Disclosure or Exposure of Personal Information

Office of the Chief Information Officer

Applies to: Faculty, Staff, and Students; Academic and administrative units; affiliated entities; agents and contractors handling personal information on the university's behalf.

POLICY

Issued: January 10, 2007
Revised: April 28, 2010

Ohio law set forth in Ohio Revised Code §1347 established requirements for notification of Ohio residents in the event that personal information is disclosed or reasonably believed to be disclosed to unauthorized persons through a system security breach. Specific requirements vary depending on the size and certainty of the disclosure. The university intends to fully comply with the statute and statutory time lines, and will also take certain steps beyond those required by law. This policy will help to ensure protection of the specified personal information and responsive notification.

Definitions

Term	Definition
Personal information	An individual's name in combination with: the individual's Social Security number; driver's license number or state identification card number; or financial account number or credit or debit card number with security codes or passwords (ORC §1347).
Unauthorized person	Any person who does not require access to personal information in the course of university employment or to perform duties or meet needs in support of the university mission. A person who receives personal information in response to an Ohio Public Records Law request is not an unauthorized person (ORC §1347).

Policy Details

I. Personal Information.

A. For the purpose of compliance with Ohio Revised Code §1347 and this policy, personal information does not include private information collected pursuant to university research or healthcare activities, absent such information being linked to an individual's Social Security number; driver's license number or state identification card number; or account number or credit or debit card number with security codes or passwords. Notification of university patients or research subjects following disclosure or exposure of private patient care or research-related information will be made in accordance with university HIPAA Privacy or Human Research Protection Program (IRB) policies. In cases where a patient or research subject's private information that is linked to personal information as defined in this policy has been inappropriately disclosed or exposed, the HIPAA Privacy Officers or IRB Institutional Official shall coordinate the university's response with the Office of the CIO's Chief Information Security Officer and the University Response Team.

B. For the purpose of compliance with Ohio Revised Code §1347 and this policy, personal information that is encrypted, redacted, or effectively obscured will not be considered to have been disclosed or exposed.

II. University units operating, maintaining, and using systems containing personal information must effectively control access to those systems to protect against disclosure or exposure of personal information to unauthorized persons.

III. Costs of remediation and notification efforts will be born by the university unit or units responsible for the disclosure or exposure.

IV. The Office of the CIO's Chief Information Security Officer will develop and publish guidelines as needed to implement this policy.

PROCEDURE

Issued: January 10, 2007
Revised: April 28, 2010

I. Notification of affected parties

A. Notwithstanding the Ohio Revised Code §1347 requirement for notification of Ohio residents, the university will make a best attempt to notify all persons whose information was disclosed or exposed regardless of state of residence.

B. The university may choose to make notifications relative to an exposure or disclosure incident that does not trigger Ohio Revised Code §1347 notification requirements.

C. Any proven or suspected disclosure or exposure of personal information in the custody of the university and stored in a computer, system, or data network resource must be immediately reported to the Office of the CIO's Chief Information Security Officer via e-mail to **Security@osu.edu**. CIO security staff and the university unit responsible for the computer, system, or resource will immediately block any further unauthorized access to the personal data.

D. The Office of the CIO and University Communications, in collaboration with the Office of Legal Affairs, will develop template individual and public notification letters and announcements. With the assistance of the university response team, the templates will be tailored by the university unit responsible for a security lapse causing the disclosure or exposure in response to specific incidents.

E. Any individual or public notifications stemming from a specific incident will be issued in the name of the university data trustee, as defined in the Policy on Institutional Data, responsible for the category of disclosed or exposed data in conjunction with an appropriate signatory from the university unit responsible for the security lapse causing the disclosure or exposure.

II. University Response Team.

A. The Office of the CIO's Chief Information Security Officer will notify the CIO and any affected university unit's higher management of potential disclosure or exposure incidents, convene and chair the University Response Team for each potential disclosure or exposure incident under this policy, and manage the overall university macro communications response to each incident.

B. The University Response Team for each computer or network-related disclosure or exposure incident will include representatives from the Office of University Communications; the Office of Legal Affairs; the University Risk Management Coordinator; the university unit responsible for the category of data disclosed or exposed (e.g., the University Registrar for student data); the Police division of the OSU Department of Public Safety, and any university unit responsible for a security lapse causing the disclosure or exposure. Additional university personnel appropriate to a specific incident may be added as necessary.

C. The University Response Team for each computer or network-related potential disclosure or exposure incident will be responsible for determining whether or not an actual disclosure or exposure has taken place; whether or not Ohio Revised Code §1347 notification requirements have been triggered; and which

individuals, government agencies or political subdivisions, news organizations, and commercial or nonprofit entities should be notified either to comply with Ohio Revised Code §1347 or to serve the best interests of the university.

III. Enforcement.

A. The Office of the CIO's Chief Information Security Officer will notify the CIO, other university administration as appropriate, and a violating unit's higher management of any violation of this policy with recommendations for corrective measures.

B. In a perceived emergency situation, Office of the CIO security staff or other university technical staff may take immediate steps to secure personal data, ensure the integrity of the university data network and systems, or protect the university from liability. Steps taken may include denial of access to OSUNet and/or Internet access.

C. All decisions, notifications, or measures taken under this policy may be appealed to the Office of the CIO. Appeals should be submitted by e-mail to ITPolicy@osu.edu.

Responsibilities

Position or Office	Responsibilities
Office of the Chief Information Officer (CIO), Chief Information Security Officer	1. Lead the development of individual and public notification letters and announcements. 2. Notify the CIO and management of potential disclosure or exposure incidents. 3. Convene and chair University Response Team. 4. Coordinate university communications for each incident. 5. Notify the CIO, university leadership and violating unit's management of policy violations. 6. Recommend corrective measures.
University Communications	1. Collaborate on the development of individual and public notification letters and announcements. 2. Serve on University Response Team.
Legal Affairs	1. Collaborate on the development of individual and public notification letters and announcements. 2. Serve on University Response Team.
University Risk Management Coordinator	1. Serve on University Response Team.
University Police	1. Serve on University Response Team.
Unit responsible for security lapse	1. Notify the director of information security immediately of any proven or suspected disclosure or exposure of personal information. 2. Serve on University Response Team. 3. Bear the costs of remediation and notification.
University Response Team	1. Determine if an actual disclosure or exposure has occurred. 2. Determine if ORC §1347 notification requirements have been triggered. 3. Determine who needs to be notified to comply with ORC §1347 and to serve the university's interests.
Individuals who suspect or believe a disclosure or exposure has occurred	1. Notify the director of information security immediately of any proven or suspected disclosure or exposure of personal information.

Disclosure or Exposure of Personal Information

Office of the Chief Information Officer

Applies to: Faculty, Staff, and Students; Academic and administrative units; affiliated entities; agents and contractors handling personal information on the university's behalf.

Technical staff	1. In perceived emergency situations: A. Take immediate steps to secure personal data B. Ensure integrity of university data network and systems C. Protect the university from liability.

Resources

Ohio Revised Code ORC §1347 - http://codes.ohio.gov/orc/1347
Policy on Institutional Data - http://cio.osu.edu/policies/institutional_data/
Identity Theft Red Flags Policy 5.16 - http://busfin.osu.edu/FileStore/516_IdentityTheftRedFlags.pdf

Contacts

Subject	Office	Telephone	E-mail/URL
Policy questions	Office of the CIO Associate Director, Information Technology Policy and Guidelines	614-292-9600	ITpolicy@osu.edu
HIPAA privacy	OSU Health System, Associate Director, Medical Information Management	614-293-4477	Jennifer.Cironi@osumc.edu
Human research protection program	Office of Responsible Research Practices	614-292-1840	Neidig.1@osu.edu
Report suspected incident	Office of the CIO Chief Information Security Officer		Security@osu.edu

History

Issued: January 10, 2007 (Interim)
Revised: April 28, 2010
Edited: May 31, 2012 (updated title)