES, AND  
23 WEBSITE ADDRESSES FOR:

24                   1. THE FEDERAL TRADE COMMISSION; AND

25                   2. THE OFFICE OF THE ATTORNEY GENERAL; AND

26           (II) A STATEMENT THAT AN INDIVIDUAL CAN OBTAIN  
27 INFORMATION FROM THESE SOURCES ABOUT STEPS THE INDIVIDUAL CAN TAKE TO  
28 AVOID IDENTITY THEFT.

29           (H) (1) BEFORE GIVING THE NOTIFICATION REQUIRED UNDER  
30 SUBSECTION (B) OF THIS SECTION, THE UNIVERSITY SYSTEM OF MARYLAND SHALL  
31 PROVIDE NOTICE OF A BREACH OF THE SECURITY OF A SYSTEM TO THE OFFICE OF  
32 THE ATTORNEY GENERAL.

1           **(2) IN ADDITION TO THE NOTICE REQUIRED UNDER PARAGRAPH (1)**  
2 **OF THIS SUBSECTION, THE UNIVERSITY SYSTEM OF MARYLAND SHALL PROVIDE**  
3 **NOTICE OF A BREACH OF SECURITY TO THE DEPARTMENT OF INFORMATION**  
4 **TECHNOLOGY.**

5           **(I) A WAIVER OF ANY PROVISION OF THIS SECTION IS CONTRARY TO PUBLIC**  
6 **POLICY AND IS VOID AND UNENFORCEABLE.**

7           **(J) COMPLIANCE WITH THIS SECTION DOES NOT RELIEVE THE UNIVERSITY**  
8 **SYSTEM OF MARYLAND FROM A DUTY TO COMPLY WITH ANY OTHER REQUIREMENTS**  
9 **OF FEDERAL LAW RELATING TO THE PROTECTION AND PRIVACY OF PERSONAL**  
10 **INFORMATION.**

11 **10-13A-06.**

12           **THE PROVISIONS OF THIS SUBTITLE ARE EXCLUSIVE AND SHALL PREEMPT**  
13 **ANY PROVISION OF LOCAL LAW.**

14 **10-13A-07.**

15           **(A) IF THE UNIVERSITY SYSTEM OF MARYLAND IS REQUIRED UNDER §**  
16 **10-13A-05 OF THIS SUBTITLE TO GIVE NOTICE OF A BREACH OF THE SECURITY OF**  
17 **A SYSTEM TO 1,000 OR MORE INDIVIDUALS, THE UNIVERSITY SYSTEM OF**  
18 **MARYLAND ALSO SHALL NOTIFY, WITHOUT UNREASONABLE DELAY, EACH**  
19 **CONSUMER REPORTING AGENCY THAT COMPILES AND MAINTAINS FILES ON**  
20 **CONSUMERS ON A NATIONWIDE BASIS, AS DEFINED BY 15 U.S.C. § 1681A(P), OF THE**  
21 **TIMING, DISTRIBUTION, AND CONTENT OF THE NOTICES.**

22           **(B) THIS SECTION DOES NOT REQUIRE THE INCLUSION OF THE NAMES OR**  
23 **OTHER PERSONAL IDENTIFYING INFORMATION OF RECIPIENTS OF NOTICES OF THE**  
24 **BREACH OF THE SECURITY OF A SYSTEM.**

25 **10-13A-08.**

26           **THE UNIVERSITY SYSTEM OF MARYLAND OR A NONAFFILIATED THIRD PARTY**  
27 **THAT COMPLIES WITH § 501(B) OF THE FEDERAL GRAMM-LEACH-BLILEY ACT, 15**  
28 **U.S.C. § 6801, § 216 OF THE FEDERAL FAIR AND ACCURATE CREDIT TRANSACTIONS**  
29 **ACT, 15 U.S.C. § 1681W DISPOSAL OF RECORDS, THE FEDERAL INTERAGENCY**  
30 **GUIDELINES ESTABLISHING INFORMATION SECURITY STANDARDS, THE FEDERAL**  
31 **INTERAGENCY GUIDANCE ON RESPONSE PROGRAMS FOR UNAUTHORIZED ACCESS**  
32 **TO CUSTOMER INFORMATION AND CUSTOMER NOTICE, AND ANY REVISIONS,**  
33 **ADDITIONS, OR SUBSTITUTIONS OF THOSE ENACTMENTS, SHALL BE DEEMED TO BE**  
34 **IN COMPLIANCE WITH THIS SUBTITLE.**

1 SECTION 3. AND BE IT FURTHER ENACTED, That the Laws of Maryland read  
2 as follows:

3 Article – State Government

4 10–1302.

5 (c) This subtitle does not apply to the Legislative or Judicial Branch of State  
6 [Government.] GOVERNMENT OR the Office of the Attorney General[, or the University  
7 System of Maryland].

8 SECTION 4. AND BE IT FURTHER ENACTED, That Section 2 of this Act shall take  
9 effect October 1, 2019. It shall remain effective for a period of 1 year and 9 months and, at  
10 the end of June 30, 2021, Section 2 of this Act, with no further action required by the  
11 General Assembly, shall be abrogated and of no further force and effect.

12 SECTION 5. AND BE IT FURTHER ENACTED, That Section 3 of this Act shall take  
13 effect July 1, 2021.

14 SECTION ~~2~~ 6. AND BE IT FURTHER ENACTED, That, except as provided in  
15 Sections 4 and 5 of this Act, this Act shall take effect October 1, 2019.

Approved:

\_\_\_\_\_  
Governor.

\_\_\_\_\_  
Speaker of the House of Delegates.

\_\_\_\_\_  
President of the Senate.