Law/Act:	Data Breach Response Requirements	
HRS Citation:	HRS § 487N	
Federal Regulatory Citation:	45 C.F.R. §§ 164.400-414 (2014) (HIPAA); 34 C.F.R. pt. 99 (2014)(FERPA); 16 C.F.R. pts. 313 and 314 (2014) (GLBA).	
Responsible Regulator:	Hawaii Department of Commerce and Consumer Affairs Federal Trade Commission (FACTA, GLBA) Department of Education (FERPA) U.S. Department of Health and Human Services (HIPAA) Federal Trade Commission (FACTA)	
BYU–Hawaii Responsible Officer:	Operations Vice President	
	Updated: Nov. 2022	Updated by: MP
	Version 1.0	Effective date: N/A

I. PURPOSE

Various laws establish information security standards and mandate certain responses (e.g., notification) in the event of personally identifiable information (PII) or other sensitive information. This memo outlines the current requirements and standards applicable to responding to data breaches.

II. HISTORY

In 2016 alone, hundreds of millions of records were stolen from institutions as prominent as the U.S Department of Justice, Yahoo, and Verizon.[1] The increase in electronic recordkeeping and occurrence of data breaches has led lawmakers to legislate data security standards for PII and other sensitive information.[2] Numerous federal statutes and regulations address the privacy rights of individuals, security standards, and breach notification requirements.[3] In addition, the laws of various states require entities that store or process PII to notify the owners of the information in the event of a security breach.[4]

III. APPLICABILITY TO BYU–Hawaii

Like most universities, BYU–Hawaii maintains a large volume of PII and other sensitive information regarding students, faculty, staff, alumni, applicants, customers, and others. Inadvertent disclosure of this information or failure to respond properly to a data breach may violate state law, federal law, and/or industry standards, and may subject the university to adverse publicity, fines, and/or lawsuits.

Generally, BYU–Hawaii is subject in part to Hawaii Revised Statute (HRS) §487 Security Breach of Personal Information and to various federal laws, including the Health Insurance Portability and Accountability Act (HIPAA), the Family Educational Rights and Privacy Act (FERPA), and the Red Flag Rules under the Fair and Accurate Credit Transactions Act (FACTA), and the Gramm-Leach-Bliley Act (GLBA). BYU–Hawaii also has agreed to comply with certain standards, including the Payment Card Industry (PCI) Data Security Standard, and may be required in certain instances to comply with the security standards established by the National Institute of Standards and Technology (NIST). As outlined

[1] *The Biggest Data Breaches in 2016*, IDENTITYFORCE, https://www.identityforce.com/blog/2016-data-breaches (last visited Feb. 22, 2017).
[2] Ashley Smith, *The Changing Global Landscape of Data Protection Laws,* INSIDECOUNSEL, Feb. 19, 2014, *available at* http://www.insidecounsel.com/2014/02/19/the-changing-global-landscape-of-data-protection-l.
[3] *E.g.*, 45 C.F.R. §§ 164.400-414 (2017).
[4] HRS § 487N-2(b)

below, each of these laws and standards include requirements and/or guidelines relevant to BYU's response to data breaches.

IV. REQUIREMENTS

A. Security Breach of Personal Information – HRS

HRS 487N Security Breach of Personal Information[5] includes specific requirements for safeguarding personal information and responding to data breaches applicable to residents of Hawaii.[6] Anyone who maintains data that qualifies as "personal information"[7] and that contains names or data elements that are unencrypted or not otherwise rendered unreadable must comply with this HRS.

Under HRS §487N , [a]ny business that owns or licenses personal information of residents of Hawaii, any business that conducts business in Hawaii that owns or licenses personal information in any form. . . or any government agency that collects personal information for specific government purposes shall provide notice to the affected person that there has been a security breach following discovery or notification of the breach.[8] A breach is defined as means an incident of unauthorized access to and acquisition of unencrypted or unredacted records or data containing personal information where illegal use of the personal information has occurred, or is reasonably likely to occur and that creates a risk of harm to a person.[9]

The notice shall include a description of the following:

1. The incident in general terms;
2. The type of personal information that was subject to the unauthorized access and acquisition;
3. The general acts of the business or government agency to protect the personal information from further unauthorized access;
4. A telephone number that the person may call for further information and assistance, if one exists; and
5. Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.[10]

Notice may be provided in any of the following ways:

a) Written notice to the last available address;
b) Electronic mail notice;
c) Telephone notice;
d) Substitute notice consisting of electronic mail notice, conspicuous posting on the website, notification to major statewide media.[11]

---

[5] *Id.* §487N.
[6] *Id.* §487N-2.
[7] *Id.* §487N-1 defines "personal information" as an individuals' first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social Security number; (2) Driver's license number or Hawaii identification card number; or (3) Account number, credit or debit care number, access code, or password that would permit access to an individual's financial account.
[8] *Id. §*487N-2
[9] *Id.* §487N-1
[10] *Id.* §487N-2-(d) *(1-5)*
[11] *Id.* §487N-2-(e) *(1-4)*

B. Health Insurance Portability and Accountability Act (HIPAA)

HIPAA regulates the disclosure of Protected Health Information (PHI) held by covered entities.[12] Health information includes any information created or received by health care entities, including schools and universities, that relates to past, present or future physical or mental health, the provision of health care, and health care payments of individuals.[13] Covered entities are required to ensure PHI remains confidential and is protected against reasonably anticipated security threats and unlawful disclosures.[14] The university may use any security measures it deems appropriate to comply with HIPAA requirements.[15] This includes administrative, physical, and technical safeguards as well as organizational requirements.[16]

HIPAA requires covered entities, within a certain period after discovery of a breach of PHI, to provide notice of breaches to individuals, the Department of Health and Human Services (HHS), and even the media.[17] A breach is considered to be "discovered" when an entity or any of its workers have knowledge of the breach or would have knowledge of it by exercising reasonable diligence.[18]

1. Notification of Individuals

A covered entity must give adequate notice of the uses and disclosures of protected health information to the individual that the information concerns.[19] If PHI is breached or inappropriately disclosed, the covered entity is required to notify each individual whose PHI has been accessed, acquired, used, or disclosed within 60 days of the breach being discovered.[20] The notification must include, to the extent possible, the following:

1. a brief description of what happened, including the date of the breach and its discovery;
2. a description of the types of unsecured PHI that were involved in the breach;[21]
3. any steps individuals should take to protect themselves from potential harm from the breach;
4. a brief description of what the covered entity involved is doing to investigate the breach, mitigate harm, and protect against further breaches; and
5. contact procedures for individuals to ask questions or learn additional information including a toll-free telephone number, an email address, web site, or postal address.[22]

A written notification must be delivered in plain language to each individual whose PHI has been breached.[23] This written notification must be delivered by first-class mail to the individual's last known

---

[12] 45 C.F.R. § 164.302 (2017).
[13] *Id.* § 160.103.
[14] *Id.* § 164.306(a).
[15] *Id.* § 164.306(b)-(c).
[16] *Id.* §§ 164.308-164.316.
[17] *Id.* pt. 164, subpt. D. If a business associate of a covered entity discovers a breach of unsecured PHI, the business associate must promptly report the breach to the entity without unreasonable delay and no later than sixty days after the breach is discovered. *Id.* § 164.404(b).
[18] *Id.* § 164.404(a)(2).
[19] *Id.* § 164.520(a)(1).
[20] *Id.* § 164.404(a)(1), (b).
[21] This could include full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information involved. *Id.* § 164.404(c)(1)(B).
[22] *Id.* § 164.404(c).
[23] *Id.* § 164.404(c)(2), (d).

address, or by email if the individual has consented to receiving notifications electronically.[24] If the covered entity knows that the individual whose PHI has been breached is deceased, the entity must send written notification via first-class mail to the next of kin or to a personal representative.[25]

If the contact information for the individual is out-of-date or insufficient, the covered entity may deliver a substitute notice.[26] If there is insufficient or our-of-date information for fewer then ten individuals, the substitute notice may be provided by an alternative form of written notice, telephone, or other means.[27] If information is insufficient for ten or more individuals, the substitute notice must be posted conspicuously on the home page of the entity's website for ninety days, or in major print or broadcast media near affected individuals.[28] This notice must include a toll-free phone number that allows individuals to learn whether their PHI was compromised in the breach.[29] A substitute notice does not need to be delivered to a next of kin or representative if a covered entity has insufficient contact information for an individual who is deceased.[30]

If a covered entity decides that a security breach requires urgent notification due to PHI being imminently misused, the entity may provide information to individuals by telephone or other appropriate means in addition to the written notification that is required.[31]

2. Notification to the Secretary of Health and Human Services

If a covered entity discovers a breach of unsecured PHI, the entity must notify the Secretary of the U.S. Department of Health and Human Services (HHS).[32] If a breach involves 500 or more individuals, the covered entity must notify the Secretary of HHS contemporaneously with the individuals affected, except if delayed by law enforcement officials.[33] This notice must be provided no later than sixty days from discovery of the breach and must be submitted electronically via the form provided on the HHS website.[34]

If the breach involves less than 500 individuals, the covered entity must maintain record of the breach and notify the Secretary of HHS no later than sixty days after the end of the calendar year during which the breach occurred.[35] Information about the breach must be reported online using the form descried above.[36]

3. Notification to the Media

If a breach of unsecured PHI involves more than 500 residents of a State or jurisdiction, a covered entity must notify prominent media outlets serving the geographic area within sixty calendar days of the

---

[24] *Id.* § 164.404(d)(1)(i).
[25] *Id.* § 164.404(d)(1)(ii).
[26] *Id.* § 164.404(d)(2).
[27] *Id.* § 164.404(d)(2)(i).
[28] *Id.* § 164.404(d)(2)(ii)(A).
[29] *Id.* § 164.404(d)(2)(ii)(B).
[30] *Id.* § 164.404(d)(2).
[31] *Id.* § 164.404(d)(3).
[32] *Id.* §§ 164.408(a), 160.103.
[33] *Id.* § 164.408(b).
[34] *Id.* § 164.408(b); *see also Submitting Notice of a Breach to the Secretary,* U.S. DEP'T OF HEALTH & HUMAN SERVICES, https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html (last visited Feb. 22, 2017) ["HHS Breach Notice"] (providing instructions on when and how to submit breach notifications to HHS).
[35] 45 C.F.R. § 164.408 (2017).
[36] HHS Breach Notice, *supra* note 40.

breach's discovery, unless the notification is delayed due to needs of law enforcement officials.[37] This notification must include all information necessary to notify the individual described above.[38]

C. Family Educational Rights and Privacy Act of 1974 (FERPA)

The purpose of FERPA is to protect parent and student privacy and to limit disclosures of personal information without consent.[39] FERPA applies to universities that receive funds under Title IV of the Higher Education Act of 1965, such as Pell Grant and Guaranteed Student Loan Program funds.[40] Under FERPA, the university must allow students to inspect and review their education records, have an opportunity to amend their education records, and control disclosures of their education records.[41]

FERPA itself does not specifically mandate that institutions notify individuals whose educational records have been breached. However, the U.S. Department of Education (DOE) strongly encourages institutions to safeguard student information and has published several best practices for safeguarding student privacy, including those relevant to responding to data breaches.[42] For example, the DOE's Privacy Technical Assistance Center has prepared a Data Breach Response Training Kit, which provides an interactive exercise aimed at improving institutions' data breach response procedures.[43]

D. Fair and Accurate Credit Transactions Act of 2023 (FACTA) – the Red Flag Rules

The Fair and Accurate Credit Transactions Act of 2023 (FACTA) is intended to ensure the confidentiality, accuracy, relevancy, and proper use of credit information by consumer reporting agencies as well as to ensure the detection, prevention, and mitigation of identity theft.[44] FACTA requires creditors[45] and financial institutions[46] that handle covered accounts[47] to establish and maintain an identity theft program that identifies, assesses, and responds to red flags.[48] Red flags are patterns, practices, or specific activities that indicate the possibility of identity theft.[49] Among other things, a financial

---

[37] *Id.* §§ 164.406, 164.412.
[38] *Id.* § 164.406(c).
[39] 34 C.F.R. § 99.2 (2017).
[40] *Id.* § 99.1(a), (c)(2).
[41] 20 U.S.C. § 1232g(a)(1)(A), (a)(2), (b)(1) (2017).
[42] U.S. Dep't of Educ., *Safeguarding Student* Privacy, https://www2.ed.gov/policy/gen/guid/fpco/ferpa/safeguarding-student-privacy.pdf (last visited Feb. 22, 2017).
[43] U.S. Dep't of Educ., Privacy Technical Assistance Center, *PTAC Toolkit*, http://ptac.ed.gov/toolkit (last visited Feb. 22, 2017).
[44] 15 U.S.C. § 1681(b) (2017); *see* 16 C.F.R. § 681.1(d)(1) (2017) (requiring identity theft programs).
[45] Creditors are (a) persons who obtain or use consumer reports or who furnish information to consumer reporting agencies in connection with credit transactions; (b) persons who advance funds to or on behalf of a person, based on that person's obligation to repay the funds; or (c) persons who regularly engage in extending, renewing, or continuing credit. 16 C.F.R. § 681.1(b)(5) (2017); 15 U.S.C. §§ 1681m(e)(4), 1691a(e) (2017).
[46] Financial institutions include banks, credit unions, or other persons that hold deposits or accounts on which the depositor or account holder may make withdrawals. 15 U.S.C. § 1681a(t) (2017).
[47] "Account means a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household or business purposes." Accounts include an extension of credit and a deposit account. 16 C.F.R. § 681.1(b)(1) (2017).
[48] *Id.* § 681.1(a); *see id.* § 681.1(d) (requiring financial institutions or creditors that offer or maintain covered accounts to create and apply Identity Theft Programs).
[49] *Id.* § 681.1(b)(9) (defining "red flag").

institution's identity theft program must "respond appropriately to any red flags that are detected … to prevent and mitigate identity theft."[50]

The regulations implementing FACTA include a list of interagency "guidelines" that an institution "must consider" and, if "appropriate", must include as part of its identity theft program.[51] According to these guidelines, in identifying red flags, institutions should consider the types of accounts if offers or maintains, the methods it provides to open and access those accounts, and its previous experiences with identity theft.[52] Institutions also should incorporate relevant red flags from the following:

1. incidents of identity theft the institution has experienced;
2. possible methods of identity theft that the institution has identified as an identity theft risk;
3. applicable supervisory guidance;
4. alerts and other warnings from consumer reporting agencies and other service providers;
5. the presentation of suspicious documents or personally identifying information; and,
6. notifications from customers, victims of identity theft, and law enforcement agencies.

Under the same guidelines, an institution's "policies and procedures should provide for appropriate responses to the Red Flags," which "are commensurate with the degree of risk posed."[53] "In determining an appropriate response to [red flags, an institution] should consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a customer's account records."[54] Appropriate responses to red flags may include, among other possible steps, monitoring covered accounts; contacting consumers; notifying law enforcement agencies; changing passwords, security codes, or other security devices; not opening a new covered account; or closing existing covered accounts.[55] Institutions also may determine that "no response is warranted under the particular circumstances."[56]

E. Gramm-Leach-Bliley Act (GLBA)

Universities that offer financial products or services (e.g., institutional student loans and other financial aid programs) are considered covered financial institutions regulated by the GLBA.[57] Under GLBA regulations implemented by the Federal Trade Commission (FTC), financial institutions must safeguard and respect the privacy of consumer financial information.[58] GLBA regulations provide that universities that are compliant with FERPA automatically meet the GLBA privacy rule but still must meet the separate GLBA safeguards rule.[59]

While no specific security breach notification requirements currently exist under the GLBA or its regulations, the law does require entities to develop, implement, and maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information. In developing these safeguards, the FTC has indicated that institutions "should

[50] *Id.* § 681.1(d)(2)(iii).
[51] *Id.* § 681.1(f) and app. A.
[52] *Id.* pt. 681, app. A, (II)(a).
[53] *Id.* pt. 681, app. A, (IV).
[54] *Id.*
[55] *Id.* pt. 681, app. A, (IV)(a)-(i).
[56] *Id.*
[57] Privacy of Consumer Financial Information, 65 Fed. Reg. 33,646, 33,648 (May 24, 2000) (codified at 16 C.F.R. pt. 313).
[58] 15 U.S.C. § 6801.
[59] 16 C.F.R. § 313.1(b) (2017) (FERPA compliance meets GLBA privacy rule); *id.* pt. 314 (separate safeguards rule).

consider" a number of best practices, including taking the following specific steps to diagnose and respond to security incidents[60]:

1. "take immediate action to secure any information that has or may have been compromised";
2. "preserve and review files or programs that may reveal how the breach occurred";
3. "if feasible and appropriate, bring in security professionals to help assess the breach";
4. "notify consumers if their personal information is subject to a breach that poses a significant risk of identity theft or related harm";
5. "notify law enforcement if the breach may involve criminal activity or there is evidence that the breach has resulted in identity theft or related harm"; and
6. "notify the credit bureaus and other businesses that may be affected by the breach"

The FTC also has published a *Data Breach Response Guide for Business*, which contains additional recommendations on how to respond to a data breach.[61]

F. Additional Security Standards Relevant to Data Breaches

1. *Payment Card Industry Data Security Standard*

The Payment Card Industry Data Security Standard (PCI Standard) was created to develop streamlined data security measures that could be implemented globally to enhance payment cardholder data security.[62] The PCI Standard establishes minimum requirements for protecting account data.[63] Merchants are encouraged, but not required, to comply with the PCI Standard because it improves a company's reputation and makes a company more dependable due to its secure system.[64] Additionally, violations may result in credit card company fines being passed on to vendors.

To comply with the PCI Standard, a merchant must "establish, publish, maintain, and disseminate a security policy."[65] In doing so, the merchant must create a risk-assessment process that identifies critical assets, threats, and provides risk-assessment results.[66] Among other requirements, merchants must review logs and security events on a daily basis, and must maintain logs for at least a year, while making the most recent there months of logs *immediately* available for analysis in the event of a security breach.[67]

---

[60] Fed. Trade Comm'n, *Financial Institutions and Customer Information: Complying with the Safeguards Rule*, https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying (last visited February 22, 2017).

[61] *Data Breach Response, A Guide for Business*, Fed. Trade Comm'n, https://www.ftc.gov/system/files/documents/plain-language/pdf-0154_data-breach-response-guide-for-business.pdf (last visited Feb. 22, 2017).

[62] *Payment Card Industry (PCI) Data Security Standard*: *Requirements and Security Assessment Procedures,* PCI SECURITY STANDARDS COUNCIL 5 (Apr. 2016), https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf [hereinafter *PCI Standard*].

[63] *Id.* at 5 (noting that other methods should be put in place to strengthen the PCI standards).

[64] *Why Security Matters?*, PCI SECURITY STANDARDS COUNCIL, https://www.pcisecuritystandards.org/pci_security/why_security_matters (last visited Feb. 22, 2017).

[65] *Id.* § 12.1, at 105.

[66] *Id.* § 12.2, at 105. The risk assessment needs to be performed annually, as well as after significant changes to the environment of the company. *Id.*

[67] *Id.* § 10.6 to 10.7 at 92-94.

A merchant also must have and implement an incident response plan and be prepared to responds immediately to a system breach.[68] The incident response plan must address the following, at a minimum[69]:

1. roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum;
2. specific incident response procedures;
3. business recovery and continuity procedures;
4. data backup processes;
5. analysis of legal requirements for reporting compromises;
6. coverage and responses of all critical system components; and
7. reference or inclusion of incident response procedures from the payment brands.

Merchants also must review and test each of these elements of its incident response plan at least annually.[70]

2. *National Institute of Standards and Technology (NIST) Standard*

The National Institute of Standards and Technology (NIST), part of the U.S. Department of Commerce, has developed its own information security standards in NIST Special Publication 800-171 (NIST Standard).[71] The NIST Standard contains recommended federal data security requirements for what is known as "controlled unclassified information" –generally any non-public information that is not considered classified.[72] The U.S. Department of Education "strongly encourages" institutions of higher education to comply with the NIST Standard.[73] Also, certain federal contractors who enter into agreement with the U.S. Department of Defense are required to comply with the NIST standard by no later than December 31, 2017.[74]

The NIST standard includes specific requirements that fall within various data security categories, one of which is incident response. To comply with the incident response requirements of the NIST standard, organizations must do the following[75]:

1. Establish an operational incident-handling capability for information systems, which includes adequate preparation, detection, analysis, containment, recovery, and user response activities;
2. Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization; and
3. Test the organizational incident response capability.

---

[68] *Id.* § 12.10, at 113.
[69] *Id.* § 12.10.1, at 113.
[70] *Id.* § 12.10.2, at 113.
[71] NIST, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf (last visited Feb. 22, 2017) ["NIST"].
[72] *Id.*
[73] Ted Mitchell, Undersecretary, U.S. Department of Education, *Dear Colleague Letter: Protecting Student Information* (July 1, 2016).
[74] 48 C.F.R. § 252.204-7012(b)(2)(ii)(A) (2017).
[75] NIST, *supra* note 77 § 3.6.

V. COMPLIANCE CALENDAR

Under Hawaii law, the university must conduct a prompt investigation upon becoming aware of a breach of system security and must notify affected Hawaii residents of security breaches immediately following discovery of the breach, consistent with the legitimate needs of law enforcement.[76]

Under HIPAA, no later than 60 calendar days after a breach of PHI is discovered, the university must provide notification to each individual whose information has been compromised and, if the breach involves more than 500 people, to the Secretary of HHS and the media.[77] If the breach involves 500 people or less, the university must notify the Secretary of HHS within 60 days after the end of the calendar year in which the breach occurred.

VI. STAYING UP-TO-DATE

The following websites provide valuable information regarding this law and its applicability.

DOCUMENT/REFERENCE	DESCRIPTION
Data Breach Response, A Guide for Business	The Federal Trade Commission's data breach response guide.
Security Breach Notification Laws	The National Conference of State Legislatures' list of state laws regarding security breach notification.
HHS Information on Breach Notification Rule	The Department of Health and Human Service's website with information on the requirements that apply to breach of PHI.
Data Breach Responses, A Guide for Business	The Federal Trade Commission's data breach response guide.
PTAC Data Security Checklist	The Department of Education's Privacy Technical Assistance Center's data security checklist

[76] HRS § 487N-2(b)
[77] 45 C.F.R. § 164.404(b) (2017).