

Confidentiality of Health Care Information

Martha Dye-Whealan
R.Ph., J.D.

1

Objectives

- Understand HIPAA and applicability in pharmacy practice
- Understand WA Uniform Health Care Act; STD/HIV/AIDS Information Act and applicability in pharmacy practice
- Pursuant to above statutes, recognize situations where patient specific information may be disclosed without patient consent versus situations when consent is required.

2

Sources of Confidentiality Duty:

- State and federal law
- Professional ethical standards
- Accrediting organizational standards (e.g. JCAHO)
- Institutional policies

3

Major Statutes Regulating Health Care Information

- Health Insurance Portability and Accountability Act of 1996 (45 CFR 142, 160, 164)
- Uniform Health Care Information Act (RCW 70.02)
- STD/HIV/AIDS Information (RCW 70.24.105)

4

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Legislation enacted by Congress in 1996. Reach of statute includes portability and continuity of health care coverage, simplification of administration of health insurance, and other health care issues. Authorized Department of Health and Human Services (HHS) to issue regulations governing confidentiality of certain types of health care information if Congress itself did not do so within three years of Act.

5

Legislative History of HIPAA (cont'd):

- Because Congress failed to enact privacy protections in the time specified, regulations were developed by HHS. Body of regulations was entitled the "Privacy Rule" [45 CFR 160 and 164 A) and E)].
- Final version of Privacy Rule published August 14, 2002. Effective for most health care entities: April 14, 2003.

6

HIPAA Info on the Web

- Fact sheet: www.privacyrights.org/fs/fs8-med.htm
- Advisory, Phoenix Health Systems: www.hipaadvisory.com/regs/HIPAA_primer.htm
- UWMC HIPAA Program Office: [know1.mcis.washington.edu/proj_hipaa/?](http://know1.mcis.washington.edu/proj_hipaa/)
 - Access via My UW

7

Who is subject to the Privacy Rule under HIPAA?

- "Covered entities":
 - Health plans
 - Health care providers (either institutional providers like hospitals, or individual practitioners)
 - Health care clearinghouses

8

What is Protected Health Information (PHI) under the Privacy Rule?

“Individually identifiable health information” that is transmitted or maintained in any medium, and is held by covered entity or business associate.

9

What is PHI (cont'd)?

- “Individually Identifiable Health Information” is information that is created or received by covered entity or employer that relates to the:
 - Past, present, or future physical or mental health/condition; or
 - Provision of health care to an individual; or
 - Past, present or future payment of health care; AND
 - Identifies the individual or can be used to identify the individual

10

General Principle for Uses and Disclosures of PHI:

- A covered entity may not use or disclose PHI, except either:
 - As the Privacy Rules permits or requires;
 - As the individual who is the subject of the information authorizes in writing.
- “Disclosure”: a release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

11

Required Disclosures:

- A covered entity **MUST** disclose PHI in only two situations:
 - To individuals (or their personal representatives) specifically when they request access to, or an accounting of the disclosures of, their PHI; and
 - To HHS when it is undertaking a compliance investigation or review or enforcement action.

12

Permitted Disclosures:

- To the Individual
- For the Purposes of Treatment, Payment, and Health Care Operations
 - “Treatment”: Provision, coordination and management of health care and related services for an individual by one or more health care providers, including patient consultations and referrals. (Usual situation where pharmacists disclose information).

13

Permitted Disclosures (cont'd):

- For the Purposes of Treatment, Payment, and Health Care Operations (cont'd)
 - “Payment” refers to activities of a health care plan to obtain premiums, determine or fulfill responsibilities for coverage or provision of benefits, and furnish or obtain reimbursement for an individual.
 - Also refers to activities of a health care provider to obtain payment or be reimbursed for provision of health care to an individual (RPh to insurance plans for drug coverage).

14

Permitted Disclosures (cont'd):

- For the Purposes of Treatment, Payment, and Health Care Operations (cont'd)
 - “Health care operations” include:
 - QA activities, including case management and care coordination
 - Competency assurance activities
 - Conducting or arranging for medical reviews, audits, or legal services
 - Specified insurance functions
 - Business planning, development, management and administration

15

Permitted Disclosures (cont'd):

- Uses and Disclosures with Opportunity to Agree or Object
 - Informal permission may be obtained from individual by asking the individual outright, or by circumstances that clearly give the individual the opportunity to agree or object.
 - E.g. facility (hospital) directories: name, general condition, location in provider’s facility.

16

Permitted Disclosures (cont'd):

- Uses and Disclosures with Opportunity to Agree or Object (cont'd)
 - For notification and other purposes: a covered entity may also rely on informal permission to disclose to individual's family, friends, or to other persons whom the individual identifies, PHI directly relevant to that person's involvement in the individual's care or payment for care.
 - E.g. pharmacist dispensing of a filled prescription to a person acting on behalf of the patient.

17

Permitted Disclosures (cont'd):

- Incidental Use and Disclosure
 - A use or disclosure of PHI that occurs as a result of, or as "incident to" an otherwise permitted use or disclosure is allowed as long as the covered entity has adopted reasonable safeguards as required by the Privacy Rule, and the information shared was limited to the "minimum necessary".

18

Permitted Disclosures (cont'd):

- Public Interest and Benefit Activities
 - As required by law (statute, regulation, or court order)
 - Public health activities
 - Regarding victims of abuse, neglect, or domestic violence
 - Health oversight activities (audits, investigations)
 - Law enforcement purposes

19

Permitted Disclosures (cont'd):

- Public Interest and Benefit Activities (cont'd)
 - Regarding decedents
 - To facilitate organ or tissue donation
 - For research (extensive guidelines from HHS and NIH)
 - In situations where there is a serious threat to health or safety

20

Permitted Disclosures (cont'd):

- Public Interest and Benefit Activities (cont'd)
 - For essential government functions (e.g. military missions, intelligence gathering, Secret Service, protect health/safety of inmates in federal correctional facilities)
 - Worker's compensation: covered entities may release PHI as authorized by, and to comply with, worker's compensation laws.

21

Permitted Disclosures (cont'd):

- Limited Data Set: PHI from which certain specified direct identifiers of individuals and their relatives, household members, and employers have been removed.
 - May be used and disclosed for research, health care operations, and public health purposes.

22

(Written) Authorization Requirements:

- Covered entity must obtain authorization to use or disclose PHI for purposes other than treatment, payment, and healthcare operations or as otherwise permitted or required by Privacy Rule (see above).
- The content of the consent form, and the process for obtaining consent, are at the discretion of the covered entity.

23

(Written) Authorization Requirements (Cont'd):

- Privacy Rule does require, however, that consent form be written in "plain language", and contain specific information with regard to:
 - How the PHI is to be disclosed or used,
 - The person(s) disclosing and receiving the PHI,
 - Expiration of consent and how to revoke consent.

24

Examples of Situations Requiring Authorization:

- Disclosure to life insurer for coverage purposes
- Disclosures to an employer of results of pre-employment physical or lab test
- Disclosure to attorney's offices
- Also in this category: Psychotherapy notes

25

"Minimum necessary" Requirement:

- Covered entity must make reasonable efforts to use, disclose, and request only the minimum amount of PHI needed to accomplish the intended purpose of the use, disclosure, or request.

26

"Minimum Necessary" Requirement (cont'd):

- Covered entity must implement policies and procedures that limit the PHI to the amount reasonably necessary to achieve the purpose of the disclosure.

27

"Minimum Necessary" Requirement (cont'd):

- Need to know principle: user should access only the specific information necessary to perform a particular function in the exercise of his or her duties.
- Example: technicians should access medical records to the extent necessary to obtain insurance information and supporting documentation vs. pharmacists, who may need to delve further in the patient's record to assure appropriate medication use.

28

“Minimum Necessary” requirement not applicable in certain situations:

- Disclosures to or requests by a health care provider for treatment purposes
- Disclosures to individual, or individual's personal representative
- Use or disclosure made pursuant to a (written) authorization
- Disclosures required by law (including to HHS for compliance investigation or review)

29

Patient Rights under HIPAA:

- Privacy practice notice: Patient must be provided with a notice of the practices of the covered entity.
 - Must give notice of its information practices, including how it uses and discloses info: uwmedicine.org/Global/Legal/privacy.htm
- Access: Patient may inspect or get a copy of their PHI that is maintained by the covered entity, subject to certain limitations.

30

Patient Rights under HIPAA (cont'd):

- Amendment of PHI
- Accounting of disclosures of PHI for six years prior to date of request
 - Privacy rule does not require accounting for the following disclosures: disclosure to carry out treatment, payment, or healthcare operations; to patient or patient's PR; disclosures for facility directory or to persons involved in patient's care; or to law enforcement or correctional facilities.

31

Patient Rights under HIPAA (cont'd):

- Restriction request: Patients may ask covered entity to restrict how PHI is disclosed or used.
 - Note that covered entity is under no requirement to agree to request for restrictions.
- Request for alternative means of communicating PHI:
 - Example: patient may request that covered entity communicate with patient through a designated address or phone number.

32

Patient Rights under HIPAA (cont'd):

- Complaints: individuals may complain about compliance with privacy policies and procedures of a covered entity.
 - Complaints may be filed with the covered entity, and to the Secretary of HHS.
 - Covered entity must explain procedures for filing complaint within the privacy practices notice.

33

Pre-Emption of State Law:

- HIPAA preempts state law to the extent that it is more protective of health information than state law.
- If state law provides *greater* protection of PHI than HIPAA, then Privacy Rule allows state law to prevail.

34

Penalties (Civil):

- \$100 per failure to comply with Privacy Rule requirement.
- May not exceed \$25,000 per calendar year for multiple violations of the Privacy Rule.
- No penalty imposed if violation is due to reasonable cause, did not involve willful neglect, covered entity corrected violation within 30 days of when it knew or should have known of violation.

35

Penalties (Criminal):

- A person who knowingly obtains or discloses PHI in violation of HIPAA is subject to a \$50,000 fine and up to one year imprisonment.
- Penalties increase to \$100,000/five years if conduct involves false pretenses, and up to \$250,000/10 years if intent is to sell, transfer or use PHI for commercial advantage, personal gain, or malicious intent.
- Enforcement is responsibility of DOJ.

36

Uniform Health Care Information Act (RCW 70.02)

- Except as authorized by Act, health care information cannot be disclosed to any other person without patient's written authorization.
- "Health care information ": any information, whether oral or recorded in any medium that identifies or can be readily associated with the identity of a patient and directly relates to the patient's health care (includes DNA test results).

37

Disclosure of Health Care Information without Patient Authorization (RCW 70.02.050):

- a) To a person reasonably believed to be providing health care to the patient, or,
- b) To any other person who requires info for health care education, or to provide planning, QA, peer review, or administrative, legal or financial services to health care provider (malpractice coverage),

38

Disclosure to "Other Persons" (cont'd):

- PROVIDED THAT:
 - HCP reasonably believes that person will not use or disclose health care information for any other purpose; and
 - Will take appropriate steps to protect health care information.

39

Disclosures to "Other Persons" (cont'd):

- To any other health care provider reasonably believed to have previously provided health care to the patient, to the extent necessary to provide health care to the patient, unless patient has instructed the health care provider in writing not to make the disclosure

40

Disclosure of Health Care Information without Patient Authorization (RCW 70.02.050 , cont'd):

- To avoid or minimize imminent harm or danger
- Oral, and made to those with close personal relationships with patient if in accordance with good professional practice
- Successor-in-interest health care provider

41

Disclosure of Health Care Information without Patient Authorization:

- Research project if institutional review board approves
- Audits if identifiable information removed or destroyed at earliest opportunity and no further disclosure
- To penal or custodial officials where patient detained

42

Disclosure of Health Care Information without Patient Authorization:

- Directory information, unless patient refuses
- Cases reported by fire, police, sheriff, or other public authority, directory information, nature and extent of injuries and whether patient conscious when admitted

43

Disclosure REQUIRED:

- To federal, state, or local public health authorities to the extent required by law, when needed to determine compliance with licensure, certification, registration laws, or to protect the public health
- To law enforcement
- To county coroners and medical examiners for investigations of deaths
- Pursuant to compulsory process in accordance with RCW 70.02.060

44

Patient Authorization of Disclosure, Requirements (RCW 70.02.030):

- In writing, dated and signed by patient
- Identify nature of information to be disclosed
- Identify the name, address, and institutional affiliation of person information being disclosed to
- Identify provider making disclosure
- Identify the patient

45

Duration of Authorization:

- 90 days, unless form specifically provides expiration date.
- Patient may revoke authorization in writing at any time (some exceptions)

46

Patient's Right to Review Medical Record: (RCW 70.02.080)

- Written request from patient to examine or copy
- Provider has 15 days to respond by:
 - Making records available
 - Informing patient that records do not exist
 - Provide name and address of person maintaining records if known
 - Deny the request in whole or part in limited circumstances

47

Denial of Right to Review:

- If provider reasonably concludes that knowledge of information:
 - Would be injurious to patient's health
 - Would identify a person who provided information in confidence, where confidentiality was appropriate
 - Could be reasonably expected to cause danger to the life or safety of individual

48

Denial of Right to Review (cont'd):

- The health care information was compiled and is used solely for litigation, quality assurance, peer review, or administrative purposes; or,
- Access to the health care information is otherwise prohibited by law.

49

Patient's Right to Amend or Correct Record (RCW 70.02.100):

- For purposes of accuracy or completeness
- Request in writing
- Provider must make correction, inform patient that record no longer exists, or inform patient who has record
- No more than 21 days from request
- Patient has right to include a written statement of correction or amendment
- Mark as corrected or amended

50

Refusal to Correct or Amend (RCW 70.02.110)

- If provider refuses to correct or amend, must:
 - Permit patient to file a statement of disagreement
 - Mark the challenged entry alleged to be inaccurate
 - Forward any statement of disagreement with the medical records when requested

51

Consent by Others

- Consent may be provided on behalf of the patient by:
 - Legally authorized surrogate for healthcare decisions (see RCW 7.70.065)
 - Personal Representative of deceased patient
- Parental consent: effective only in situations where parental consent required (usually age 14 or under).

52

Civil Remedies:

- Actual damages, reasonable attorneys' fees, and other reasonable expenses
- Court injunction (provider ordered to comply with chapter)
- 2 year statute of limitations after violation discovered

53

Disclosure of Test Results for HIV/STD's (RCW 70.24.105)

- "No person may disclose or be compelled to disclose the identity of any person who has investigated, considered, or requested a test or treatment for a sexually transmitted disease, except as authorized by this chapter".

54

Disclosure of HIV Test Results, Identity of Subject

- Only to:
 - Subject of test
 - Legal representative for health care decisions
 - Exception: minor over 14 years of age and otherwise competent.
 - Pursuant to specific release from subject/legal representative
 - Otherwise authorized by this chapter

55

Patient Authorization to Disclose HIV/STD results:

- Must be in writing and signed by the test subject.
- Dated
- Must specify to whom the disclosure may be made.
- Must specify time period that authorization is valid
- May be made by legal representative, except minor over age 14

56

Disclosures Permitted without Patient Consent to the Following Entities:

- State or local public health officer, or CDC in conjunction with reporting requirements for a diagnosed case of STD
- Health care facility/provider that procures, processes, distributes or uses body parts or fluids
- State or local public health officer (considering restrictive measures), provided the record was obtained via court-ordered HIV testing

57

Disclosures Permitted without Patient Consent to the Following (cont'd):

- Local law enforcement (carrying out restrictive measures)
- Persons who, because of their behavioral interaction with infected individual, have been placed at risk for acquiring STD if health officer believes that person unaware of risk and the disclosure of identify of infected person necessary
- Court ordered access after good cause shown. Court shall limit disclosure.

58

Disclosures Permitted without Patient Consent to the Following (cont'd):

- Law enforcement officer, fire fighter, health care provider, health care facility staff, etc. who has requested a test of a person whose bodily fluids he or she has been exposed to
- Claims management personnel for prompt and accurate evaluation and payment of medical or related claims
- DSHS worker, child placing agency worker or guardian ad litem responsible for making/reviewing placement decisions to court regarding a child under 14 with STD in DSHS custody

59

Disclosures Permitted without Patient Consent to the Following (cont'd):

- Limited release within correctional facilities and jails to authorized staff, only as necessary for disease prevention or control and for protection of the safety and security of staff, offenders, and the public
- To the victim of a sexual assault, upon request

60

Re-disclosure Prohibited

- Person to whom test results have been disclosed may not disclose results to another person unless authorized as above.

61

Penalties for Violation of RCW 70.24

- Negligent violations
 - \$1,000 or actual damages, whichever is greater (per violation)
- Intentional or reckless violations
 - \$10,000 or actual damages (whichever is greater)
- Plus Attorney's fees and costs
- 3 year statute of limitations
- Criminal violations: tried as gross misdemeanor, violator subject to 1 year imprisonment and/or fine up to \$5,000.

62

Disposal of Personal Information (RCW 19.215)

- Business entity must take all reasonable steps to destroy, or arrange for destruction of, personal financial and health information. Refer to HIPAA, Uniform Health Act, as more restrictive.
- UW Policy: paper documents are placed in "confidential recycling", and are subsequently shredded.
- Also applies to diskettes, CD's, magnetic tape, and hard drives (if equipment is reassigned or decommissioned).

63

Other Washington Statutes Dealing with Patient Confidentiality Issues

Drug and Alcohol Treatment (RCW 70.96A and 42 CRF Section 2.13)

- Registration records and other records of treatment programs are confidential.
- Disclose only with
 - Prior written consent of patient
 - If authorized by a court order
 - To comply with state reporting requirements for suspect child abuse
 - When crime committed on program premises

64

Other Washington Statutes Dealing with Patient Confidentiality Issues

Mental Health Information (RCW 71.05, 71.24 and 71.34)

- Fact of admission for mental health services and all records of mental health treatment are confidential.
- Limited circumstances under which these records may be disclosed.

65

Violations of HIPAA, State Law in Normal Pharmacy Practice

- Usually can be avoided by exercising reasonable care and professional judgment. Watch out for:
 - Careless "chatter": e.g. elevator or cafeteria talk
 - Careless disposal or mishandling of patient records (includes paper records/receipts, patient-specific medication information generated when processing a prescription).

66

Violations of HIPAA, State Law in Normal Pharmacy Practice

- Failure to adequately ascertain relationship of patient to person picking up medication or inquiring about medication for patient.
- Forwarding of e-mail with patient information to non-secure site.
- Failure to protect faxed information.
- Viewing PHI on computer of patient you are not going to be interacting with.

67