

Does HIPAA¹ Apply to Our Department?

The Health Insurance Portability and Accountability Act (HIPAA) places significant privacy and security requirements on health care practitioners and researchers that handle individually identifiable health information. If the data in your unit or department is covered by HIPAA, you will need to take additional steps in your risk analysis and response.

PHI and ePHI

ePHI stands for Electronic Protected Health Information. It is any protected health information (PHI) that is created, stored, transmitted, or received electronically. Protected Health Information (PHI) under HIPAA means any information that identifies an individual and relates to at least one of the following:

- The individual's past, present or future physical or mental health.
- The provision of health care to the individual.
- The past, present or future payment for health care.

Information is deemed to identify an individual if it includes either the individual's name or any other information that could enable someone to determine the individual's identity or make them easily traceable.

Data or information is “individually identifiable” if they include any of the 18 types of identifiers, listed below, for an individual or for the individual's employer or family member, or if the provider or researcher is aware that the information could be used, either alone or in combination with other information, to identify an individual.

Does your department or unit create, store, transmit or receive medical information that is combined in any way with one or more of the following identifiers? If the answer is “yes,” then HIPAA may apply to your department and you should immediately contact the IT Security Office and or the Privacy Office for further discussion.

The identifiers include the following (alone or in any combination) including:

- Names
- All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census the geographic unit formed by combining all zip codes with the same three initial digits contains less than 20,000 people
- All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except

¹ Health Insurance Portability and Accountability Act

that such ages and elements may be aggregated into a single category of age 90 or older

- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code that is derived from or related to information about the individual

Does GLBA² Apply to Our Department?

Does your department provide financial services that place you under the security provisions of the federal Financial Services Modernization Act, (also known as the Gramm-Leach-Bliley Act of 1999), which includes regulations to protect consumers' personal financial information? GLBA regulates the disclosure of non-public personal information by financial institutions. Institutions of higher education are covered by the law's definition of "financial institutions" as they participate in financial activities, (e.g. offering Federal Perkins Loans).

- Do you collect personal financial information pursuant to issuing credit, including credit cards? (Accepting credit cards does not make you subject to GLBA, but it may require other handling procedures, see PCI).
- Do you collect personal financial information pursuant to granting loans (student or otherwise)?
- Do you collect payments on which interest is paid? (Deferred payment plans that do not charge interest do not apply.)
- Do you broker investments or mortgages?
- Do you provide financial advice for a fee?
- Do you collect personal financial information pursuant to any other "financial product or service"? (Think about the services banks, brokerages and insurance companies provide.)
- Have you negotiated a contract with a financial service provider or do you plan to in the future?

GLBA applies both to paper and electronic information handling, privacy and security.

Note: HIPAA standards are more comprehensive than those of GLBA; all the practices required by GLBA are also required by HIPAA. Additionally the FERPA standards and practices will overlap for privacy, but not for security purposes regarding GLBA.

² Gramm-Leach-Bliley Act

Does FERPA³ Apply to Our Department?

The Family Educational Rights and Privacy Act (FERPA) provides higher education students the right to have access to their education records, the right to seek to have the records amended, and the right to have some control over the disclosure of personally identifiable information from the education records.. More information on the University's FERPA-related policies are found at www.privacy.ku.edu/student_records/ and at www.vpss.ku.edu/records.shtml.

The University may disclose personally-identifiable information designated as Directory Information from a student's education records without prior consent, unless the student informs the Office of the University Registrar in writing that directory information should not be released without written consent. This certification does not preclude the verification of degrees awarded. Directory information at KU is defined as:

- Student name
- Home and school addresses, telephone numbers, e-mail address
- Year of birth
- Country of citizenship
- Major(s)
- School of enrollment
- Full or part-time status
- Year in school
- Participation in officially-recognized activities and sports
- Dates of attendance
- Degrees, honors, scholarships, and awards received
- Most recent previous educational institution attended
- Names of parents or guardians
- Weight and height of members of athletic teams.

All other student information maintained by the University and pertaining to a student that is not specifically listed, including but not limited to grades, courses, days and times of course meetings, withdrawals, suspension, and month and day of birth, cannot be disclosed without the student's permission. Such information needs to be protected not only from external release, but also protected from access by those within the University who do not have an authorized, job-related need to see it.

³ Family Educational Rights and Privacy Act

Does PCI⁴ Apply to Our Department?

The Payment Card Industry PCI Data Security Standard places stringent requirements on the storage, processing, and transmission of data elements⁵ found on payment cards⁶. The standards were developed by a group of companies including American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International. The PCI standards include requirements for security management, policies, procedures, network architecture, software design, and other protective measures. Organizations wishing to accept payment cards (aka credit or debit cards) must adhere to these regulations. Failure to meet the requirements as set forth by PCI standards will result in suspension of electronic payment capability. Fines may also be imposed by the affected credit card company. These fines may start at \$50,000 for the first violation and increase with each subsequent violation.

Does your department do any one or more of the following, including:

- Accept credit or debit cards for face-to-face (in-person) sales?
- Accept credit or debit cards for e-commerce sales (over the internet)?
- Accept credit or debit card for fax transmission or phone transmission sales?
- Store, process, and/or transmit credit or debit card information in any form (paper or electronic) that relates to or contains the Primary Account Number information?

If you can answer “yes” to any of these questions, the regulations of the PCI Data Security Standard apply to your department. Any merchant who stores cardholder data on any computer that is accessible from the internet is considered “vulnerable to compromise” and must establish appropriate internal and external controls to protect cardholder data from exposure.

⁴ Payment Card Industry

⁵ Data elements include: Primary Account Number (PAN), cardholder name, service code, expiration date, CVC2/CVV2/CID, and PIN/PIN block

⁶ Examples of payment cards include but are not limited to credit cards, debit cards, charge cards, and smart cards.