BDK03 Ethical Issues in Use of Big Data

Unit 3: Privacy laws, FDA Regulations, and Evaluation pertaining to software

Exercise:

Analyze the case studies below.

*Case 1. Mental Health Center Provides Access after Denial Covered Entity: Mental Health Center*

The complainant alleged that a mental health center (the "Center") improperly provided her records to her auto insurance company and refused to provide her with a copy of her medical records. The Center provided the US Office of Civil Rights with a valid authorization, signed by the complainant, permitting the release of information to the auto insurance company. OCR also determined that the Center denied the complainant's request for access because her therapists believed providing the records to her would likely cause her substantial harm. The Center did not, however, provide the complainant with the opportunity to have the denial reviewed, as required by the Privacy Rule. Among other corrective action taken to resolve this issue, the Center provided the complainant with a copy of her records.

Discuss this case based on the 5 axes:

* **Autonomy** ‐ self‐determination, right to privacy, individual freedom, informed consent
* **Veracity** ‐ Telling the truth, keeping promises
* **Beneficence** ‐ Do good, promote well‐being of others, obligation to help those in need
* **Nonmaleficence** ‐ Avoid harm to others (Hippocratic oath)
* **Justice** ‐ Fairness, equal respect, equitable allocation of resources, social policy Who are the individuals or organizations that impact on or are impacted by the situation? How do their interests and influences relate to their relationships? What are the underlying problems that the individuals were trying to address? What categories do they fall into (e.g. computational, financial, etc.) What went wrong?

Source: http://www.hhs.gov/ocr/privacy/hipaa/enforcement

*Case 2. FBI investigating hackers*This case takes place in Virginia:

The FBI is investigating a $10 million ransom demand by a hacker or hackers who say they have stolen nearly 8.3 million patient records from a Virginia government Web site that tracks prescription drug abuse, an FBI official confirmed Wednesday. The state police in Virginia are also investigating the possible breach of confidential records. "This is a crime and it is being treated that way," Gov. Timothy M. Kaine said Wednesday. The FBI official said the Virginia Information Technologies Agency (VITA) referred the case to the FBI last week, asking for help. Asked whether people's personal information is secure, the official said he couldn't say. "I really can't make a declarative statement as to whether anyone's information is in jeopardy at this point," the official said. Asked whether people have been notified that their information may have been breached, the official said it would be up to VITA to do that.

Questions:

1. What are the lessons to be learned from this incident?
2. How responsible are individual entities (clinics, hospitals, pharmacies, government organizations, etc.) for the level of security of the data they hold?
3. Who should pay?
4. Who should notify the patient?
5. Could this have occurred in the European Union, and how might the response have been different?

Source: <http://www.foxnews.com/story/0,2933,519187,00.html>.