Health Informatics

Lecture 6

Samantha Kleinberg
samantha.kleinberg@stevens.edu

Final project

- **Proposals due March 28 at latest**
  - **Max possible grade on project is A- if you do not submit a proposal. I encourage you to submit early!**
- Proposal content:
  - What will you do? How will you do it? If you need data, do you have it?
  - How will you determine if you were successful? What are the key outcomes of your project?
  - If 2 person team, how labor will be divided.
- 1 page. This is a hard limit.

Final project

- Some combination of computing/health
- Possible formats:
  - **Applications** Develop a computational system (app, website, piece of software) that addresses some aspect of health
  - **Grant** Write a proposal (formatted like a grant) for a biomedical informatics study. Extensive lit review (i.e. why it's an open problem), plan along with contingencies (what are the challenges and what happens if things go wrong?) and work showing feasibility
  - **Experiment** Analysis of health-related data

Paper/presentation/etc

- Presentations during final class
- Papers
  - 6-8 pages in NIPS format.
  - Templates: https://nips.cc/Conferences/2015/PaperInformation/StyleFiles

Midterm

- Next week!
- In class
- Closed book
- On everything covered up to the midterm

HIPAA

Health Insurance Portability and Accountability Act

Includes definitions for protected health information (PHI), and what can be shared and with whom

- Who's covered by HIPAA?
  - Ex: healthcare provider, researchers working with PHI from hospital
- What's required?
  - Usually need consent, unless waiver from IRB or meet certain other criteria
- Key component: If data are de-identified and you don't have reason to believe that they can be re-identified… no longer covered by HIPAA

18 HIPAA identifiers

1. Names
2. Certain geographic information
3. Dates other than year; all ages over 89 and all elements of dates (including year) indicative of such age, except when aggregated into a category of age 90 or older;
4. Phone numbers;
5. Fax numbers;
6. Electronic mail addresses;
7. Social Security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers;
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. URLs
15. IP addresses
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code

- Not required to be removed
  - Genetic information
  - Text
- Use imperfect method or just give up?

- Should people be able to consent?

- No longer treated as identifiable
  - Safe Harbor: Remove 18 HIPAA identifiers, and no knowledge that people can be re-identified
  - Statistical method: Or guarantee “small” chance of re-identification
- Limited dataset (e.g.for research, public health)
  - 16 of 18 removed (can keep dates)
  - No consent needed
  - Re-identification prohibited

OPEN ACCESS

Building public trust in uses of Health Insurance Portability and Accountability Act de-identified data

Deven McGraw

Correspondence to
Deven McGraw, Center for Democracy & Technology, 1634 I Street, NW Suite 1100, Washington, DC 20006, USA; deven@cdt.org

Received 26 March 2012
Accepted 31 May 2012
Published Online First 26 June 2012

1. Prohibiting unauthorized re-identification of de-identified data;
2. Ensuring the robustness of de-identification methodologies;
3. Establishing reasonable security safeguards for de-identified data;
4. Increasing public transparency about uses of de-identified data.

roval of certain uses

Reinvestment Act
ent of Health and
ue a report on the
lard.[5] In response,
de-identification in
had not yet been
ubmitted for publi-
linger about the
dentification, while
e. In 2011 the USA
centive programme
electronic medical

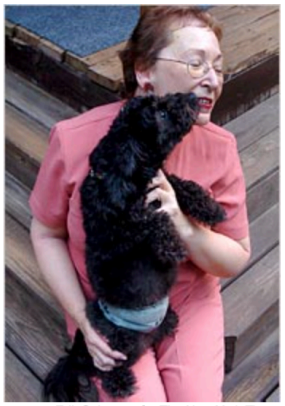
Scope HIPAA sets forth methodologies for de-identifying health data; once such data are de-identified, they are no longer subject to HIPAA regulations and can be used for any purpose. Concerns have been raised about the sufficiency of HIPAA de-identification methodologies, the

records by healthcare providers. One goal of the programme is to enhance the quality and efficiency of the healthcare system, which will require greater access to health information for analytics purposes. Failure to address concerns about the de-identifica-

A Face Is Exposed for AOL Searcher No. 4417749

By MICHAEL BARBARO and TOM ZELLER Jr.
Published: August 9, 2006

Buried in a list of 20 million Web search queries collected by AOL and recently released on the Internet is user No. 4417749. The number was assigned by the company to protect the searcher's anonymity, but it was not much of a shield.



Erik S. Lesser for The New York Times

Thelma Arnold's identity was betrayed by AOL records of her Web searches, like ones for her dog, Dudley, who clearly has a problem.

Multimedia

Graphic: What Revealing Search Data Reveals

No. 4417749 conducted hundreds of searches over a three-month period on topics ranging from "numb fingers" to "60 single men" to "dog that urinates on everything."

And search by search, click by click, the identity of AOL user No. 4417749 became easier to discern. There are queries for "landscapers in Lilburn, Ga," several people with the last name Arnold and "homes sold in shadow lake subdivision gwinnett county georgia."

It did not take much investigating to follow that data trail to Thelma Arnold, a 62-year-old widow who lives in Lilburn, Ga., frequently researches her friends' medical ailments and loves her three dogs. "Those are my searches," she said, after a reporter read part of the list to her.

AOL removed the search data from its site over the weekend and apologized for its release, saying it was an unauthorized move by a team that had hoped it would benefit academic researchers.

But the detailed records of searches conducted by Ms. Arnold and 657,000 other Americans, copies of which

Breaches Affecting 500 or More Individuals

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. These breaches are now posted in a new, more accessible format that allows users to search and sort the posted breaches. Additionally, this new format includes brief summaries of the breach cases that OCR has investigated and closed, as well as the names of private practice providers who have reported breaches of unsecured protected health information to the Secretary. The following breaches have been reported to the Secretary:

Show Advanced Options

Breach Report Results

	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
	Brooke Army Medical Center	TX	Healthcare Provider	1000	10/21/2009	Theft	Paper/Films
	Mid America Kidney Stone Association, LLC	MO	Healthcare Provider	1000	10/28/2009	Theft	Network Server
	Alaska Department of Health and Social Services	AK	Healthcare Provider	501	10/30/2009	Theft	Other, Other Portable Electronic Device
	Health Services for Children with Special	DC	Health	3800	11/17/2009	Loss	Laptop

			Provider				
	MD Manage (Vcarve LLC)	NJ	Business Associate	35357	10/22/2014	Unauthorized Access/Disclosure	Network Server
	Vcarve LLC d/b/a MD Manage	NJ	Business Associate	585	10/06/2014	Unauthorized Access/Disclosure	Network Server
	Sutherland Healthcare Solutions, Inc.	NJ	Business Associate	342197	05/22/2014	Theft	Email, Laptop
	N/A	NJ	Business Associate	2500	10/01/2013	Theft	Laptop
	SpaMed Solutions, LLC, Edward McMenamin President,	NJ	Business Associate	3000	08/28/2011	Theft, Unauthorized Access/Disclosure	Desktop Computer, Electronic Medical Record, Email, Laptop, Network Server, Other, Other Portable Electronic Device, Paper/Films
	Horizon Healthcare Services, Inc., doing business as Horizon Blue Cross Blue Shield of New Jersey, and its affiliates	NJ	Health Plan	1173	09/24/2015	Unauthorized Access/Disclosure	Other
	Horizon Healthcare Services, Inc., doing business as Horizon Blue Cross Blue Shield of New Jersey, and its affiliates	NJ	Business Associate	839711	01/03/2014	Theft	Laptop
	Barnabas Health Medical Group	NJ	Healthcare Provider	1100	11/05/2013	Theft	Laptop
	G&S Medical Associates, LLC	NJ	Healthcare Provider	3000	01/14/2016	Hacking/IT Incident	Desktop Computer
	Jersey City Medical Center	NJ	Healthcare Provider	1447	04/17/2015	Unauthorized Access/Disclosure	Email
	Jersey City Medical Center - Barnabas Health	NJ	Healthcare Provider	36400	08/07/2014	Loss	Other
	Inspira Health Network Inc.	NJ	Healthcare Provider	1411	02/21/2014	Theft	Desktop Computer

HIPAA and genomic data?

Technical Evaluation ■

An Evaluation of the Current State of Genomic Data Privacy Protection Technology and a Roadmap for the Future

BRADLEY A. MALIN, MS, MPHIL

Abstract The incorporation of genomic data into personal medical records poses many challenges to patient privacy. In response, various systems for preserving patient privacy in shared genomic data have been developed and deployed. Although these systems de-identify the data by removing explicit identifiers (e.g., name, address, or Social Security number) and incorporate sound security design principles, they suffer from a lack of formal modeling of inferences learnable from shared data. This report evaluates the extent to which current protection systems are capable of withstanding a range of re-identification methods, including genotype–phenotype inferences, location–visit patterns, family structures, and dictionary attacks. For a comparative re-identification analysis, the systems are mapped to a common formalism. Although there is variation in susceptibility, each system is deficient in its protection capacity. The author discovers patterns of protection failure and discusses several of the reasons why these systems are

Privacy protection approaches

- De-identification (i.e. HIPAA safe harbor)
  - Remove explicit and quasi-identifying data
- Trusted third party
  - Used for identifying subjects

  Researcher -> physician -> TTP -> researcher
  - Restricted version where 3rd party only has encrypted data

Reidentification of genomic data

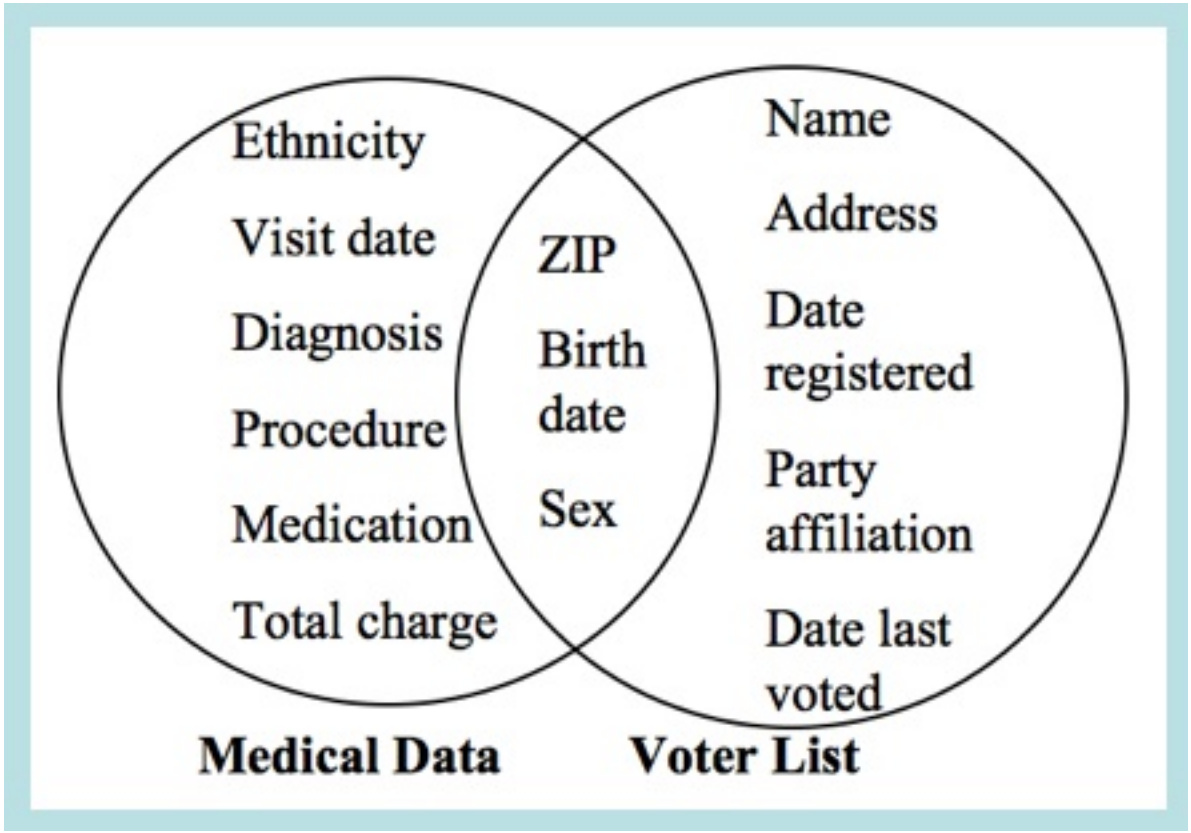
- Family structure
- Combine data
- Genotype-phenotype
- Reverse engineer pseudonymization

De-identifying data

- Bare minimum: replace all IDs with research ID, change dates, remove HIPAA identifiers
  - Should have different shift/function for each patient

- Structured data
  - Add noise
- Text
  - Manual vs statistical
- Genome
  - Generalize sequence
- Images
  - Facial blur

Limits of deidentification



"87% of the U.S. Population are uniquely identified by {date of birth, gender, ZIP}."

http://latanyasweeney.org/work/identifiability.html

Matchin
in Wash

Public Record

-State sells patient-level data
-Includes hospitalizations w/demographics, diagnoses, procedures, hospital, zipcode
-Searched newspapers for hospitalized - > articles have name and reason
"This is the same kind of information an employer may know about an employee taking a medical leave, a creditor may know about a debtor citing health concerns as a reason for tardy payments, and family, friends or neighbors may know about a patient in a hospital."

-Can combine w/public records to get age, then map to hospital data

Step 2

Information from news accident reports uniquely and exactly matched medical records in publicly available Washington State health data in 43% of the cases, thereby putting names to patient records.

Sweeney L. Matching Known Patients to Health Records in Washington State Data. Harvard University. Data Privacy Lab. 1089-1. June 2013. PDF

http://thedatamap.org/risks.html

Order CHARS data

Public use CHARS data set

This de-identified data set is available free of charge.

Order public use CHARS data

Limited CHARS data set

Inpatient limited files and observation limited files are available for purchase and are subject to a data use agreement. Data users may purchase one or several years' data.

Order limited CHARS data

Confidential CHARS data set

This set is protected by state privacy regulations.

Please contact DOH DCHS Data Requests for more information.

Comprehensive Hospital Abstract Reporting System (CHARS) Current files contain 2014 data. 2015 data expected June 2016.	**Inpatient Limited* Files, 1987 through 2014** Coded hospital inpatient discharge information (derived from billing systems). Contains age, sex, zip code and billed charges, diagnosis and procedure codes, etc. *Potentially identifiable. Includes indirect patient identifiers.	Order Form (Word) Data Sharing Agreement Information Sheet (Word)	$50 per Year	Standard Reports by Year File Layout and Data Dictionary (Excel) Annual Data Notes CHARS Download Information
	Observation Limited Files, 2009 through 2014 Coded hospital observation data. Contains age, sex, zip code and billed charges, diagnosis and procedure codes, etc. Includes indirect patient identifiers	Order Form (Word) Data Sharing Agreement Information Sheet (Word)	$50 per Year	Standard Reports by Year File Layout and Data Dictionary (Excel) Annual Data Notes
	CHARS Revisit File, 2008 through 2014 Linked inpatient hospital discharge information. This file can be used to count individuals who have been hospitalized more than once in this time period. Requires inpatient/observation limited files for demographic/diagnosis information	Order Form (Word)	$50 per Year	Data Dictionary (Excel)
	CHARS Public Use File, 2014	CHARS	No	Data

Table 2. A summary of successful re-identification attacks on the evaluation criteria.

ID	Study	Pub Year [§]	Health data included?	Profession of adversary	Number of individuals re-identified	Country of adversary	Proper de-identification of attacked data ?	Re-identification verified ?
A	[70]	2001	No	Researchers	29 of 273	Germany	"Factually anonymous"	Yes (records containing insurance numbers only)
B	[71]	2001	No	Researchers	75% of 11,000	USA	Direct identifiers removed	No
C	[67]	2002	Yes	Researcher	1 of 135,000	USA	Removal of names and addresses	Yes
	[56]	2003	No	Researchers	219 unique matches, 112 with 2 possibilities, 8 confirmed	UK	Yes	Verified matches, but not identities
D	[22]	2006	No	Journalist	1 of 657,000	USA	No	Yes (with individual)
E	[72]	2006	Yes	Researchers	79% of 550	USA	No	Verified (with original data set)
	[73]	2006	No	Researchers	Of 133 users, 60% of those who mention at least 8 movies	USA	Direct identifiers removed	No
F	[52]	2006	Yes	Expert Witness	18 of 20	USA	Only type of cancer, zip code and date of diagnosis included in request	Yes (verified by the Department of Health)
G	[74]	2007	No	Researchers	2,400 of 4.4 million	USA	Identifying information removed	Verified using original data
	[53]	2007	Yes	Broadcaster	1	Canada	Direct Identifiers removed & possibly other unknown de-id methods used	Yes
H	[23]	2008	No	Researchers	2 of 50	USA	Direct identifiers removed+maybe perturbation	No
I	[75]	2009	Yes	Researcher	1 of 3,510	Canada	Direct identifiers removed	Yes
J	[76]	2009	No	Researchers	30.8% of 150 pairs of nodes	USA	Identifying information removed	Verified using ground-truth mapping of the 2 networks
K	[57,58][‡‡‡]	2010	Yes	Researchers	2 of 15,000	USA	Yes - HIPAA Safe Harbor	Yes

(§This is the first year that the report or article appears. Some of the reports we cite have been updated at later dates. Some reports describe re-identification attacks that may have occurred in earlier years. ‡ Since the appearance of the original results in 2010 a second article has been published more recently).
doi:10.1371/journal.pone.0028071.t002

El Emam K, Jonker E, Arbuckle L, Malin B (2011) A Systematic Review of Re-Identification Attacks on Health Data. PLoS ONE 6(12): e28071. doi: 10.1371/journal.pone.0028071
http://journals.plos.org/plosone/article?id=info:doi/10.1371/journal.pone.0028071

Are cells really anonymous?

Science
AAAS

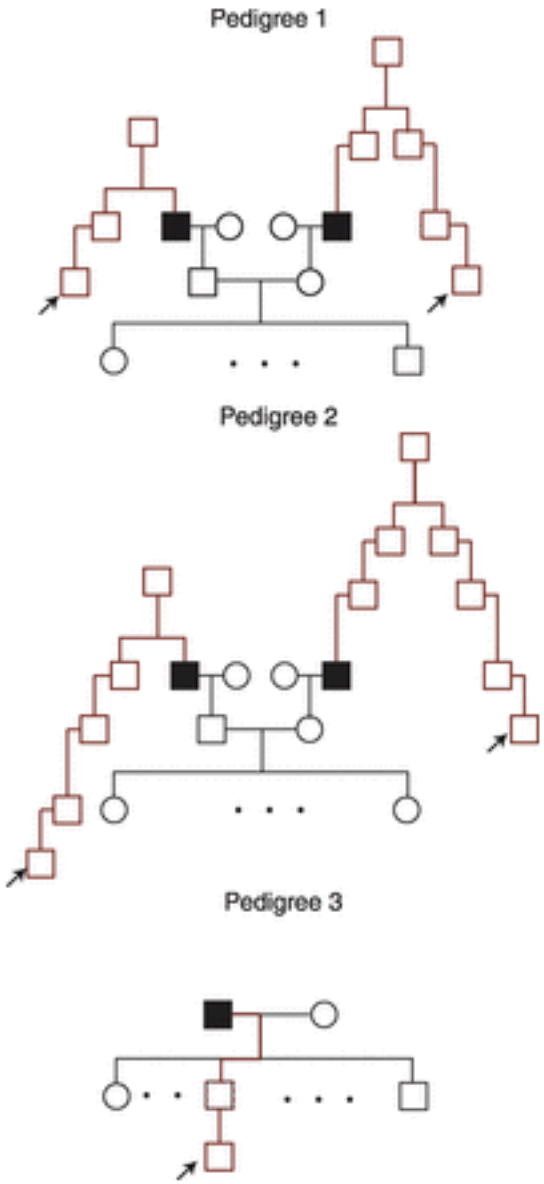
Identifying Personal Genomes by Surname Inference
Melissa Gymrek *et al.*
Science **339**, 321 (2013);
DOI: 10.1126/science.1229566

Sharing sequencing data sets without identifiers has become a common practice in genomics. Here, we report that surnames can be recovered from personal genomes by profiling short tandem repeats on the Y chromosome (Y-STRs) and querying recreational genetic genealogy databases. We show that a combination of a surname with other types of metadata, such as age and state, can be used to triangulate the identity of the target. A key feature of this technique is that it entirely relies on free, publicly accessible Internet resources. We quantitatively analyze the probability of identification for U.S. males. We further demonstrate the feasibility of this technique by tracing back with high probability the identities of multiple participants in public sequencing projects.

Table 1. Comparison of CEU identification cases.

Feature	Pedigree 1		Pedigree 2		Pedigree 3
Genome for surname recovery	Paternal grandfather	Maternal grandfather	Paternal grandfather	Maternal grandfather	Father
Surname freq. in U.S.*	Rare	Rare	Common	Rare	Rare
Meioses between target and source	3	5	5	7	2
Relationship between target and source	Nephew	First cousin once removed	Great-great nephew	Second cousin once removed	Grandchild
Supporting evidence	State of residency, pedigree structure, age, and maiden name are the same		State of residency, pedigree structure, age, and maiden name are the same		State of residency, pedigree structure are the same (ages are not given)
P (random match)†	$<5 \times 10^{-9}$		$<5 \times 10^{-6}$		$<10^{-5}$

*Common: surnames with a prevalence of $>10^{-4}$; Rare: surnames with a prevalence of $\leq 10^{-4}$. †The estimated probability of finding at least one family with the same characteristics after scanning all Utah households.



View larger version:
» In this window » In a new window
» Download PowerPoint Slide for Teaching

Fig. 3.

Illustrations of the three CEU pedigrees (black) showing how genetic information from distant patrilineal relatives (arrow; red, patrilineal lines) can identify individuals. Filled squares represent sequenced individuals. To respect the privacy of these families, only abbreviated versions are presented. The sex of the CEU grandchildren was randomized. The numbers of grandchildren are not given.

Found on the Web, With DNA: a Boy's Father

By Rob Stein
Washington Post Staff Writer
Sunday, November 13, 2005

Like many children whose mothers used an anonymous sperm donor, the 15-year-old boy longed for any shred of information about his biological father. But, uniquely, this resourceful teenager decided to try exploiting the latest in genetic technology and the sleuthing powers of the Internet in his quest.

By submitting a DNA sample to a commercial genetic database service designed to help people draw their family tree, the youth found a crucial clue that quickly enabled him to track down his long-sought parent.

"I was stunned," said Wendy Kramer, whose online registry for children trying to find anonymous donors of sperm or egg helped lead the teenager to his father. "This had never been done before. No one knew you could get a DNA test and find your donor."

While welcomed by advocates of children trying to locate anonymous donors, the case -- apparently the first of its kind -- has raised alarm among sperm banks and some medical ethicists. They are concerned it might start a trend that could violate the privacy of thousands of sperm donors and discourage future ones.

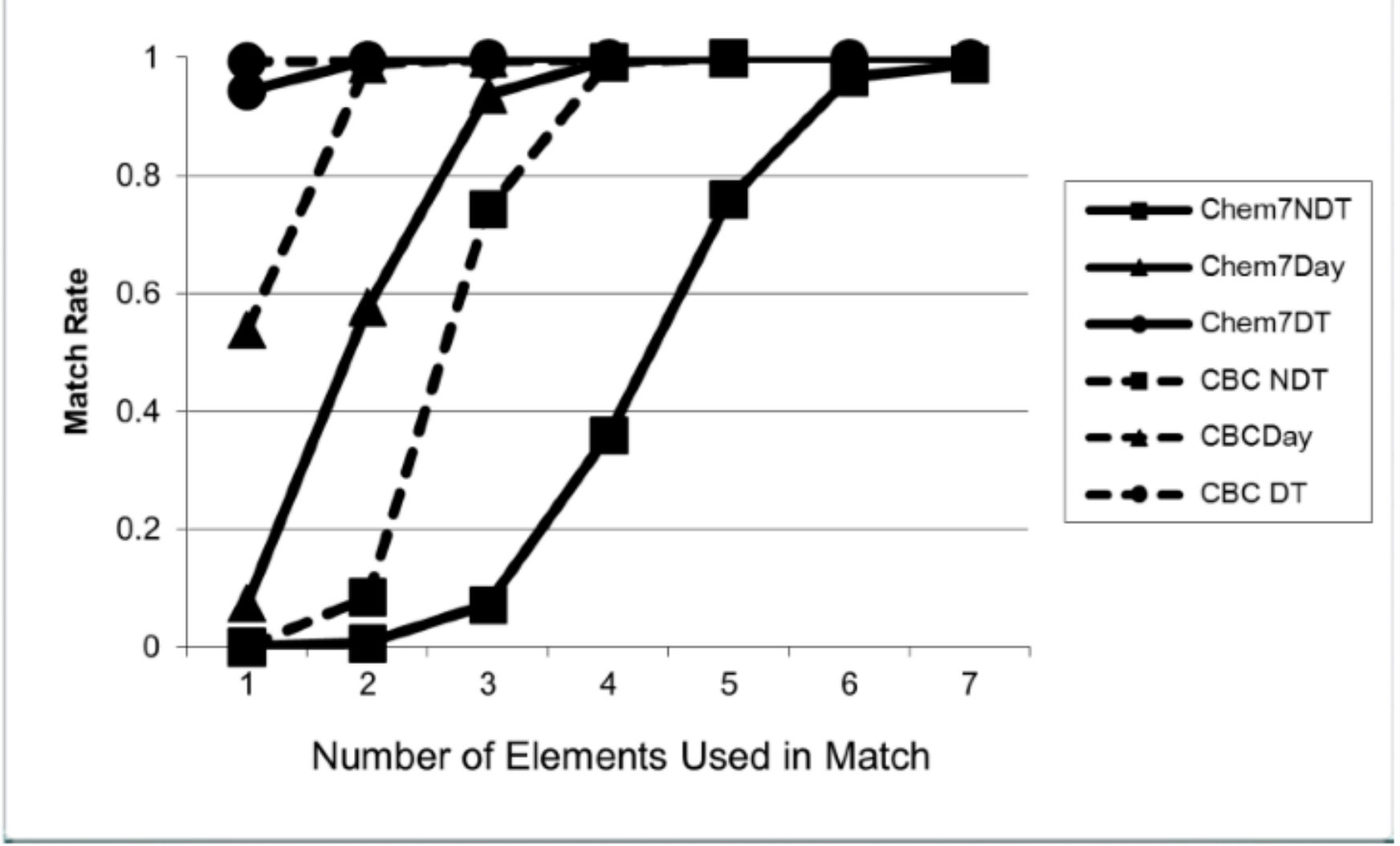


Fig. 2 Match Rate (MR) for CBC and Chem7, without date or time information (NDT), with date-only (Day) and with date and time (DT). The graphs show that with no date information (circle), data are relatively unique (low MR) when a small number of elements are available for matching, but rapidly become unique (high MR) when more of the panel is available. While addition of date and date and time increase the MR with few elements (moving the graphs to the left), there is essentially no effect when most or all of the panel is available, since MR is high for all three cases. Note that CBC matches one to five elements, while Chem7 matches one to seven elements.

Identifying Participants in the Personal Genome Project by Name

	Name	Voter	Public	*Totals*
Name	80	12	17	*109*
Voter Data	12	45	74	*131*
Public Records	17	74	65	*156*
Totals	*109*	*131*	*156*	

Table 1. Discrimination of strategies. Values report the number of names specific to the strategy (e.g., embedded names contributing 74 names not otherwise found) or in common across strategies (e.g., 17 names found in both embedded names and Public Records).

	Wrong	Total	Correct%
Name	19	103	82%
Voter Data	9	130	93%
Public Records	20	156	87%

Table 2. Correctness of different re-identification strategies. Errors in matching embedded names and other strategies are due primarily to uses of nicknames rather than real names.

We linke
publicly available
Project. These pr
information, incl
procedures and
information, such
code. By linking a
as voter lists, a
attached documen
percent of the pro
Our ability to le
demographics, no
old vulnerability
minimal loss of
technical remedi
demographics to make better decisions.

quently harmed
d and take away
haring decisions,
dual choice. To
ple need an
ways technology

Genome Project
genotypic and
,000 informed
y online in an
mation provided
in the PGP includes DNA information, behavioral

Good practices

- Physical security
  - Locked cabinet/office, don't print records and leave them in common area/on desk
  - Automatically lock computer after 5 minutes inactivity
- Encryption
  - Losing laptop/thumb drive, sending hard drive for repair can be disastrous
- Restricted access to servers with PHI
- PHI in segregated, labeled, directories
- Data usage agreements

Pervasive Health, Consumer Informatics, mHealth

Common theme: decentralized patient centered technologies

- PHR
- Instrumented environments
- Wearable and implantable sensors
- Mobile apps
- Telemedicine

Why mobile?

Chronic disease accounts for 70% of healthcare spending in US

Outside clinical environment

Major burden on patients

Usual view of health IT

- Hospital or clinic-based
- Assisting clinician
- Sporadic encounters
- Better treatment

Chronic disease + maintaining health…

- ~~Hospital or clinic-based~~
- Assisting ~~clinician~~ patient/caregiver
- ~~Sporadic encounters~~
- Better ~~treatment~~ prevention/management

Benefits

- Deliver and collect information outside hospital
  - At point of need
  - Continuous (passive vs active)
  - In scenarios previously inaccessible (school, work, daily life – conditions not replicable as in-patient)
- Reach underserved populations
  - Developing countries
  - Low SES


10:30 AM | 3/11
mmol
L
5.2
Before Meal
Reminder
Notes


5.6


54.7


4:20 PM
Back
Blood pressure
June 1, 2013 4:30 PM
SYS
120
DIA
78
PULSE
72
iHealth


iHealth


95
400
350
300
250
200
150
100
50
11:00 AM
12:00 PM
12:16 PM
dexcom

(Drag to spin)


GARMIN
History
Training
Setup
Where To?

Example uses cases

- Delivering information
  - Text messages related to allergies or pregnancy
- Improve treatment adherence
  - Medication reminder systems
- Facilitate health
  - Nutrition, physical activity, weight loss

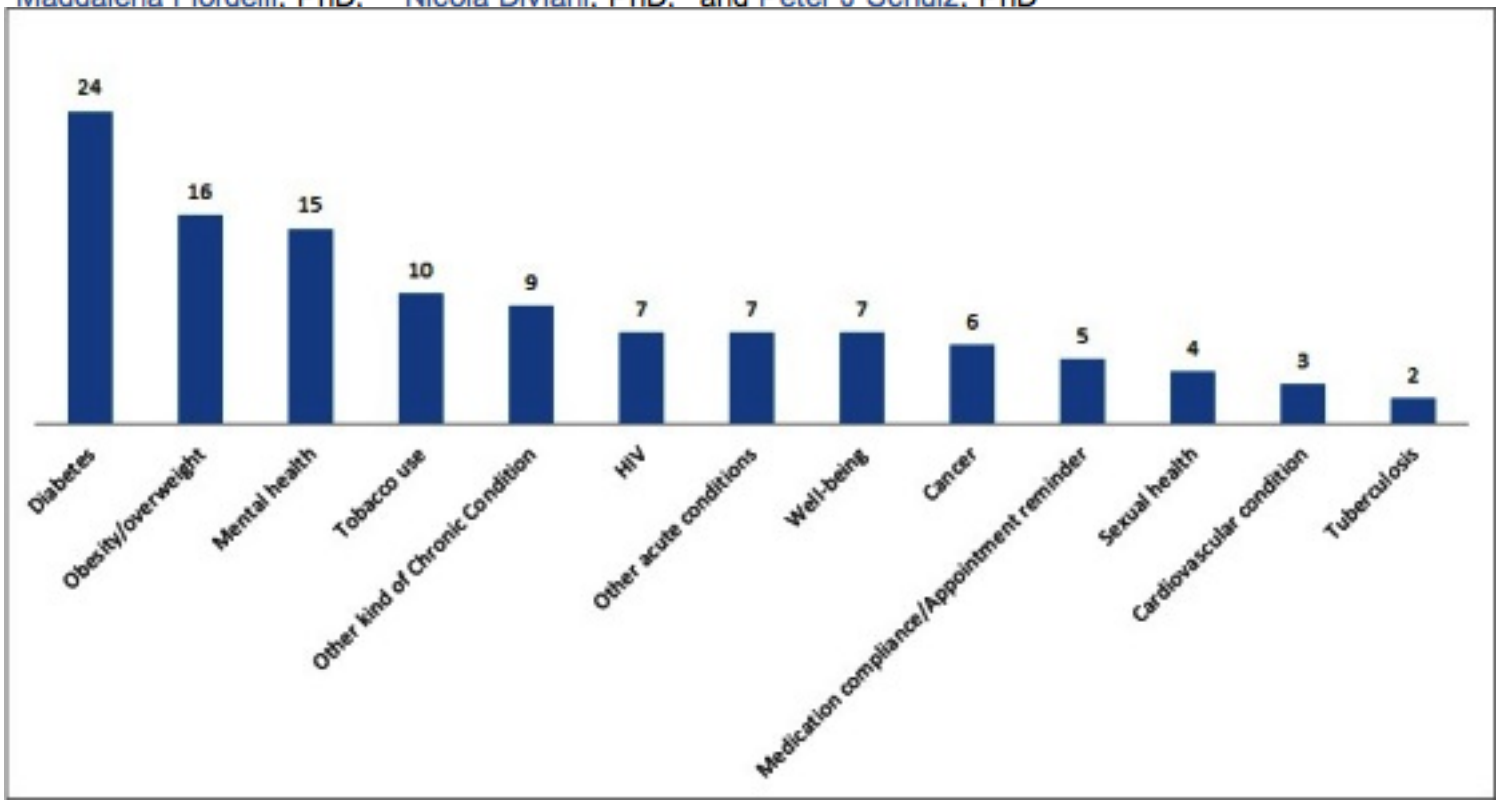
J Med Internet Res. May 2013; 15(5): e95.
Published online May 21, 2013. doi: 10.2196/jmir.2430
PMCID: PMC3668610

Mapping mHealth Research: A Decade of Evolution

Monitoring Editor: Gunther Eysenbach

Reviewed by Zaher Hajar and Robyn Whittaker

Maddalena Fiordelli, PhD,[✉1] Nicola Diviani, PhD,[1] and Peter J Schulz, PhD[1]



To provide a comprehensive view of the field of mHealth research to date and to understand whether and how the new generation of smartphones has triggered research, since their introduction 5 years ago. Specifically, we focused on studies aiming to evaluate the impact of mobile phones on health, and we sought to identify the main areas of health care delivery where mobile technologies can have an impact.

VIEWPOINT

Wearable Devices as Facilitators, Not Drivers, of Health Behavior Change

Mitesh S. Patel, MD, MBA, MS
Philadelphia VA Medical Center, University of Pennsylvania, Philadelphia.

David A. Asch, MD, MBA
Philadelphia VA Medical Center, University of Pennsylvania, Philadelphia.

Kevin G. Volpp, MD, PhD
Philadelphia VA Medical Center, University of Pennsylvania, Philadelphia.

Author Reading at jama.com

Several large technology companies including Apple, Google, and Samsung are entering the expanding market of population health with the introduction of wearable devices. This technology, worn in clothing or acces-

According to one survey (n = 6223),more than half of individuals who purchased a wearable device stop using it and, of these, one third did so before 6 months.5

these devices are increasing in popularity, little evidence suggests that they are bridging that gap.

Key issues:
1. Motivation of user. Cost/access. Who will benefit?
2. Will they continue using it? Why?
3. Is it accurate? Many sensors not yet validated
4. How is feedback presented to user?

may justify that promise, but less because of their technology and more because of the behavioral change strategies that can be designed around them.

Most health-related behaviors such as eating well and exercising regularly could lead to meaningful improvements in population health only if they are sus-

Identifying and Addressing the Gaps

Using wearable devices to effectively promote health behavior change is a complex, multistep process. First, a person must be motivated enough to want a device and

hallenge, because some de-

ollars. Perhaps for these rea-

m to appeal to groups that

a survey of wearable device

selves as "early adopters of

nger than 35 years, and 29%

$100 000 annually.[4] The individuals who might have the most to gain from these devices are likely to be older and less affluent. To better

vices must be

chanisms are

rers might pay

adhere to their

ificant down-

s that demon-

a manner simi-

Second, once a device is acquired, a person needs to remember to wear it and occasionally recharge it—additional behaviors required from individuals who may have a difficult time already. Many wearable devices require data to be sent to a phone or computer, adding additional steps and more equipment. According to one

Challenges (aka opportunities)

- Data quality (vs device cost)
- Reflection vs recommendations
- Longterm adoption/motivation

Use case: medication adherence

- Not filling prescription
- Not taking as prescribed
- Not completing treatment

Journal of Medical Internet Research
ISSN 1438-8871
The leading peer-reviewed journal for health and healthcare in the Internet age
About Search Review Archive Current Issue Submit Membership Editorial Board

J Med Internet Res. 2012 Mar-Apr; 14(2): e51.
PMCID: PMC3376506
Published online 2012 Apr 5. doi: 10.2196/jmir.2015

Improving Adherence to Antiretroviral Therapy for Youth Living with HIV/AIDS: A Pilot Study Using Personalized, Interactive, Daily Text Message Reminders

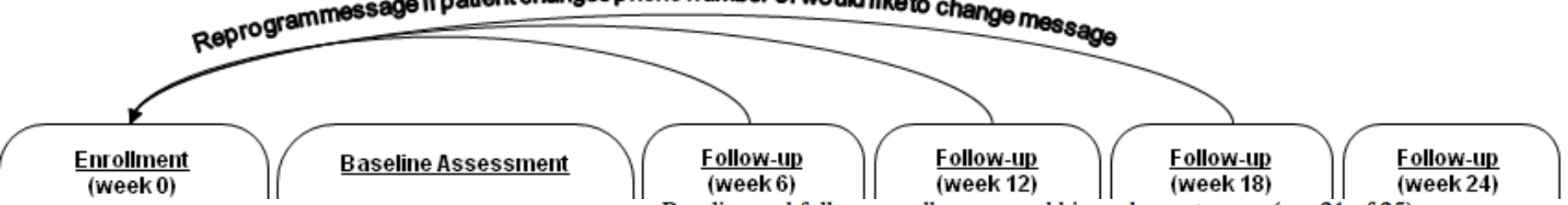
Monitoring Editor: Gunther Eysenbach

Reviewed by Karen MacDonell

Nadia Dowshen, MD,[✉12] Lisa M Kuhns, MPH, PhD,[3,4] Amy Johnson, MSW,[3] Brian James Holoyda, BS,[4] and Robert Garofalo, MPH, MD[3,4]

[1]Craig-Dalsimer Division of Adolescent Medicine, The Children's Hospital of Philadelphia, Philadelphia, PA, United States
[2]School of Medicine, University of Pennsylvania, Philadelphia, PA, United States
[3]Division of General Academic Pediatrics, Children's Memorial Hospital, Chicago, IL, United States
[4]Feinberg School of Medicine, Northwestern University, Chicago, IL, United States
Nadia Dowshen, Craig-Dalsimer Division of Adolescent Medicine, The Children's Hospital of Philadelphia, 3535 Market St, Rm 1542, Philadelphia, PA, 19104, United States, Phone: 1 267 426 2591, Fax: 1 267 426 0380, Email: dowshenn@email.chop.edu.

Author information ► Article notes ► Copyright and License information ►

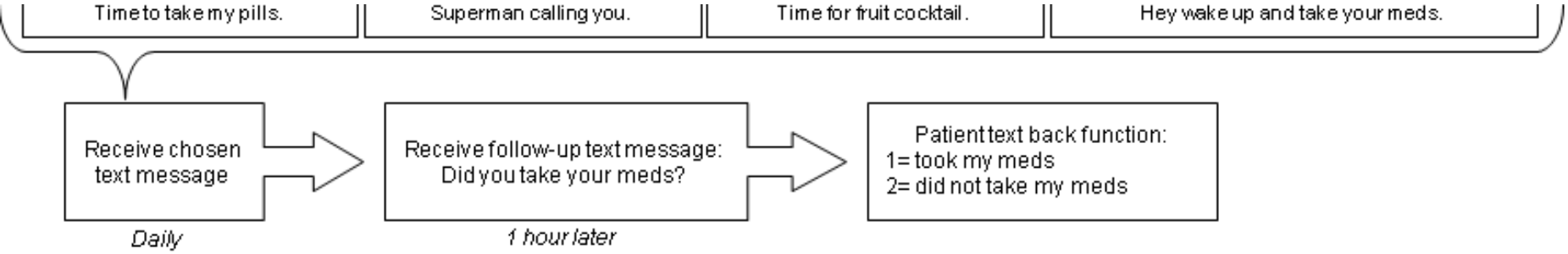


Baseline and follow-up adherence and biomarker outcomes (n = 21 of 25).

Outcome measure	Baseline		12 weeks			24 weeks		
	Mean	SD	Mean	SD	*P* value	Mean	SD	*P* value
Adherence (VAS[a])	74.7	16.5	93.3	6.6	<.001	93.1	7.7	<.001
Prior 4-day adherence (ACTG[b])	2.33	1.1	3.24	0.4	.002	3.19	0.9	.005
Viral load	2750.2	8930.8	240.5	521.1	.26	28.5	47.5	.23
CD4 cell count	501.5	239.2	552.8	234.3	.12	544.8	228.7	.37

[a] Visual analog scale.

[b] AIDS Clinical Trials Group. Response scale: 0 = never, 4 = all the time.



Antiretroviral Therapy Adherence and Viral Suppression in HIV-Infected Drug Users: Comparison of Self-Report and Electronic Monitoring

Julia H. Arnsten,[1–3] Penelope A. Demas,[1] Homayoon Farzadegan,[6] Richard W. Grant,[1] Marc N. Gourevitch,[1–3] Chee-Jen Chang,[1,4] Donna Buono,[1] Haftan Eckholdt,[5] Andrea A. Howard,[1,2] and Ellie E. Schoenbaum[1,2]

[1]AIDS Research Program, Department of Epidemiology and Social Medicine, [2]Department of Medicine, [3]Division of Substance Abuse, Department of Psychiatry and Behavioral Sciences, [4]Division of Biostatistics, Department of Epidemiology and Social Medicine, and [5]Division of Biometry, Department of Neurology, Montefiore Medical Center and Albert Einstein College of Medicine, Bronx, New York; and [6]Department of Epidemiology, Johns Hopkins University School of Hygiene and Public Health, Baltimore, Maryland

To compare electronically monitored (MEMS) with self-reported adherence in drug users, including the impact of adherence on HIV load, we conducted a 6-month observational study of 67 antiretroviral-experienced current and former drug users. Adherence (percentage of doses taken as prescribed) was calculated for both the day and the week preceding each of 6 research visits. Mean self-reported 1-day adherence was 79% (median, 86%), and mean self-reported 1-week adherence was 78% (median, 85%). Mean MEMS 1-day adherence was 57% (median, 52%), and mean MEMS 1-week adherence was 53% (median, 49%). One-day and 1-week estimates were highly correlated ($r > .8$ for both measures). Both self-reported and MEMS adherence were correlated with concurrent HIV load ($r = .43–.60$), but the likelihood of achieving virologic suppression was greater if MEMS adherence was high than if self-reported adherence was high. We conclude that self-reported adherence is higher than MEMS adherence, but a strong relationship exists between both measures and virus load. However, electronic monitoring is more sensitive than self-report for the detection of nonadherence and should be used in adherence intervention studies.

Table 2

Correlation between 1-day and 1-week self-reported (SR) and electronically monitored (MEMS) adherence at each visit.

Visit	SR adherence				MEMS adherence			
	No. of subjects	One-day SR, mean ± SD	One-week SR, mean ± SD	r[a]	No. of subjects	One-day MEMS, mean ± SD	One-week MEMS, mean ± SD	r[a]
2	63	75.6 ± 34.1	80.9 ± 23.3	.66	60	66.4 ± 42.4	60.3 ± 35.9	.77
3	59	85.3 ± 28.3	78.3 ± 26.7	.70	58	57.1 ± 41.3	52.2 ± 37.0	.80
4	56	82.9 ± 31.0	80.1 ± 23.0	.56	54	54.2 ± 40.1	54.8 ± 35.8	.66
5	55	84.3 ± 31.8	81.1 ± 27.9	.62	49	63.9 ± 41.9	54.9 ± 39.6	.74
6	50	83.2 ± 30.8	86.6 ± 22.6	.86	45	56.3 ± 36.8	53.8 ± 41.2	.86
7	49	80.4 ± 33.9	81.1 ± 29.7	.79	41	56.1 ± 38.2	55.6 ± 43.6	.86
Total	63	79.1 ± 22.5	78.1 ± 22.1	.81	60	57.3 ± 31.9	53.4 ± 33.9	.91

[a] $p = .0001$ for all correlation coefficients.

GlowCap®

remembers so you don't have to.

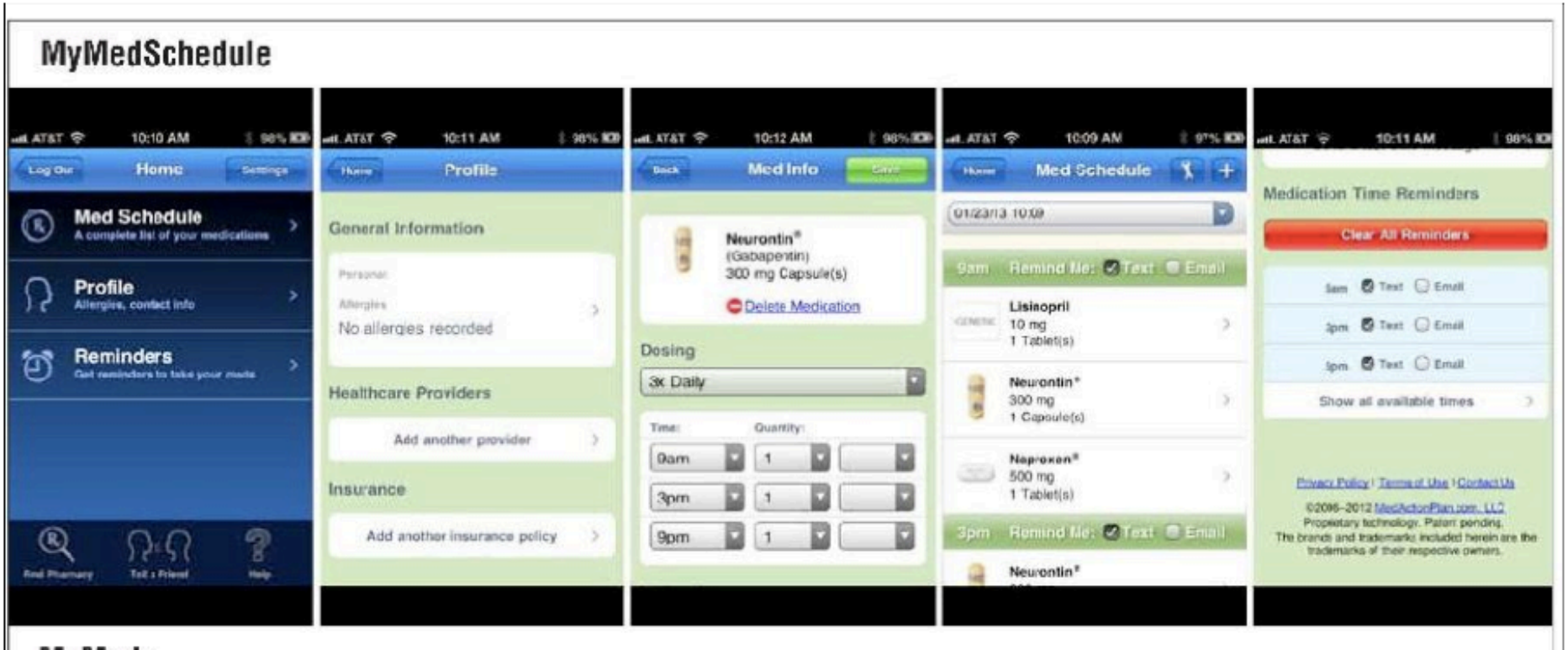
Discover a new approach to medication management through reminders, social feedbacks, financial incentives and automatic refills.
Inside the cap, a chip monitors when the pill bottle is opened and wirelessly relays alerts, through the AT&T Mobile Broadband Network, to you or your caregiver. A push button at the base of the lid makes refills easier than ever.

Vitality is dedicated to improving the management of medication for patients and healthcare professionals.

Soon the GlowPack ™ will complement the GlowCap® to monitor adherence for sirups, inhalers, ointments and blisters.

Example: medication reminder app

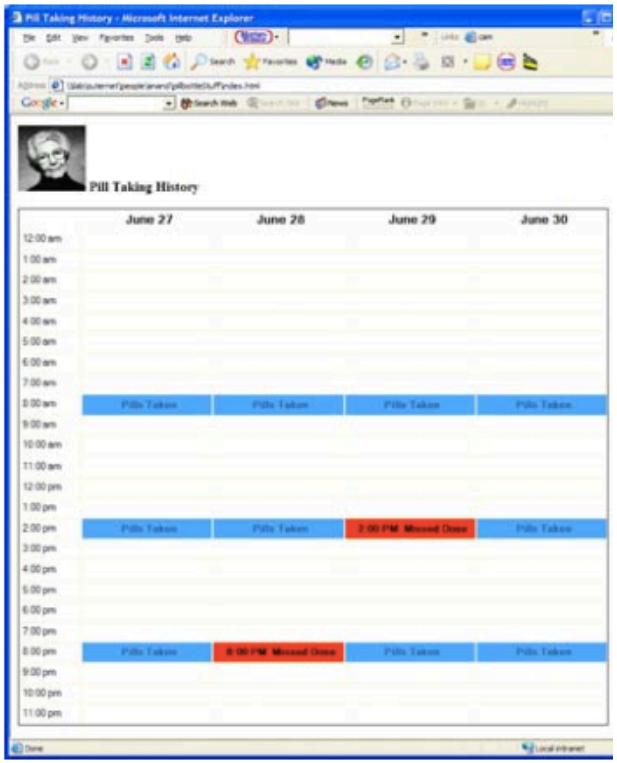
- No new hardware, portable
- Challenges:
  - Access



Example: home-based sensor

1a: Pill Bottle and stand

1b: Montior



1c: Web-based medication summary

Figure 1. Components of the system

Don't Forget Your Pill! Designing Effective Medication Reminder Apps That Support Users' Daily Routines

Katarzyna Stawarz
UCL Interaction Centre
Gower Street
London, WC1E 6BT, UK
k.stawarz@cs.ucl.ac.uk

Anna L Cox
UCL Interaction Centre
Gower Street
London, WC1E 6BT, UK
anna.cox@ucl.ac.uk

Ann Blandford
UCL Interaction Centre
Gower Street
London, WC1E 6BT, UK
a.blandford@ucl.ac.uk

ABSTRACT
Despite the fact that a third of all cases of unintentional medication non-adherence are caused by simple forgetfulness, the majority of interventions neglect this issue. Even though patients have access to smartphone applications ("apps") designed to help them remember medication, neither their quality nor effectiveness has been evaluated yet. We report the findings of a functionality review of 229 medication reminder apps and a thematic analysis of their 1,012 user reviews. Our research highlights the gap between the theory and practice: while the literature shows that many medication regimens are habitual in nature and the presence of daily routines supports remembering, existing apps rely on timer-based reminders. To address this disparity, we present design requirements for building medication reminders that support the routine aspect of

adherence and their aim is to educate people and change their attitudes and beliefs [18]. However, even motivated people can forget: forgetfulness accounts for 30% of cases of unintentional non-adherence [43] and around one million unwanted pregnancies each year are the result of non-adherence [37] and irregular use of the contraceptive pill ("the Pill"), with forgetfulness as one of the main causes [25, 41]. And yet, interventions explicitly addressing forgetfulness, especially for preventative therapies such as oral contraception, are not only few and far between, but also tend to focus on reminders alerting people to take their medication at a specified time [18, 46]. This focus on timed alerts disregards the fact that time-based tasks are more difficult to remember than tasks related to routine actions [34] and many medication regimens are habitual tasks that could be easily incorporated into a daily routine, which in

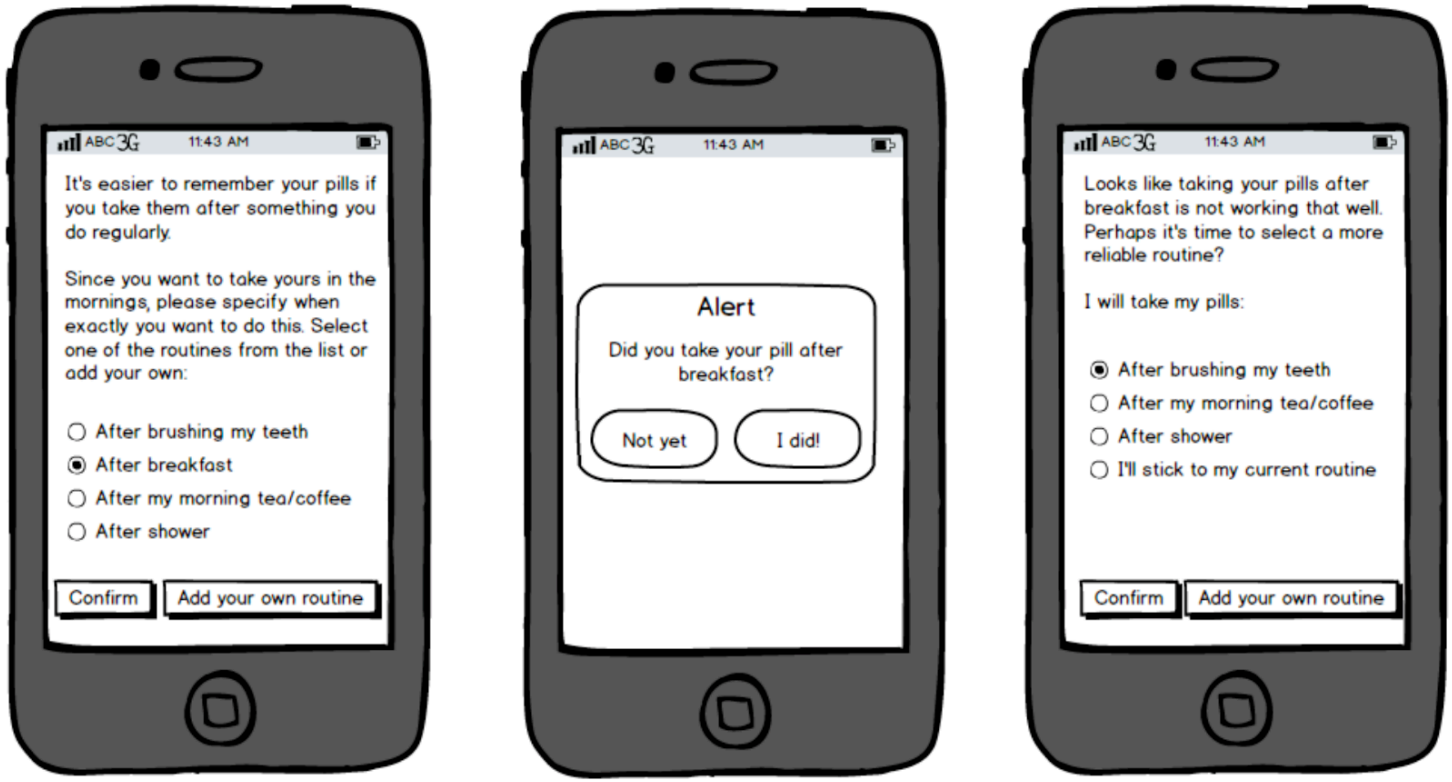


Figure 2. Sketches of a hypothetical app supporting routines. From the left: (a) setting up a new routine, (b) an example of a back-up notification, (c) adjusting the routine to user's behavior