E-Health Records (EHRs) – 10 Things to Know

Advocates claim federally-certified electronic health records (EHRs) will transform health care delivery in America. However, concerns include:

1. Computerized medical records give government health officials easy access to private details of the confidential patient-doctor relationship.

Electronic health records (EHRs) record everything. Requiring EHRs to be interoperable across the United States (able to work together and link together) gives outsiders and strangers easy access. Outside access is authorized under federal law. Specifically, because of the federal HIPAA “privacy rule,” 2.2 million entities, including state and federal government, have access to private health records without patient consent and often without patient knowledge.

2. The federal government is paying $20 billion to doctors and hospitals to buy expensive government-certified online EHR systems.

Federal incentive payments under the 2009 HITECH Act only cover about a third of the EHR system costs—and none of the hidden administrative, training and other costs. Beginning January 1, 2015, physicians will be penalized by Medicare for not using certified interoperable EHRs.

3. To receive federal incentive payments, doctors and hospitals must demonstrate “meaningful use” of EHRs.

“Meaningful use” (MU) of EHRs for clinicians and facilities is similar but different. Professional MU includes e-prescribing, reporting “quality measures” to the federal government, implementing one “clinical decision support rule,” maintaining active medications list, and recording “smoking status.” Stage 1 and 2 MU requirements have been issued. Proposed Stage 3 is called “too harsh.”

4. EHRs interfere with the practice of medicine and have harmed patients.

EHRs have been called “clunky,” frustrating, user-unfriendly and inefficient. The federal mandate to use computerized medical records has led to productivity, alterations in medical decision-making, at least six deaths, 22 new medical errors, misdiagnoses, and doubled pediatric fatality rates. Doctors are reduced to data clerks that engage less with patients.

5. “Patient engagement” gives individuals a false sense of control and encourages patients to feed more data into computerized systems.

The Personal Health Record (PHR) or collaborative health record has been touted as giving patients access to their own data. However, the PHR is merely a subset of the EHR (over which patients have no control due to HIPAA). In addition, PHRs encourage patients to feed the system more private information. Meanwhile, technology allows off-site monitoring and genetic sequencing allows patient profiling down to the DNA.

6. EHRs are part of a larger research agenda to statistically analyze everyone’s patient information and use the “findings” to rationalize health care rationing.

The HITECH modifications to HIPAA provide 2.2 million entities with patient data for study and predictive analysis. Proponents claim algorithms can be created to theoretically “see” things in the data that people cannot see and this will lead to “cures” for cancer. Failure to do so would be blamed on insufficient data, and data withholding—including refusal to share genetic data—would be a crime.

7. When EHR research finds “cures,” doctors may be required to provide certain treatments or face financial penalties and prosecution.

“Decision Support” (DS), standardized treatment protocols based on data and algorithms embedded in a physician’s computer, will push doctors to prescribe one-size-fits-all treatments rather than customized care. Not using the standards could be considered fraud, waste or abuse. Doctors using DS are less trusted.

8. EHRs have captured the interest of investors.

Private equity firms (the kind that only acquire companies with at least $100 million in revenue) are bidding on EHR companies to expand their portfolios.

9. Congress can act to protect patients.

Repealing HITECH, defunding it, or at least repealing the penalties it imposes for failure to use interoperable EHRs would be effective in protecting patients.

10. States can act to protect individuals from harm.

Blocking a state health information exchange (HIE), refusing to connect to the NHIN, refusing a state health insurance exchange (HIX), and not allowing state data storage or analytics would protect individuals from harm.

1 After The PPACA - What Should Congress Do? Dr. Marcia Cook. http://www.youtube.com/watch?v=U5r_hfH_YYE


4 Analysis of the HITECH Act’s Incentives to Facilitate Adoption of Health Information Technology,“ Robert Hudock/Patricia Wagner, EpsteinBeckerGreen Health Care & Life Sciences Client Alert, 4/09.


16 John Moore, @john_chilmark. Twitter. https://twitter.com/john_chilmark/status/275630867739713536


