**Course: Advance Bio Informatics**

**Module Title: HIPAA eHealth Privacy**

**Module No: 146**

HIPAA is the federal Health Insurance Portability and Accountability Act of 1996. The primary goal of the law is to make it easier for people to keep health insurance, protect the confidentiality and security of healthcare information and help the healthcare industry control administrative costs.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA; Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996) was enacted by the United States Congress and signed by President Bill Clinton in 1996.

HIPAA has Privacy rights and Health related companies including providers, government agencies on how to handle PHI

**HIPAA Duties**

* Extends privacy and security coverage to business associates
* Establishes breach notification requirements
* Maximum penalty amount of $1.5 million

It has been known as the Kennedy–Kassebaum Act or Kassebaum-Kennedy Act after two of its leading sponsors. Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs. Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers.

**Title I: Health Care Access, Portability, and Renewability**

Title I of HIPAA regulates the availability and breadth of group health plans and certain individual health insurance policies. It amended the Employee Retirement Income Security Act, the Public Health Service Act, and the Internal Revenue Code.

Title I require the coverage of and also limit restrictions that a group health plan can place on benefits for preexisting conditions. Group health plans may refuse to provide benefits relating to preexisting conditions for a period of 12 months after enrollment in the plan or 18 months in the case of late enrollment. Title I allows individuals to reduce the exclusion period by the amount of time that they had "creditable coverage" prior to enrolling in the plan and after any "significant breaks" in coverage. "Creditable coverage" is defined quite broadly and includes nearly all group and individual health plans, Medicare, and Medicaid. A "significant break" in coverage is defined as any 63 day period without any creditable coverage.

Title I also requires insurers to issue policies without exclusion to those leaving group health plans with creditable coverage (see above) exceeding 18 months, and renew individual policies for as long as they are offered or provide alternatives to discontinued plans for as long as the insurer stays in the market without exclusion regardless of health condition. Some health care plans are exempted from Title I requirements, such as long-term health plans and limited-scope plans such as dental or vision plans that are offered separately from the general health plan. However, if such benefits are part of the general health plan, then HIPAA still applies to such benefits. For example, if the new plan offers dental benefits, then it must count creditable continuous coverage under the old health plan towards any of its exclusion periods for dental benefits.

An alternate method of calculating creditable continuous coverage is available to the health plan under Title I. That is, 5 categories of health coverage can be considered separately, including dental and vision coverage. Anything not under those 5 categories must use the general calculation (e.g., the beneficiary may be counted with 18 months of general coverage, but only 6 months of dental coverage, because the beneficiary did not have a general health plan that covered dental until 6 months prior to the application date). Since limited-coverage plans are exempt from HIPAA requirements, the odd case exists in which the applicant to a general group health plan cannot obtain certificates of creditable continuous coverage for independent limited-scope plans such as dental to apply towards exclusion periods of the new plan that does include those coverages.

Hidden exclusion periods are not valid under Title I (e.g., "The accident, to be covered, must have occurred while the beneficiary was covered under this exact same health insurance contract"). Such clauses must not be acted upon by the health plan and also must be re-written so that they comply with HIPAA.

**Title II: Preventing Health Care Fraud and Abuse; Administrative Simplification; Medical Liability Reform**

Title II of HIPAA defines policies, procedures and guidelines for maintaining the privacy and security of individually identifiable health information as well as outlining numerous offenses relating to health care and sets civil and criminal penalties for violations. It also creates several programs to control fraud and abuse within the health care system. However, the most significant provisions of Title II are its Administrative Simplification rules. Title II requires the Department of Health and Human Services (HHS) to draft rules aimed at increasing the efficiency of the health care system by creating standards for the use and dissemination of health care information.

These rules apply to "covered entities" as defined by HIPAA and the HHS. Covered entities include health plans, health care clearinghouses, such as billing services and community health information systems, and health care providers that transmit health care data in a way that is regulated by HIPAA. Per the requirements of Title II, the HHS has promulgated five rules regarding Administrative Simplification: the Privacy Rule, the Transactions and Code Sets Rule, the Security Rule, the Unique Identifiers Rule, and the Enforcement Rule.

**Protected health information (PHI)**

Protected health information (PHI) is any information about health status, provision of health care, or payment for health care that can be linked to a specific individual. This is interpreted rather broadly[dubious – discuss] and includes any part of a patient's medical record or payment history.

**Hierarchy of PHI**

* The Patient
* Patient Representative
* Spouse- not judiciary separated
* Adult Children
* Parents (if available)
* Siblings

PHI is often sought out in datasets for de-identification before researchers share the dataset publicly. When researchers remove PHI from a dataset they do so in an attempt to preserve privacy for research participants.

**United States**: Under the US Health Insurance Portability and Accountability Act (HIPAA), PHI that is linked based on the following list of 18 identifiers must be treated with special care:

**Names**

All geographical identifiers smaller than a state, 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 more than 20,000 people; and the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000

Dates (other than year) directly related to an individual

Phone numbers

Fax numbers

Email addresses

Social Security numbers

Medical record numbers

Health insurance beneficiary numbers

Account numbers

Certificate/license numbers

Vehicle identifiers and serial numbers, including license plate numbers;

Device identifiers and serial numbers;

Web Uniform Resource Locators (URLs)

Internet Protocol (IP) address numbers

Biometric identifiers, including finger, retinal and voice prints

Full face photographic images and any comparable images

Any other unique identifying number, characteristic, or code except the unique code assigned by the investigator to code the data

**HIPAA privacy rules and PHI**

Individual data must be protected from

* intentional or
* unintentional disclosure
* except for legitimate medical or business reasons
* Participation status in a government system
* Hospital admittance & discharge dates
* Insurance coverage or enrolment/ disenrollment