School of
Geography and Planning

Privacy of Health Records: Evidence from a pan-European study

Dimitris Potoglou

Topics relevant to social prescribing

- Public perceptions on health data use and sharing

- Challenges of sharing, storing and using health data
  - Public's behavioural intentions
  - Contrasts between individual and public benefit

Focus on public preferences between privacy and security across EU27

Public Perception of Security and Privacy:

Assessing Knowledge,

Collecting Evidence,

Translating Research into Action

- A three-year project, 2012-2014:
  - www.projectpact.eu

- 11-member consortium led by:
  - Centre for Science, Society and Citizenship (CSSC, Italy)
  - Peace Research Institute (PRIO, Norway)

SEVENTH FRAMEWORK PROGRAMME

CARDIFF UNIVERSITY
PRIFYSGOL CAERDYDD
School of
Geography and Planning

Three contexts, all relevant to the European setting, were selected

1. Travelling on the Metro/Rail: Physical Surveillance and Screening

2. Choice of Internet Service Provider: Internet Surveillance

3. Health Data Records and Data Mining for Personal and Public healthcare

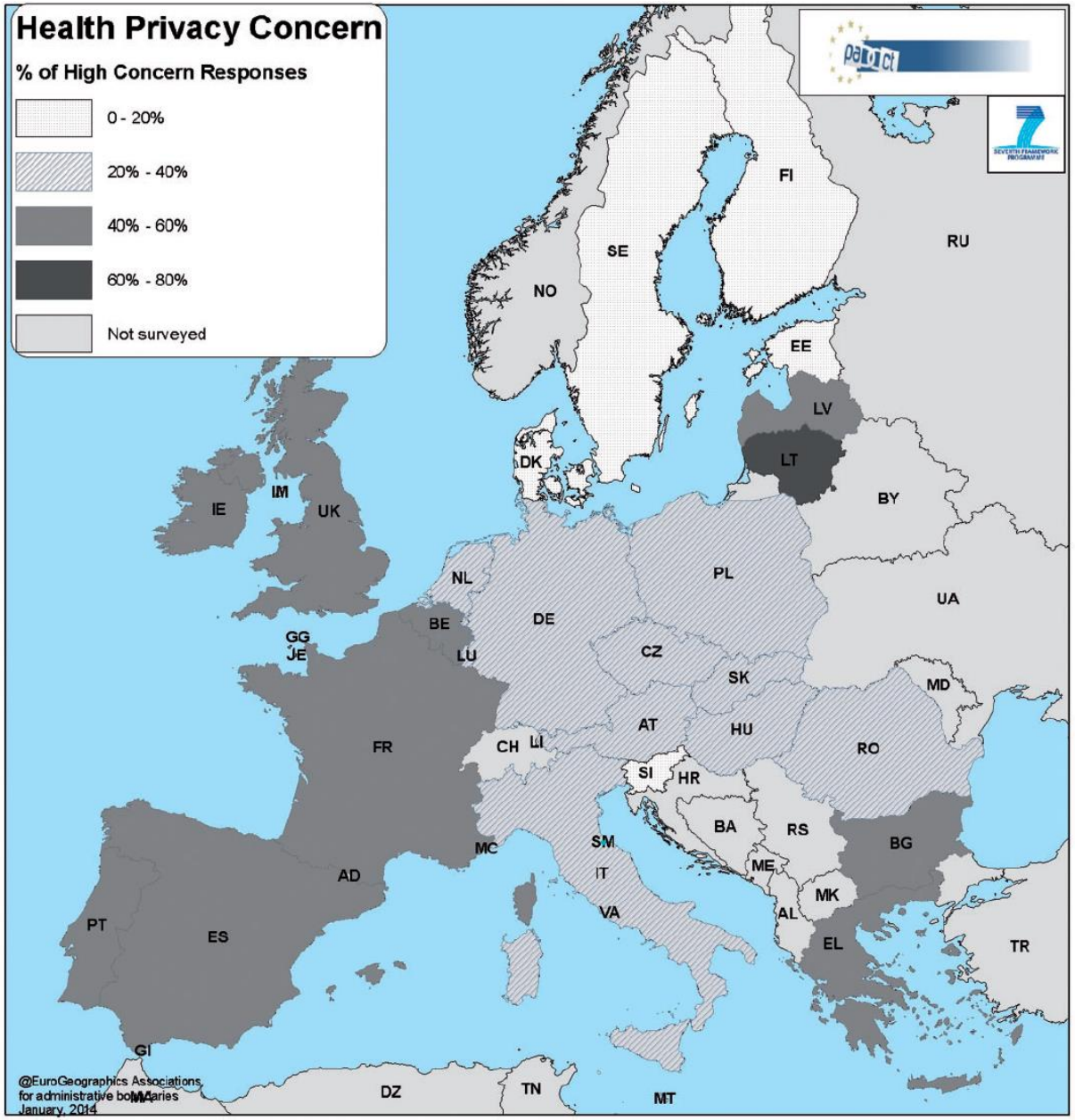
Main Survey Data Collection

Target population	General population, aged 18+
Number of countries	27 EU member states
Number of participants	26,443
Survey administration	Online: 12 countries Face-to-face: 13 countries Mixed methodology (500 online, 500 face-to-face): 2 countries
Sampling design	**"On-line" countries:** representative quotas on age, gender and region **"Face-to-face" countries:** 3 step approach (stratification and selection of sampling points, selection of addresses within each sampling point, selection of individuals within each selected household (quotas by age and gender)

Public perceptions on health data across the EU27

	N	Responses (%)	
Attitudes to data storage			
Storing health information is useful for improving treatment quality[a]	20464	75.5	Agree or agree strongly
Storing health information is useful for preventing health epidemics[b]	20361	63.9	Agree or agree strongly
Lack of personal and health information leads to delays in treatment in health emergencies[c]	20368	58.9	Agree or agree strongly
Health providers collect too much personal information[d]	20391	37.0	Agree or agree strongly
Concerns about access to data			
Access to personal information by non-medical personnel[e]	20696	48.9	Concerned or very concerned
Access to personal information by private companies[e]	20676	60.6	Concerned or very concerned
Misuse of personal information for harassment[e]	20572	54.5	Concerned or very concerned
Opinions about data security			
Healthc are providers are successful in preventing unauthorized access[f]	19372	38.4	Agree or agree strongly
Computer databases should be protected from unauthorized access, regardless of cost[g]	20134	73.4	Agree or agree strongly

Health Privacy Concern Index



Europeans' Preferences for Health Records: Choice context

Description	Option A	Option B	Option C
What information is stored on the device/system	Information on device/service	Information on device/service	
In which countries your information can be accessed?	Worldwide	Across Europe (EU)	
Who else can view this information apart from the medical specialists?	Health insurance companies	Private sector pharmaceutical companies	
Cost	£ 0.58 per month	£ 2.32 per month	

Currently, there are devices or services in the form of health ID, cards, tags, etc. that can store and allow access to your health information. This information may include personal details such as: your name, address, blood group/type, allergies, current health conditions and medical history. These devices or services are available for purchase or may be provided by your national government at some cost to you. Payment may be direct or through your income tax or health insurance contributions.

With these devices, for example, doctors can become aware of any existing medical conditions (e.g., allergies to medicine and food), authorities can identify you and respond faster in an medical-emergency situation (e.g. pandemic, flu) or in emergencies when you are traveling abroad.

On the other hand, information stored on such a device or system may be misused or may affect your privacy, for example when unauthorized users get access to such information.

What information is stored on the device/system?

Only basic health status information

Basic health status information

Identification

Lifelong health conditions

All other health conditions and medical history

Who can access the information?

Only doctors and nurses

Doctors, nurses, and emergency medical personnel (paramedics)

Doctors, nurses, emergency medical personnel (paramedics), and other non-medical emergency personnel (fire and rescue)

In which countries can your information can be accessed?

Only in [country of residence]

Across Europe (EU)

Worldwide

Who else can view this information apart from the medical specialists?

No one

Immediate family

Nurses providing home care

Health insurance companies

Private sector pharmaceutical companies

Academic researchers (If your name is not connected to the data)

Cost

Free (given by your hospital/national government)

0.5 €/month

1 €/month

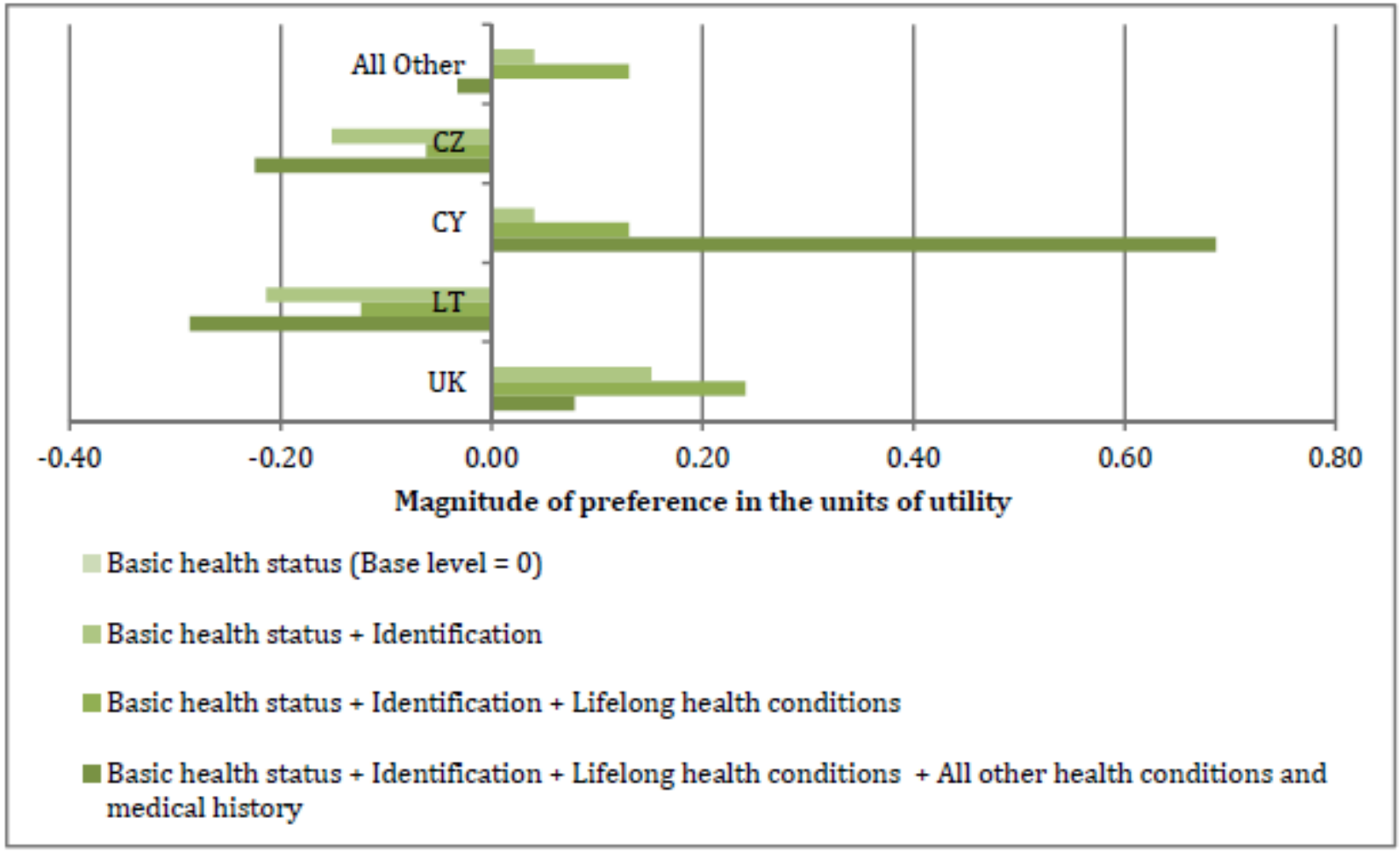
2 €/month

3 €/month

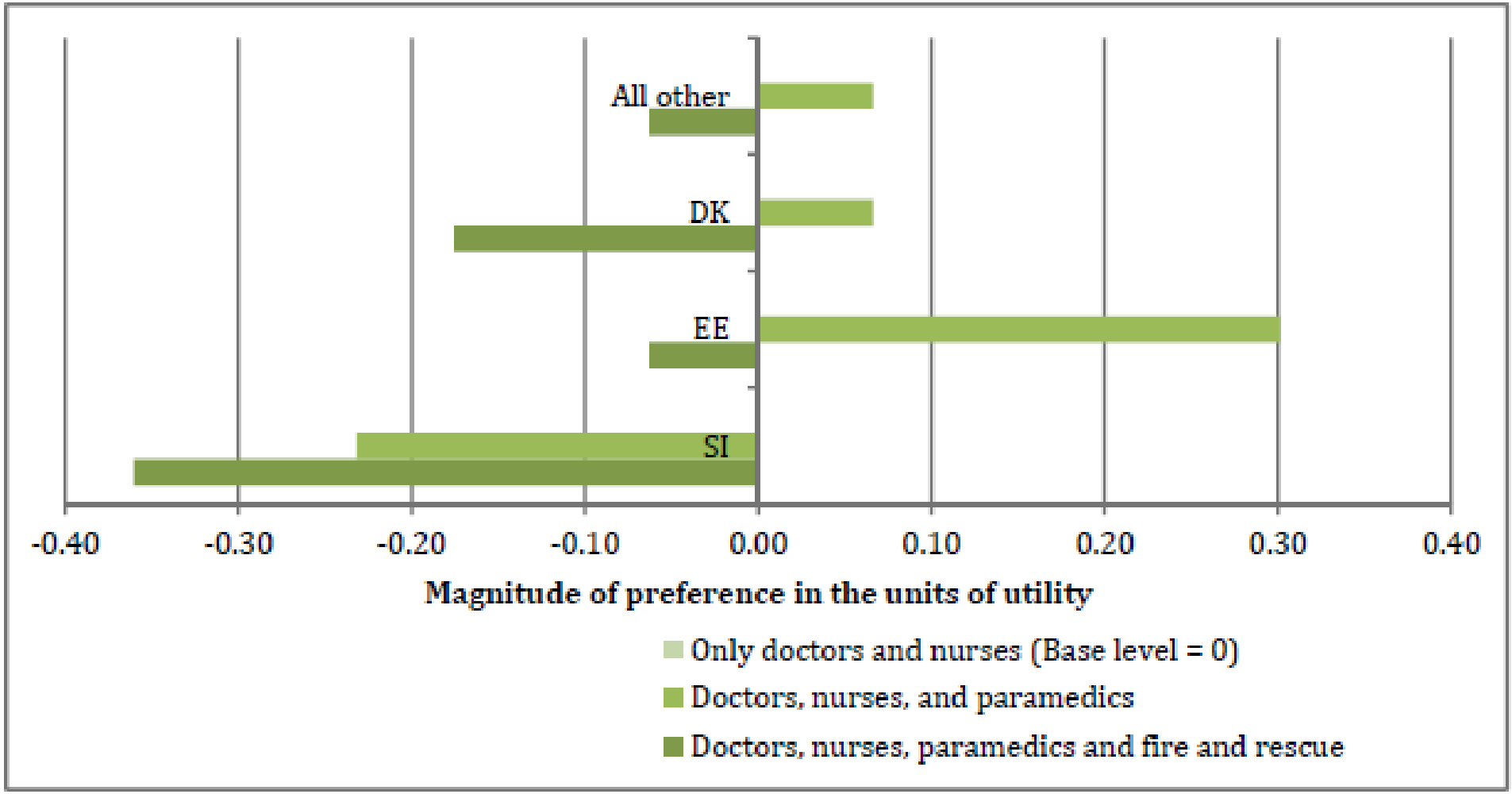
Range of attributes used in the Health—data experiment

Description	Option A	Option B	Option C
What information is stored on the device/system	**Information on device/service**	**Information on device/service**	I would not purchase any such device/service
Basic health status: blood group, allergies, diabetic status	Basic health status information	Basic health status information	
Identification: name, address, age, photograph, nationality	Identification	Identification	
Lifelong health conditions: asthma, disabilities, cancer, etc.	Lifelong health conditions	Lifelong health conditions	
All health conditions: mental health, sexual health, addictions, and medical history		All other health conditions and medical history	
Who can access the information	Doctors, nurses, and emergency medical personnel (paramedics)	Only doctors and nurses	
In which countries your information can be accessed?	Worldwide	Across Europe (EU)	
Who else can view this information apart from the medical specialists?	Health insurance companies	Private sector pharmaceutical companies	
Cost	£ 0.58 per month	£ 2.32 per month	

Most EU countries preferred a device to store increasingly expansive healthcare data, but only up to a point

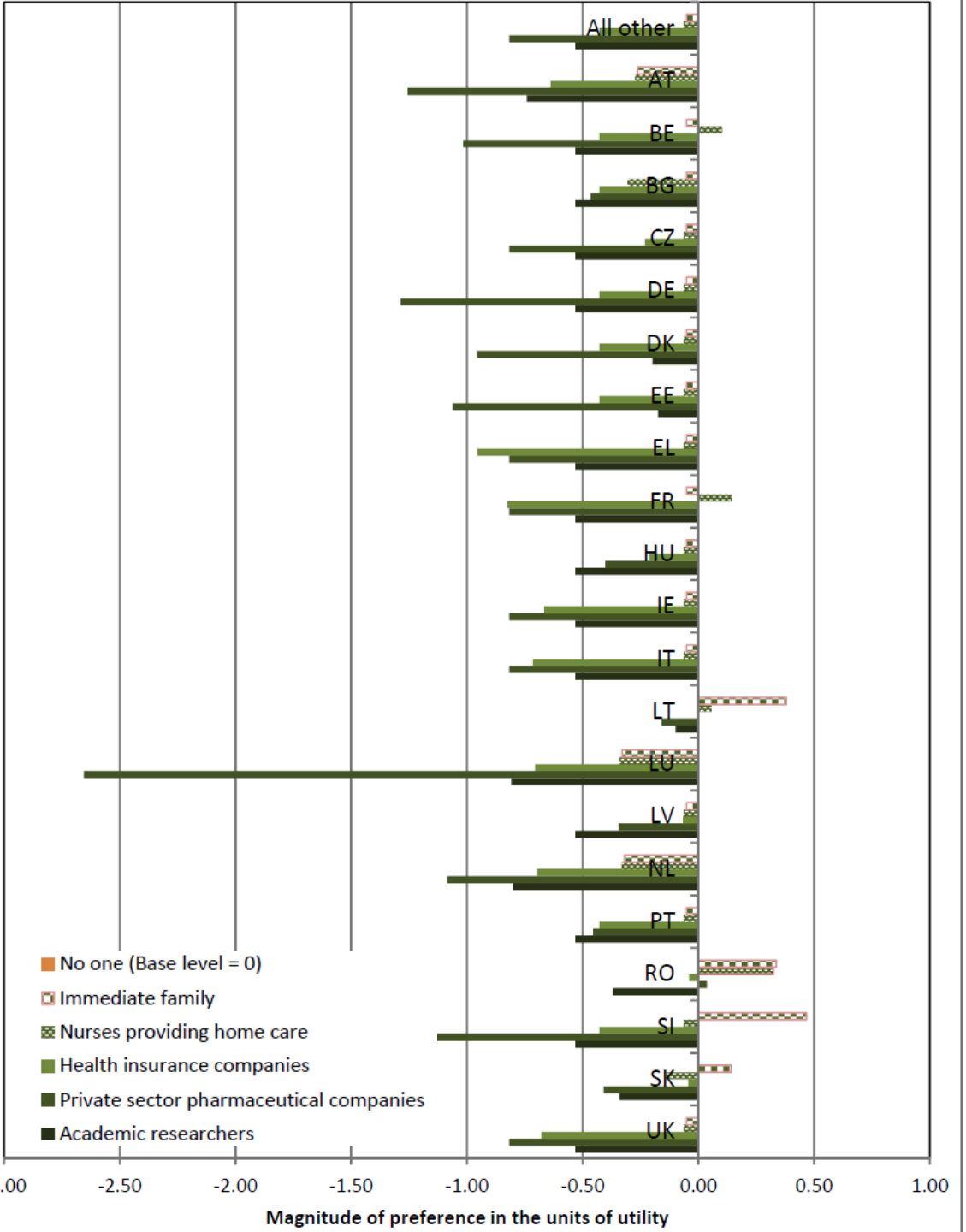


All else being equal, respondents would only allow doctors, nurses and paramedics but not other emergency services



Who else can view health data beyond medical specialists?

- With reference being ‘only medical specialists’, European citizens were overall:
  - Averse to immediate family, health insurance companies, private sector pharmaceutical companies, and academic researchers having access to their health-related data



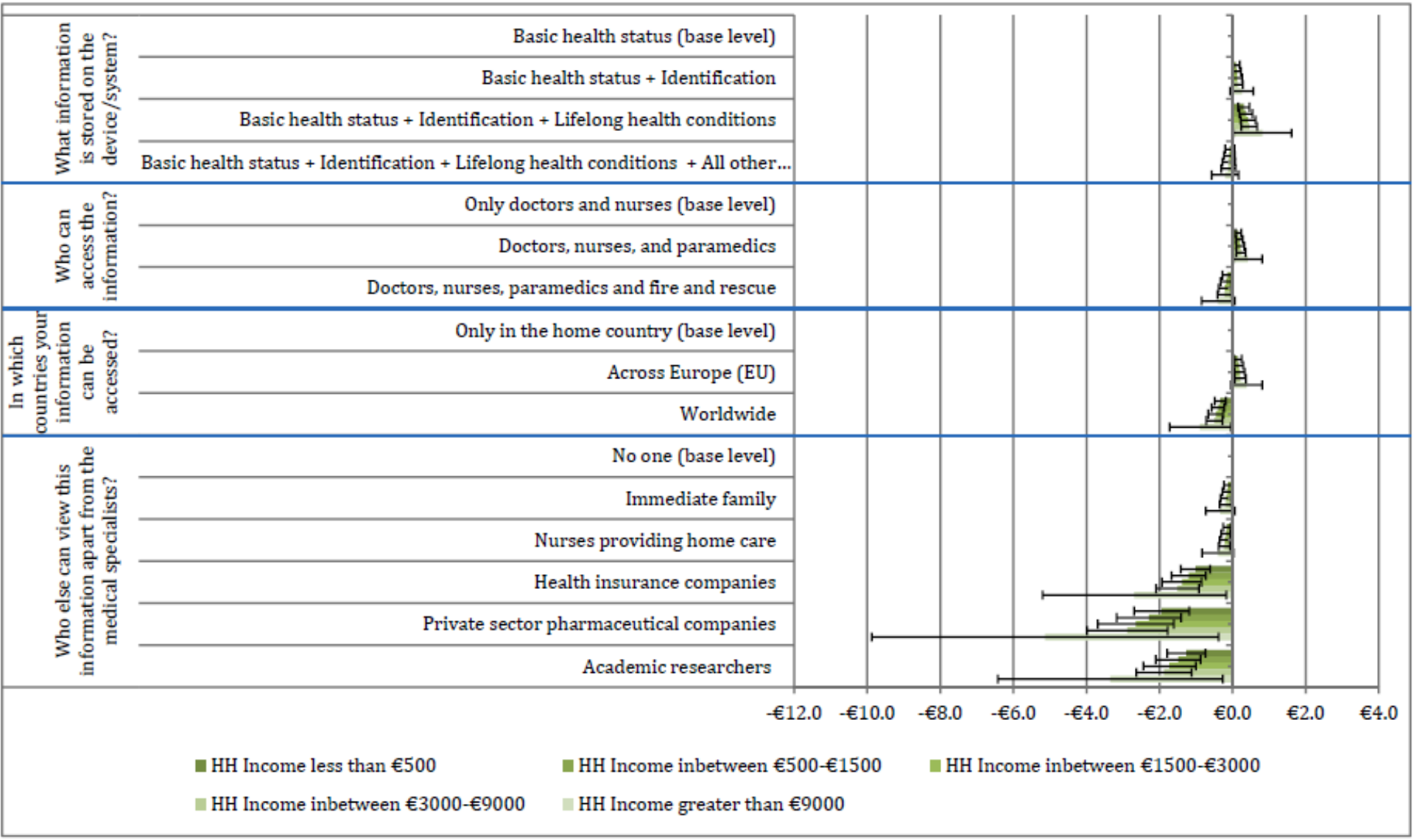
- Lithuania, Romania, Slovenia and Slovakia: in favour of immediate family to view health records

- Belgium, France, Lithuania and Romania: in favour of home care nurses be able to view health records

Evidence from cognitive testing of scenarios also showed that

- Little awareness of how health data can be stored and used – e.g. as a measure of safety
- Consent and transparency were the most important elements mentioned by participants
- People felt the need to be informed about:
  - How their data is stored
  - Who can have access to it
  - Health data should not be shared without their permission, even in emergency situations
- Risk of discrimination of people who suffer from certain illnesses

Everything else being equal, respondents were willing to pay for privacy protections but not sharing of data



Implications for policy

- Storage:
  - People across EU27 feel that benefits outweigh risks to privacy
    - Shift to electronic records is in line with the findings of this study
  - However, we do find stronger preference to include mental and sexual health, addictions and medical history among 18-34 year olds
    - those aged 35 years and over were against
  - Findings provide some support for the current system of separation and anonymity in the storage of sensitive medical records. For example, in the UK sexual health services are not stored as part of the patient's health records

Implications for policy [2]

- Access:
  - Access to information across Europe was generally preferred but worldwide access was not
  - Health information is increasingly being accessed by the police and emergency services (e.g. to enable a more effective response to emergencies) and we found in general that this is not preferred

Implications for policy [3]

- Sharing:
  - Sharing beyond health care professionals was not preferred
  - Our work provides insight across several areas in this ongoing debate; particularly, around the sharing of electronic health records for research

Conclusion

- Evidence of privacy (valuation) paradox:
  - People value privacy very highly, however, they express differing preferences when it concerns priorities that they deem important in the immediate context (money, attitudes, acceptability)

- Observed preferences reflecting a ‘free-rider’ challenge
  - Sharing of personal data for own healthcare benefits is preferred but the types of sharing likely to have wider public health benefits is less preferred

- Data sharing preferred only with designated healthcare professionals
  - Raising questions of trust

Failing to address privacy in innovative models for healthcare delivery or active aging initiatives (e.g. through non healthcare professionals or mediated by technology) may disengage individuals

Public preferences for electronic health data storage, access, and sharing — evidence from a pan-European survey

RECEIVED 14 September 2015
REVISED 24 November 2015
ACCEPTED 16 January 2016
PUBLISHED ONLINE FIRST 23 April 2016

Sunil Patil,[1] Hui Lu,[1] Catherine L Saunders,[1] Dimitris Potoglou,[2] and Neil Robinson[1]

RESEARCH AND APPLICATIONS

ABSTRACT

Objective To assess the public's preferences regarding potential privacy threats from devices or services storing health-related personal data.
Materials and Methods A pan-European survey based on a stated-preference experiment for assessing preferences for electronic health data storage, access, and sharing.
Results We obtained 20 882 survey responses (94 606 preferences) from 27 EU member countries. Respondents recognized the benefits of storing electronic health information, with 75.5%, 63.9%, and 58.9% agreeing that storage was important for improving treatment quality, preventing epidemics, and reducing delays, respectively. Concerns about different levels of access by third parties were expressed by 48.9% to 60.6% of respondents.
On average, compared to devices or systems that only store basic health status information, respondents preferred devices that also store identification data (coefficient/relative preference 95% CI = 0.04 [0.00-0.08], $P = 0.034$) and information on lifelong health conditions (coefficient = 0.13 [0.08 to 0.18], $P < 0.001$), but there was no evidence of this for devices with information on sensitive health conditions such as mental and sexual health and addictions (coefficient = −0.03 [−0.09 to 0.02], $P = 0.24$). Respondents were averse to their immediate family (coefficient = −0.05 [−0.05 to −0.01], $P = 0.011$) and home care nurses (coefficient = −0.06 [−0.11 to −0.02], $P = 0.004$) viewing this data, and strongly averse to health insurance companies (coefficient = −0.43 [−0.52 to 0.34], $P < 0.001$), private sector pharmaceutical companies (coefficient = −0.82 [−0.99 to −0.64], $P < 0.001$), and academic researchers (coefficient = −0.53 [−0.66 to −0.40], $P < 0.001$) viewing the data.
Conclusions Storing more detailed electronic health data was generally preferred, but respondents were averse to wider access to and sharing of this information. When developing frameworks for the use of electronic health data, policy makers should consider approaches that both highlight the benefits to the individual and minimize the perception of privacy risks.

Keywords: Heal

https://doi.org/10.1093/jamia/ocw012

BACKGROUND

The electronic storage, access, and sharing of medical data through personal devices or systems of clinical electronic patient records underpin current developments in record-keeping and communication between patients and professionals,[1] calculation of payments to health care providers,[2] measurement of health care quality,[3] and patient engagement with their health and health care, and they provide a resource for medical research.[4–7] The scope and volume of information stored has grown exponentially over the last 2 decades. Data sources range from personal information uploaded voluntarily to personal devices (eg, through smartphone apps[8] or fitness gadgets) or websites (eg, PatientsLikeMe in the United States or LifeSensor in Europe),[9] or in formal records of the clinical details of interactions with health services (electronic patient records).[1] Patient health records have evolved from paper documents designed for record-keeping and communication between health care professionals, protected by doctor-patient confidentiality, to electronic documents of which patients and doctors are co-producers.[1,5,7] In parallel, exploiting the economic potential of health care data is becoming embedded into research and health service strategies.[5,6,10]

Currently, the European Data Protection Directive[11] is the overarching regulatory framework governing health care data in Europe; however, there is some divergence in EU countries as to how this directive is applied in practice,[12] and it is currently under review.[13] Specific guidance for storage, access to, and sharing of health data has been slow to develop. This is partly because the speed of technological change has outpaced law-making, but also because of the difficulties of balancing the seemingly competing priorities of individual privacy of health data against other priorities for the use of this data. No clear consensus about how these priorities should be translated into law, policy, and practice has yet emerged,[14] although reviews are in progress.[13,15,16] A recent UK information governance review acknowledges this connection directly, that the duty to share information in patients' wider interests is as important as the duty to maintain patient confidentiality.[15]

Behind the need for policy guidance within the context of these sometimes competing priorities is a need for clear, high-quality evidence about what public preferences are for electronic health data, and whether or how these public preferences illuminate trade-offs of benefits and risks, between privacy and data storage, access, and sharing.[14,17,18] Research to date has been mixed, with conflicting findings, highlighting both concern and support for sharing or use of medical records in research, for example.[17,19–26]

Stated preference (SP) experiments have been used extensively in the fields of marketing, transport economics, environmental valuation, health, and health care.[27] Briefly, compared with opinion polls or traditional survey approaches, SP experiments provide a more nuanced insight into preferences and allow a number of the attributes that may

Correspondence to Sunil Patil, RAND Europe, Westbrook Centre, Milton Road, Cambridge, CB4 1YG, UK; spatil@rand.org; Tel: +44 1223 353 329. For numbered affiliations see end of article.