Elisabeth Hildt and Kelly Laas:

Models of practice: Informed consent

How far do informed consent-related principles and standards play a role in data management and review?

Definition: Informed consent

“medical: a formal agreement that a patient signs to give permission for a medical procedure (such as surgery) after having been told about the risks, benefits, etc.”

Relevant components of informed consent:

- Transparent information on the relevant aspects has to be provided.
- The (written) informed consent has a gatekeeper function. It is to be given before anything else happens. Waiver is possible.
- The participant has to get adequate information on the benefits and risks.
- A participant can quit the study at any time without negative implications. On request of the participant, the data collected has to be destroyed.
- Type and amount of data collected: The data collected is to be used only for the purpose or purposes specified.
- Data sharing: If the data is to be used in additional contexts, informed consent is needed.
- Data collected is stored only for a limited duration of time that is clearly specified. Afterwards the data is destroyed.
- Special protection for non-competent individuals (children etc.).

Transparent information on the relevant aspects has to be provided

Of central relevance. Challenges:

- Long text with a lot of details that nobody reads, people just click on it to get rid of it.
- Information is not given in a transparent way
- Users have to be aware of data collection

“Transparency:

• Develop clearly defined and accessible information on the purposes, processes, procedures and governance frameworks for data sharing. Such information should be presented in a way that is understandable and accessible in both digital and non-digital formats.
• Provide clear information on the purpose, collection, use and exchange of genomic and health-related data, including, but not limited to: data transfer to third parties; international transfer of data; terms of access; duration of data storage; identifiability of individuals and data and limits to anonymity or confidentiality of data; communication of results to individuals and/or groups; oversight of downstream uses of data; commercial involvement; proprietary claims; and processes of withdrawal from data sharing.”

Global Alliance for Genomics and Health: Framework for Responsible Sharing of Genomic and Health-related Data
“Note that consent requires that users have been provided with clear and comprehensible information first. Key information shall not be embedded in lengthy legal text.”

Germany, Federal Ministry of Justice and Consumer Protection: Draft Code of Conduct on Privacy for Mobile Health Applications

“II. TRANSPARENCY A. Third Party and Service Provider Notice
1. Third Party and Service Provider Privacy Notice — Third Parties and Service Providers should give clear, meaningful, and prominent notice on their own Web sites that describes their Online Behavioral Advertising data collection and use practices. Such notice should include clear descriptions of the following:
(a) The types of data collected online, including any PII for Online Behavioral Advertising purposes;
(b) The uses of such data, including whether the data will be transferred to a non-Affiliate for Online Behavioral Advertising purposes;
(c) An easy to use mechanism for exercising choice with respect to the collection and use of the data for Online Behavioral Advertising purposes or to the transfer of such data to a non-Affiliate for such purpose; and
(d) The fact that the entity adheres to these Principles.

2. Third Party Enhanced Notice to Consumers — In addition to providing notice as described in (1), Third parties should provide enhanced notice as set forth below in (a) or (b):
(a) Third Party Advertisement Notice — Third Parties should provide notice of the collection of data through a clear, meaningful, and prominent link to a disclosure described in II.A.(1):
(i) In or around the advertisement delivered on the Web page where data is collected; or
(ii) On the Web page where the data is collected if there is an arrangement with the First Party for the provision of such notice.
((…))

Interactive Advertising Bureau: IAB Code of Conduct

The (written) informed consent has a gatekeeper function. It is to be given before anything else happens. Waiver is possible

Of central relevance. Challenges:
- It may not be feasible to obtain consent
- Parties assume tacit consent
- Only opt-out options are offered of which users may not be aware

“There are justifiable reasons why it may be impracticable for research to be carried out without a waiver or alteration of the informed consent process. Because of the difficulty in identifying all individuals from whom consent should be sought or in practicably obtaining consent, researchers or REBs may frequently conclude that seeking a waiver of informed consent or waiver of documentation of informed consent are the only options. For example, it may be infeasible to identify, or obtain consent from millions of users whose everyday communication generates traffic across a heavily aggregated backbone link in a traffic modeling study. Or it can be
impossible to attempt to inform the owners of hundreds of thousands of compromised home computers that are being used as a single instrument of criminal activity (i.e., a botnet) under study. The Common Rule criteria for a waiver of documentation of informed consent in minimal or no-risk situations allows for less formal consent than a signed consent form, including verbal consent from a legally authorized representative rather than the research subjects themselves. REBs may also require some form of notification to research subjects, even if the REB does not require signed consent forms.”


“6. Options and Informed Consent ((…)) The default approach/setting should be that users are opted out of library services until they explicitly choose to opt in. In cases where a user opts in to a specific service, they should have the choice to opt out at a later date, in particular when privacy policies change, and at that time have the option to delete data as outlined in “Access to One’s Own User Data” (item 10 below).”


“Consent Moreover, contrary to traditional thinking, not all human behaviour can be explained by economic principles which assume that human beings are entirely rational and sensitive to economic incentives. This is relevant to the future role of consent by the individual to the processing of personal information about him or him. Under EU law, consent is not the only legitimate basis for most processing. Even where consent plays an important role, it does not absolve controllers from their accountability for what they do with the data, especially where a generalised consent to processing for a broad range of purposes has been obtained.”

European Data Protection Supervisor Opinion 4/2015: Towards a new digital ethics

“III. CONSUMER CONTROL A. Third Party Choice for Behavioral Advertising

A Third Party should provide consumers with the ability to exercise choice with respect to the collection and use of data for Online Behavioral Advertising purposes or the transfer of such data to a non-Affiliate for such purpose. Such choice should be available from the notice described in II.A.(2)(a); from the industry-developed Web page(s) as set forth in II.A.2.(b)(i); or from the Third Party’s disclosure linked to from the page where the Third Party is individually listed as set forth in II.A.2.(b)(ii).”

Interactive Advertising Bureau, IAB Code of Conduct

“The PrivacySIG is a Special-Interest-Group type of association formed by companies which are active in the field of retail intelligence, specifically the collection, storage or processing of foot traffic and visitor flow in retail environments. The companies employ wireless technologies to gather statistical data for use by its customers.
Definition of data collection
The data collected by members of the SIG is based on the presence of consumer devices (e.g. smart phones) in and around a retail shop. The presence is detected through sensors installed in the store (e.g. WiFi or Bluetooth enabled devices). The unique identifiers transmitted by devices are pseudonymised and then aggregated and used to generate analytics data.

2. Signalling to consumers
Even though no personal information is being tracked, we believe in transparency and consider the shopper whose presence is being captured as a key stakeholder in our businesses. In order to promote transparency to all parties involved, the companies in the SIG will supply its customers (e.g. the retailers) with signatory material such as stickers. These are designated to be deployed in store and at store entrances to signal to the shopper that Retail Intelligence is being practised around this location.

8. Consumer Choice/ Opt out
The organisation provides an opt-out page where individuals can opt out by entering their unique MAC address. Each of the members agree to discard any information received from a MAC address that has opted out and not use it for any kind of data analytics. Each of the members shall provide instructions on their website on how to opt-out and a link to the opt-out page provided by the organisation.”
SIG Code of Conduct

Type and amount of data collected: The data collected is to be used only for the purpose specified

“Data Quality Principle
8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle
9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.”

“4. Data Collection and Use ((…)) Users’ personal data should only be used for purposes disclosed to them and to which they consent. Certain types of personal data (e.g., regarding race, gender, socioeconomic class, ability, etc.) are perceived to be more sensitive, and if they are to be held or used by a library, content, or software provider, should require higher levels of scrutiny and justification. In addition, such data require extra protection once they are collected.”
Data sharing: If the data is to be used in additional contexts, informed consent is needed

“Use Limitation Principle
10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: a) with the consent of the data subject; or b) by the authority of law.”


“7) Can I use personal data collected via my mHealth app for secondary purposes, e.g. for ‘big data’ analysis?
Any processing of personal data must be compatible with the purposes for which you originally collected the personal data, as communicated to the users of your app. Secondary processing of the data for historical, statistical or scientific purposes (assuming that these purposes were not originally communicated) is however still considered as compatible with original purposes if it is done in accordance with any national rules adopted for such secondary processing. This means that, in order to process data for such secondary purposes, you will need to determine which national laws apply, and respect any restrictions. Typically this implies that you will need to anonymise data wherever possible, or pseudonymise it.14. ((...))”

Germany, Federal Ministry of Justice and Consumer Protection: Draft Code of Conduct on Privacy for Mobile Health Applications

Data collected is stored only for a limited duration of time that is clearly specified. Afterwards the data is destroyed.

“4) How long can I keep the data?
You may not store any personal data, including data concerning health, longer than necessary for the functionalities of the app. Clear criteria must be set for the deletion of data, and these must be clearly communicated to the user, along with the consequences.
E.g. after a certain period of time of non-use of the app, data should be considered expired and must be deleted, even if the user takes no action to do so herself. At any rate data must be deleted when it is no longer relevant for the functionalities of the app.
Extended periods of retention shall only be used when continued retention is necessary for the purposes outlined to the user.
Instead of deletion, you may also choose to irreversibly anonymise data. Note however that this can be very challenging for data concerning health: it must be practically impossible for anyone to link the data to any individual.
When the app is uninstalled from a device by the user, users should be asked whether they want to delete their personal data, either locally or remotely, or both.”

Germany, Federal Ministry of Justice and Consumer Protection: Draft Code of Conduct on Privacy for Mobile Health Applications
Special protection for non-competent individuals (children etc.)

Protection for children is integrated in many Codes of Conduct. Challenge:

- How can vulnerable individuals be identified?

“VI. SENSITIVE DATA A. Children
Entities should not collect “personal information”, as defined in the Children’s Online Privacy Protection Act (“COPPA”), from children they have actual knowledge are under the age of 13 or from sites directed to children under the age of 13 for Online Behavioral Advertising, or engage in Online Behavioral Advertising directed to children they have actual knowledge are under the age of 13 except as compliant with the COPPA.”

Interactive Advertising Bureau, IAB Code of Conduct