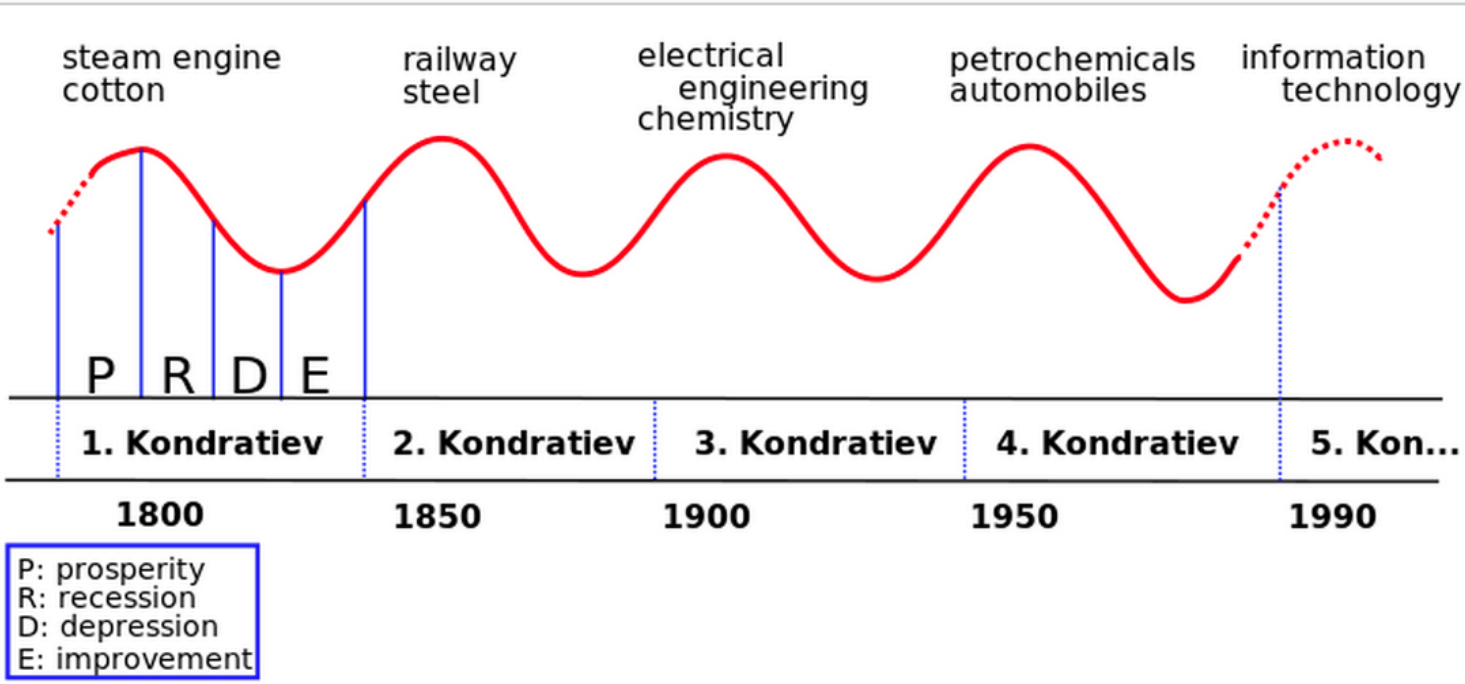
eHealth and Electronic Medical Records Problem and Pitfalls

Mark W. Sonderup
Associate Professor, University of Cape Town
Vice-Chairman, South African Medical Association



E-Health: future global economy



A rough schematic drawing showing growth cycles in the world economy over time according to the Kondratiev theory.

"All this talk about EMRs and EHRs is just a fad - like the Internet thing."

International Landscape for e-Health

- World Health Assembly resolution 58.28 on e-Health adopted that all members must develop E-Health Strategy
- International Federation of Health Information Management Associations (IFHIMA) collaborates with WHO on electronic health Information

e-Health

- Terminology that applies to use of information, computer or communication technology to some aspects of health or healthcare delivery
- Electronic Health Records are an example of an e-Health technology allowing for the acquisition, transmission or storage of patient data

A case for E-Health

- Improve efficiency within the resource constraint setting
- Improve governance
- Improve quality of health care
- Increased value for money for governments and all health care funders
- Increase access to health care

Components of e-Health

E-health embodies a significant spectrum of technologies, including:

- Health care informatics
- Mobile health (m-health),
- E-prescriptions
- Electronic health records
- Telemedicine

e-Health

- Major thinking is to improve health care locally, regionally, and worldwide by using information and communication technology
- Acceptance is almost universal but implementation has been problematic
- Barriers include financial, legal, ethical and social factors
- Understanding and addressing these barriers allows for more effective utilization of e-Health

International and South African Legislative Framework

International Legal Framework

- The Universal Declaration of Human Rights

Article12: No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks

- The European Convention on Human Rights

The European Convention on Human Rights

1. *Everyone has the right to respect for his private and family life, his home and his correspondence.*
2. *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

South African Regulatory Framework

The Constitution

- *S(10): Everyone has inherent dignity and the right to have dignity respected and protected*
- *S(14): Everyone has the right to privacy*

National Health Act

National Health Act 61 of 2003

- *S(13) obliges for health establishment to keep records in accordance with National Archives Act 43 of 1996 and Promotion of Access to Information Act 2 of 2000*
- *S(14) makes provision for confidentiality and requires that health information data can only be disclosed under the following conditions*
- *Consent has been provided by user*
- *There is a court order*
- *Failure to disclose information could represent threat to public health*

SA: National Health Act

- *S (15) makes provision for health care worker to disclose information to other health care workers and establishment as is necessary for the scope of their worker and such disclosure is in the interest of the user. This section allows for sharing of the information between health care workers and establishment.*
- *S (16) makes provision for access to health records for health care workers for treatment, research and training.*
- *S (17) makes provision for the protection of health records and places the onus on the person responsible for the health establishment (i.e. Medical Managers, specialists and GPs) to prevent unauthorised access to records and storage of such. The section also outlines offences related to unauthorised access, damage and amendments of health records*

Electronic Communication Transaction Act (ECTA)

- CH.VIII(50.1) provides for the protection of personal information obtained through electronic transactions
- Makes provision for sharing of data
- Requires written authorisation before electronic distribution of any information

POPI Act

Protection of Personal information Act (PoPI), 2004

The purpose of the act is:

- *To give effect to the constitutional right to privacy, by safeguarding personal information when processed by a responsible party, subject to justifiable limitations that are aimed at—*
  - *balancing the right to privacy against other rights, particularly the right of access to information; and*
  - *protecting important interests, including the free flow of information within the Republic and across international borders;*

ELECTRONIC HEALTH RECORDS

Electronic Health Records

*A **personal health record** (PHR)* is an electronic application through which individuals can access, manage, and share their health information, and that of others for whom they are authorised, in a private, secure, and confidential environment. This record is owned by the patient, and is populated by the patient or user.

The **electronic health record** (EHR) is a digital version of a patient's paper chart. Populated by healthcare professionals

Electronic Health Record (EHR)

- It includes all information contained in **a traditional health** record including a patient's *health profile such as medical history, diagnosis, treatment and care as well as investigations.*
- It can be accessed by multiple professionals in care of patient
- It allows for the inclusion of information across multiple episodes and providers, which will ultimately evolve into a lifetime record

EHR Benefits

- **Improved productivity, efficiency, accessibility**
  - Streamlines/eliminates paper work
  - Promotes Evidence-Based Medicine
- **Quality of Care Improvement**
  - Legible records e.g. reduced drug errors
- **Job Satisfaction Improvement**
  - Fewer repetitive, tedious tasks
  - Less "chart chasing”

EHR - Challenges

- Ethical issues
- Legal issues
- Cost
- Infrastructure needs e.g. rural areas and developing countries
- Litigation risk
- Potential Data errors
- Reduced Physician autonomy
- Culture change

Ethical Issues

Basic ethical principles

1. Principle of Autonomy
2. Principle Beneficence
3. Principle of Non-Maleficence
4. Principle of Justice

Ozair, F et al. *Perspect Clin Research*. 2015 6(2) 73-76

Ethical Issues

Basic ethical principles

1. Privacy and Confidentiality - Autonomy
2. Security breaches – Non maleficence
3. System implementation - Beneficence
4. Data inaccuracies - Justice

Ozair, F et al. *Perspect Clin Research*. 2015 6(2) 73-76

Principle of Autonomy: Privacy and Confidentiality

- Privacy “right to be let alone” or “keeping information about yourself from being disclosed”
- Physicians can potentially breach confidentiality rules when data is shared with other people
- Most of the country’s legal frameworks allows for sharing of data between health professionals

Autonomy: Confidentiality

- Preauthorized privileges allow for levels of security – user is thus accountable
- Unauthorised access may harm the patient
- Unauthorised sharing of data for financial gain will reduce patient trust and physicians should guard against this

Green AH. *JAHIMA*. 2011; 82:58

Confidentiality

- Key to preserving confidentiality is to restrict access to database through authorizing users
- Survey found that 73% of physicians text each other about patients
- Mobile devices are not secure!
- Availability of data can tempt researchers to analyse data
- However public health concerns can emerge from the data
- Most of countries have legislation that makes provision to monitor and analyse routine collected data to improve health care, in sharing this information doctors must conceal identity of their patients and ensure compliance with country legislation.

Autonomy: Consent

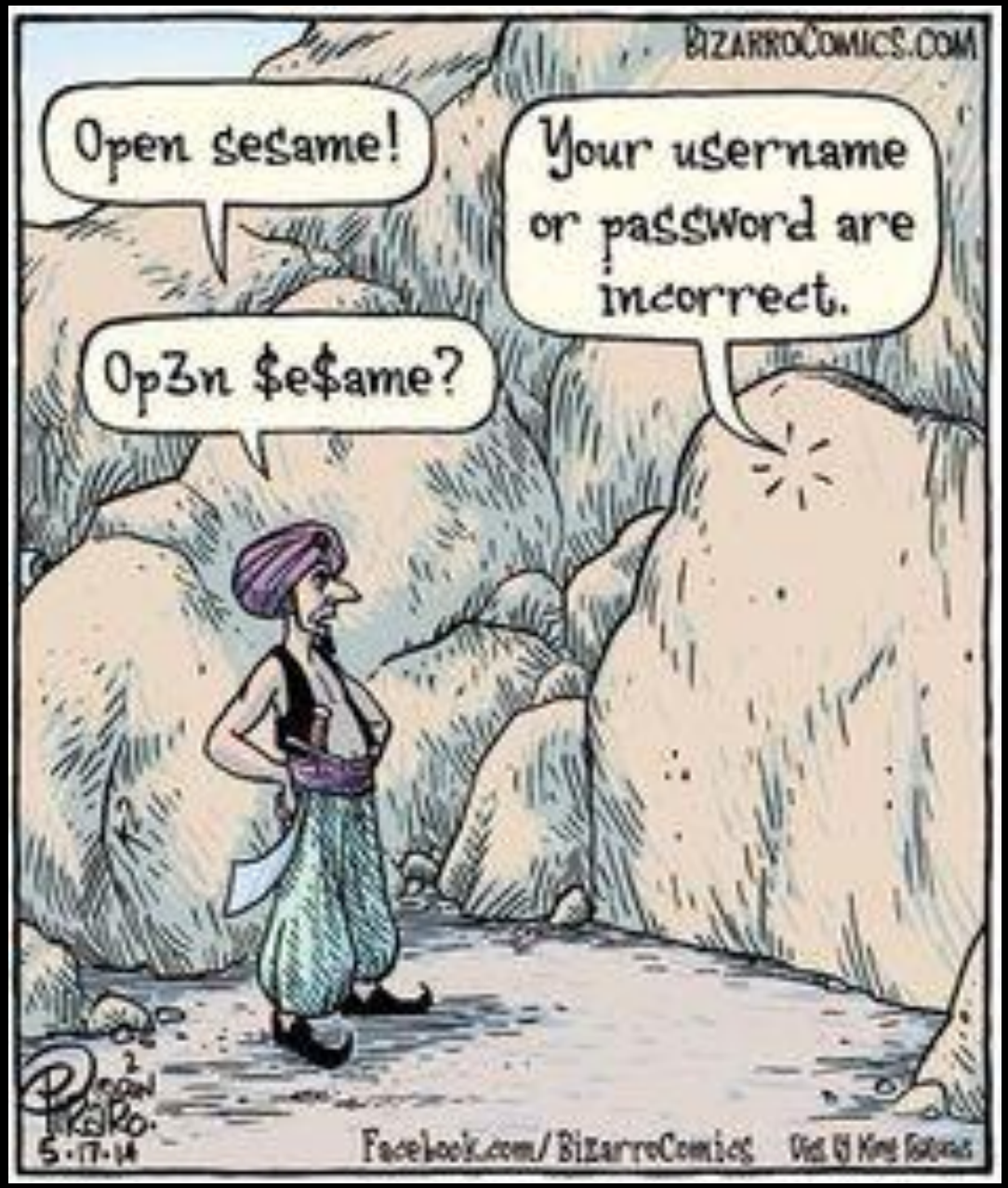
- Consent for EHR is different from clinical consent
- Consent must include the purpose of the data which may include the following:
  - Access to other health professional in care of patient, teaching, research, submission of claims, statutory reporting obligations
  - Consent can be prescribed by law
  - Implied consent can be used when sharing data amongst health professional

Non-maleficence/Security breaches

- Patient and health service user deserve to know what their information will be used for
- Information should only be used for the specified and agreed purpose.
- Any use other than what the USER understands it to be will erode the patient-doctor trust compact
- Doctors, being the link between patients and other users (e.g. funders) must always understand the use for data and guard against inappropriate use of clinical information

Data security and security breaches

- *Physical Security:* All devices are stored in a secure environment – typically lacking with EHR
- *Procedural Security* : availability policies and procedures covering the security of the electronic records
- *Operating system security*: users are provided ID and password
- *Software Application Security:* Each user has their unique user ID and secret password for the application,
- *Data encryption:* especially with cloud application


BIZARROCOMICS.COM
Open sesame!
Your username or password are incorrect.
Op3n $e$ame?
5-17-14
Facebook.com/BizarroComics

Data security and security breaches

- *2013 -* Washington Hospital employee charged under HIPAA for selling patient data
- Similarly *34000* patients data had been compromised through being downloaded onto a laptop that was then stolen
- Data was password protected but unencrypted
- Data needs password protection and encryption


OH, I FORGOT THAT YOU MISSED THE MEETING. OUR DATA SECURITY TEAM ADDED SOME NEW PROTECTION WHEN ACCESSING PATIENT DATA FILES.
CARTOONSTOCK .com
Search ID: jcen1493
© Jon Carter • cartertoons

Ownership of data

- **Multiple views on data ownership**
  - **Individual**: only the patient can decide who has access to their data. This gives patient autonomy but may adversely affect health come when physicians cannot obtain data
  - **Joint**: This seems to be a reasonable ground as it enables access for care of the patient but patient need to give permission for any uses of data
  - **Organisation and doctors:** This means organisation can do as they wish with data, reducing autonomy of patients which may violate individuals right to privacy and increases confidentiality bridges
- **Ownership may be defined in the rule of law**
- **Ownership Conflict may arise when data is sold.**
- **It is imperative that NMAs establish ownership of data in their respective countries**

Principle of Beneficence/System implementation

- Implementation requires adequate funding
- Involvement of clinicians, IT specialists, educators
- Many projects fail because they don't include physicians/clinicians
- Interface between user and computer is critical – can determine success or failure

Justice/Data inaccuracies

- Integrity of data entered is paramount
- “Cut and paste” phenomenon harmful and unacceptable
- “Drop down menus” also remove physicians clinical intuitiveness and repertoire
- When the system is down no access to health records : may increase morbidity?

Justice

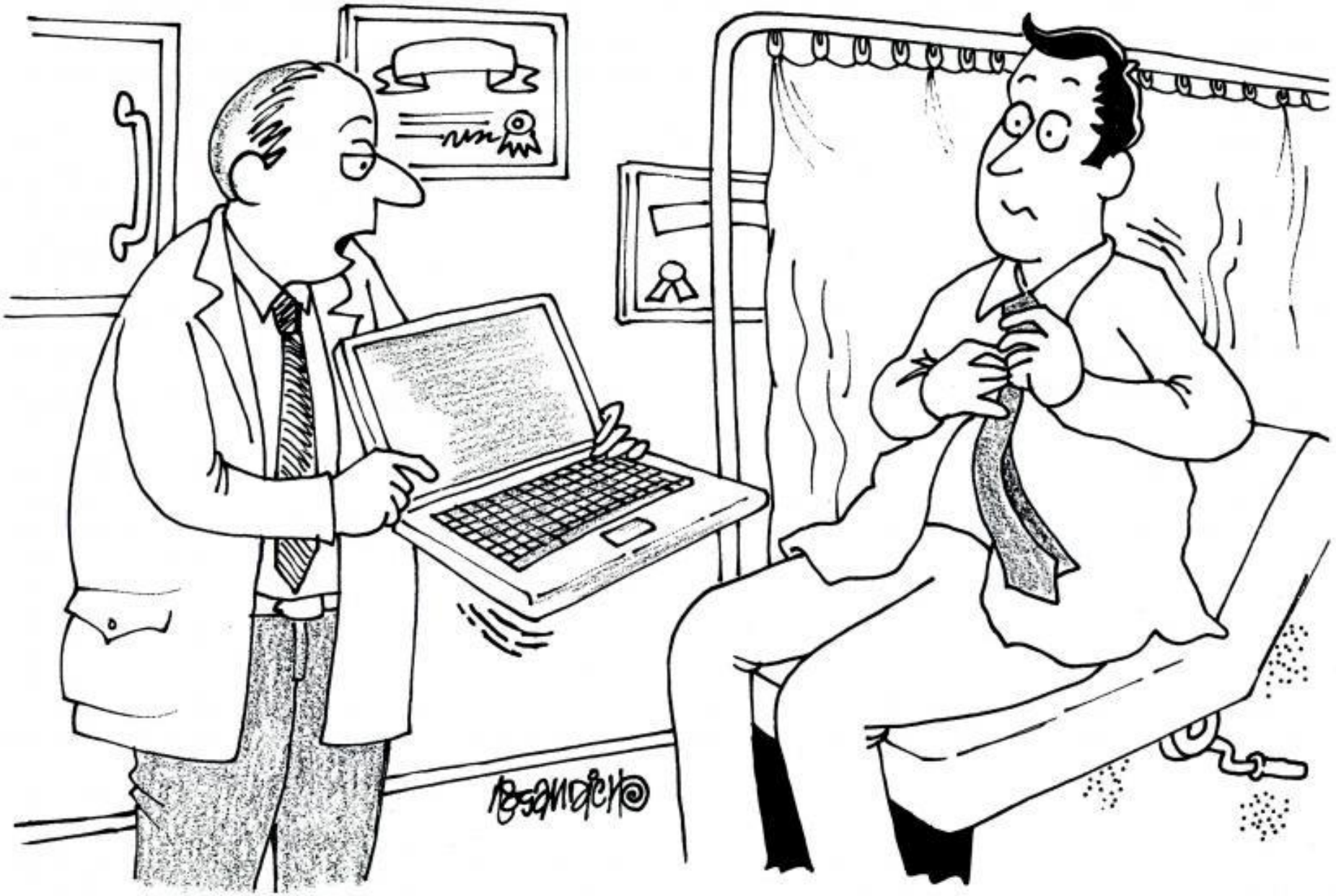
- e-health is a ***potential*** tool to promote justice
- Can enable us to monitor disparities in health care:
- e-health has potential for infrastructural development in disadvantaged communities- creating jobs and improving access to health care and technology simultaneously
- Prioritising previously disadvantage communities in rolling out e-health can reduce the economic, health and technology gaps

Successful EHR

- Strategic and integrated action at the national level
- Detailed planning to achieve efficiency
- Proper legislation
- Collaboration between Health and ICT sector, public and private sector
- Political buy-in
- Proper funding
- Involvement of end user i.e. doctors and patients

An ethically sound EHR system

- An ethically sound EHR system will
- Promote individual autonomy seeks to minimise security breaches and respect the nature of the confidential relationship between doctor and patient.
- Policies in place to control access
- Patients have element of control of health records



"If you want a second opinion, I'll ask my computer."