Privacy and confidentiality in pragmatic clinical trials

Alan Rubel, J.D., Ph.D.
Associate Professor
Information School
Legal Studies Program
University of Wisconsin, Madison

Based on paper by Deven McGraw, Sarah M. Greene, Caroline S. Miner, Karen L. Staman, Mary Jane Welch, and Alan Rubel.
Working Group

• Deven McGraw, Department of Health and Human Services (formerly Manatt, Phelps & Phillips, LLP)

• Sarah M. Greene, Health Care Systems Research Network (formerly PCORI)

• Caroline S. Miner, Kaiser Permanente

• Karen L. Staman, CHB Wordsmith, Inc.

• Mary Jane Welch, Rush University Medical Center

• Alan Rubel, University of Wisconsin-Madison
Privacy and confidentiality in pragmatic clinical trials

Deven McGraw¹, Sarah M Greene², Caroline S Miner³, Karen L Staman⁴, Mary Jane Welch⁵ and Alan Rubel⁶

Abstract
With pragmatic clinical trials, an opportunity exists to answer important questions about the relative risks, burdens, and benefits of therapeutic interventions. However, concerns about protecting the privacy of this information are significant and must be balanced with the imperative to learn from the data gathered in routine clinical practice. Traditional privacy protections for research uses of identifiable information rely disproportionately on informed consent or authorizations, based on a presumption that this is necessary to fulfill ethical principles of respect for persons. But frequently, the ideal of informed consent is not realized in its implementation. Moreover, the principle of respect for persons—which encompasses their interests in health information privacy—can be honored through other mechanisms. Data anonymization also plays a role in protecting privacy but is not suitable for all research, particularly pragmatic clinical trials. In this article, we explore both the ethical foundation and regulatory framework intended to protect privacy in pragmatic clinical trials. We then review examples of novel approaches to respecting persons in research that may have the added benefit of honoring patient privacy considerations.

Keywords
Privacy, pragmatic clinical trials, autonomy, respect for persons, fair information practice principles
Overview

• Consider the problem
• Values underwriting privacy
• Fair Information Practice Principles (FIPPs)
• Regulatory Framework
• Some models and recommendations
PCTs and Privacy

• PCTs capable of harnessing proliferation of health information at point of care to investigate questions regarding comparative balance of benefits, burdens, and risks of health interventions.

• Yet, patients consistently express concerns about privacy of health information (exacerbated by well-publicized breaches).

• Traditional protections involve de-identification and prior, opt-in, express consent. Each has problems.

• Nonetheless, there is evidence that there be greater comfort with research use of clinical health information.
Privacy: What?

Definitions are varied:

• control over information about oneself

• a condition in which others are unable to access information about oneself

• respect for contextual norms regarding flows of personal information

• limitation on reasonable inferences about a person
Privacy: So What?

• Respect for persons
  • Autonomy: ability to act according to one’s values as one sees fit
  • Trust and implicit expectation of being treated with respect

• Optimal care
  • Evidence that where people are concerned about health information privacy, they may engage in privacy-protecting behaviors

• Harms
  • Information disclosure can lead to harms through misuse or through use in ways that are disagreeable to data subjects

• Justice
  • De-identified data may be used to discern racial or ethnic disparities in health issue, may create stigmas, and may harden stereotypes, even where no single person is identified
  • Because stigma and stereotypes are unjustifiable grounds for distribution of important social grounds, they would be a source of injustice
Fair Information Practice Principles (FIPPS)

- Promulgated by U.S. Department of Health, Education & Welfare, 1973

FIPPs

- Openness and transparency
- Purpose specification
- Collection limitation and data minimization
- Use limitation
- Individual participation and control
- Data quality and integrity
- Security safeguard and controls
- Accountability and oversight
- Remedies
<table>
<thead>
<tr>
<th>Principle</th>
<th>Description (from The Markle Connecting for Health Common Framework for Networked Personal Health Information)</th>
<th>Link to Ethical Principles</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Openness and Transparency</strong></td>
<td>“Consumers should be able to know what information has been collected about them, the purpose of its use, who can access and use it, and where it resides. They should also be informed about how they may obtain access to information collected about them and how they may control who has access to it.”</td>
<td>Openness and transparency allow individuals to better understand how their information is collected and used at all stages of the research process (including scientific publications), which is itself important for respecting persons independent of their choice in matters and targets the fundamental principle of the individual’s right to know.</td>
</tr>
<tr>
<td><strong>Purpose Specification</strong></td>
<td>“The purposes for which personal data are collected should be specified at the time of collection, and the subsequent use should be limited to those purposes, or others that are specified on each occasion of change of purpose.”</td>
<td>Specifying purposes ensures that persons have the opportunity to understand and endorse the purposes to which their information is put, which is an important facet of respecting them as participants.</td>
</tr>
<tr>
<td><strong>Collection limitation and data minimization</strong></td>
<td>“Personal health information should only be collected for specified purposes and should be obtained by lawful and fair means. The collection and storage of personal health data should be limited to that information necessary to carry out the specified purpose. Where possible, consumers should have the knowledge of or provide consent for collection of their personal health information.”</td>
<td>Because health information is associated with some of the deepest, most personal, and most intimate facets of ourselves, respect for persons demands that sharing health information occur only under appropriate conditions, to appropriate parties, and for appropriate reasons. Limiting collection and minimizing data helps ensure that sharing is limited to such circumstances.</td>
</tr>
<tr>
<td><strong>Use Limitation</strong></td>
<td>“Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified.”</td>
<td>See comment under “collection limitation and data use.”</td>
</tr>
<tr>
<td><strong>Individual Participation and Control</strong></td>
<td>“Consumers should be able to control access to their personal information – specifically, they should know who is storing what information on them, and how that information is being used. They should also be able to review the way their information is being used or stored.”</td>
<td>Individual choice, or consent, is a component of the FIPPs, but it is not absolute and the degree of choice may depend on how completely the other principles are exercised. Moreover, choice may be based on alternative models, such as opt out models that allow individuals with particularly acute privacy concerns to avoid information sharing, rather than seeking opt-in permission from all individuals.</td>
</tr>
<tr>
<td><strong>Data Quality and Integrity</strong></td>
<td>“All personal data collected should be relevant to the purposes for which they are to be used and should be accurate, complete, and up-to-date.”</td>
<td>Data integrity helps ensure that information attributed to people is actually about them, and hence that they are not treated unfairly or unjustifiably; again, this is important in respecting persons.</td>
</tr>
<tr>
<td><strong>Security Safeguards and controls</strong></td>
<td>“Reasonable safeguards should protect personal data against such risks as loss or unauthorized access, use, destruction, modification, or disclosure.”</td>
<td>Data security policies and technical requirements should be in place to help protect data and reinforce stewardship practices adopted to implement the other principles.</td>
</tr>
<tr>
<td><strong>Accountability and Oversight</strong></td>
<td>“Entities in control of personal health information must be held accountable for implementing these principles.”</td>
<td>Helps ensure all of the principles are followed.</td>
</tr>
<tr>
<td><strong>Remedies</strong></td>
<td>“Remedies must exist to address security breaches or privacy violations.”</td>
<td>Allowing persons to exercise control in effecting remedies is a crucial aspect of respecting persons whose data security or privacy has been breached.</td>
</tr>
</tbody>
</table>
# FIPPs: Examples

<table>
<thead>
<tr>
<th>Principle</th>
<th>Description (from The Markle Connecting for Health Common Framework for Networked Personal Health Information)</th>
<th>Link to Ethical Principles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Openness and Transparency</td>
<td>“Consumers should be able to know what information has been collected about them, the purpose of its use, who can access and use it, and where it resides. They should also be informed about how they may obtain access to information collected about them and how they may control who has access to it.”</td>
<td>Openness and transparency allow individuals to better understand how their information is collected and used at all stages of the research process (including scientific publications), which is itself important for respecting persons independent of their choice in matters and targets the fundamental principle of the individual’s right to know.</td>
</tr>
<tr>
<td>Individual Participation and Control</td>
<td>“Consumers should be able to control access to their personal information – specifically, they should know who is storing what information on them, and how that information is being used. They should also be able to review the way their information is being used or stored.”</td>
<td>Individual choice, or consent, is a component of the FIPPs, but it is not absolute and the degree of choice may depend on how completely the other principles are exercised. Moreover, choice may be based on alternative models, such as opt out models that allow individuals with particularly acute privacy concerns to avoid information sharing, rather than seeking opt-in permission from all individuals.</td>
</tr>
<tr>
<td>Remedies</td>
<td>“Remedies must exist to address security breaches or privacy violations.”</td>
<td>Allowing persons to exercise control in effecting remedies is a crucial aspect of respecting persons whose data security or privacy has been breached.</td>
</tr>
</tbody>
</table>
Current regulatory framework (U.S.)

- Primarily Health Insurance Portability and Accountability Act (HIPAA) and Common Rule
- Rely heavily on consent
- Create disincentives toward research versus other uses of data
- De-identified data and limited data sets leave gaps
- Regulations themselves have problems
Consent

- Reliance on consent: HIPAA and Common Rule emphasize individual consent (or express authorization) in order to use identifiable information for research.
- Exceptions: IRB (for Common Rule) or Privacy Board (HIPAA) may waive or modify consent requirement
### Waiving or altering consent (authorization) under Common Rule and HIPAA:

<table>
<thead>
<tr>
<th>Common Rule (45 CFR 46.116)</th>
<th>HIPAA (45 CFR 164.512(i))</th>
</tr>
</thead>
<tbody>
<tr>
<td>The research involves no more than minimal risk to the subjects.</td>
<td>The use or disclosure of protected health information (PHI) involves no more than a minimal risk to the privacy of individuals (i.e., there is an adequate plan to protect identifiers, a plan to destroy the identifiers at earliest opportunity, and there are adequate assurances of no reuse or re-disclosure).</td>
</tr>
<tr>
<td>The research could not practicably be carried out without the waiver or alteration.</td>
<td>The research could not practicably be conducted without the waiver or alteration; and</td>
</tr>
<tr>
<td>The waiver or alteration will not adversely affect the rights and welfare of the subjects</td>
<td>The research could not practicably be conducted without access to and use of the protected health information.</td>
</tr>
<tr>
<td>Whenever appropriate, the subjects will be provided with additional pertinent information after participation</td>
<td></td>
</tr>
</tbody>
</table>
Regulation of research vs. other uses of data

• Research defined the same in Common Rule and HIPAA: “a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.”

• HIPAA allows identifiable information to be used for treatment, facilitating payment for care, and for certain “health care operations” (e.g., quality assessment, care coordination, insurance underwriting, review and auditing, business management)

• This creates some perverse incentives (e.g., only undertaking quality improvement study where results are used internally, rather than generalizable)

• Penalties under HIPAA encourage conservative interpretations.
De-identified data

- Common rule regulates only human subjects research, which is defined to include research using identifiable data
- HIPAA does not cover data that have been “de-identified”
- HIPAA allows entities to use “limited data sets” for research purposes
  - Limited data sets have had certain identifiers (e.g., name, address) removed or masked
  - Use of limited data sets is contingent on data use agreements, which define purpose of use and prohibit re-identification
- NOTE 1: use of de-identified data may limit usefulness for the purposes of PCTs
- NOTE 2: even de-identified data may not be sufficiently protective
Issues with HIPAA and Common Rule Regulatory Framework

IOM 2009: HIPAA privacy rule does not protect privacy as well as it should and impedes important health research:

- Privacy rule not uniformly applicable to all health research,
- Overstates ability of informed consent to protect privacy
- Potentially conflicts with other regulations (e.g., Common Rule)
- Different interpretations
- Creates barriers to research
- Leads to biased research samples
Potential changes

• HHS “Omnibus Rule” (January 2013) offered HIPAA guidance to allow individuals to authorize use of data for multiple research projects and for unspecified future research.

• Office for Human Research Protections proposed rule in 2011 to change Common Rule, including provision that would allow secondary use of data for research purposes without IRB review
Taking stock

• HIPAA and Common Rule rely on consent, but consent processes limited:
  • Emphasis on forms
  • Secondary uses of data may not be covered
• De-identified data not subject to authorization or consent requirements under HIPAA and Common Rule
  • But may not be as useful, and may not be totally privacy protective
  • Even so, people have an interest in their health information
• Altered consent possible, but still need some criteria for what altered consent should look like
• Waiver of consent possible, but people still have interests in information
• So: opt in consent isn’t the only thing and the only consideration
Mechanisms for respecting privacy and autonomy interests
Greater input into research and research policy

For example

• PCORI: requirement that funded research be patient centered, including directly engaging people representing study populations

• PCORnet Patient Council, acting as advisory group to PCORnet steering committee and leadership, which generates best practices

• Collaboratory Stakeholder Engagement Core: patient and consumer representatives, provides feedback to Collaboratory leadership on study design and implementation issues

• Note: these are examples of FIPPs, and hence respecting patients in use of data, not privacy protective per se
Opt Out

Strategies and Opportunities to Stop Colorectal Cancer in Priority Populations (STOP CRC)

- Traditional informed consent in research trials is opt-in.
- An opt-out model includes participants automatically.
- STOP CRC aimed to improve CRC screening among patients receiving care through Federally Qualified Health Centers.
- Mailed fecal immunochemical kit (FIT) to patients identified through electronic medical record.
- Information letter sent prior to FIT with the option to opt out.
- Reminders sent to participants (unless/until they opt out).
- Respect for persons / autonomy by provision of information and continuing ability to opt out.
Broad Notification

Randomized Evaluation of Decolonization versus Universal Clearance Eliminate MRSA (REDUCE MRSA)

• Comparison of three strategies for presenting MRSA infections in intensive care units

• Waiver of informed consent granted

• IRB required patient notification via notices in each ICU room

• Respect for patients via provision of information
Individual Notification

Collaboratory’s Time to Reduce End Stage Renal disease (TiME) trial

- Cluster-randomized trial evaluating minimum hemodialysis session duration of 4.25 hours compared with usual care for patients with end-stage renal disease
- Patients provided with written information including trial sponsor, purpose of trial, treating physician’s role, description of the transmission of de-identified patient data to the University of Pennsylvania, and contact information for questions and opt out provisions
- Advances FIPPs, independent of privacy protections
Community Consultation

- Persons agree to be governed by decisions of community representatives

- Rather than individual control, respect for persons involves ability to delegate decisions to representatives
Conclusions

• Balancing protection of privacy interests and benefits of research using patient data in PCTs requires looking at values that underwrite privacy claims in the first instance.

• HIPAA and Common Rule provide important protections, but not tailored to address all research uses of data, and may create disincentives to use.

• Rules designed to protect persons against risks of interventional research may not be a good fit for addressing privacy risks.

• Modified approaches to consent and engagement projects may be a better way for ensuring appropriate, justifiable uses of health information and hence respecting persons.
Declaration of conflicting interests
Deven McGraw is the head of the PCORnet Data Privacy Task Force and has no other potential conflicts of interest to report. Sarah Greene, Caroline Miner, Karen L Staman, Mary Jane Welch, and Alan Rubel have no conflicts of interest.

Funding
This work was supported by the National Institutes of Health (NIH) Common Fund, through a cooperative agreement (U54 AT007748) from the Office of Strategic Coordination within the Office of the NIH Director. Additional support was provided by the Patient-Centered Outcomes Research Institute (PCORI) Award for development of the National Patient-Centered Clinical Research Network (PCORnet).