Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.
January 15, 2022

Office of Science and Technology Policy
Executive Office of the President
The White House
via email to BiometricRFI@ostp.eop.gov

Re: Comments of Prof. Barbara J. Evans, Ph.D., J.D., LL.M. in response to Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies, Federal Register; 86(193):56,300-56,302 (Oct. 8, 2021)

Thank you for the opportunity to participate in Nov. 18, 2021 Biometric Technologies Listening Session and to comment in the above-captioned RFI.

I am commenting today in my personal capacity as a member of the public, rather than on behalf of my institution or the State of Florida, which is my employer. For purposes of identification, I am Professor of Law and Stephen C. O’Connell Chair at the University of Florida Levin College of Law, with joint appointment as Professor of Engineering at the University of Florida Wertheim College of Engineering, located in Gainesville, Florida. I have over 25 years’ experience – both as a scholar and, before that, as a partner in private law practice – addressing regulatory and ethical issues with major infrastructure systems, including large-scale data infrastructures. My current focus is on data privacy, safety, and civil rights concerns affecting medical software and, in particular, artificial intelligence/machine learning (AI/ML) clinical decision support (CDS) software and software supporting the genomic bioinformatics pipeline. I have no conflicts to disclose.

I am attaching a legal research paper analyzing some of the questions raised by your RFI. It supplies a more complete account, with citations to relevant statutes, government advisory documents, and scholarly literature, of the points I briefly summarize below.

All of the page references below are to that research paper: Barbara J. Evans, The HIPAA Privacy Rule at Age 25: Pushing Past Boomer Bioethics to Promote Equity in AI-Enabled Health Care (University of Florida Levin College of Law Legal Studies Research Paper Series No 21-36) [for brevity, “Evans, LSRP 21-36”]
A one-size-fits-all approach to an AI Bill of Rights is inappropriate because the safety, privacy, and civil rights concerns raised by AI software depend heavily on the context in which it is applied.

The “Bill of Rights” analogy is memorable but it incorporates two core beliefs: First, a unitary Bill of Rights can protect people’s interests in all contexts where AI/ML software is applied. Second, protecting those rights is primarily a federal concern. Both these beliefs require careful scrutiny.

In particular, I would urge OSTP to distinguish AI-enabled biometric technologies intended for use in clinical healthcare settings from those employed by retailers, educators, credit-scorers, social media providers, law enforcement, and other non-medical actors in modern “surveillance societies.” See Evans, LSRP 21-36, at pages 3-4.

Some AI-enabled biometric software is in the nature of clinical decision support (CDS) software, offering diagnostic or treatment recommendations to healthcare professionals in clinical healthcare settings. Protecting safety and civil rights in clinical healthcare settings involves the interplay of state, federal, and non-governmental authorities already involved with these matters.

More generally, medical and non-medical AI differ in ways that may justify different civil rights protections, including for data privacy. For non-medical AI/ML tools, the United States has glaring gaps in privacy and other civil rights protections that are a worthy focus for OSTP’s policymaking efforts. In clinical healthcare settings, however, the “overlay” of the federal HIPAA Privacy Rule onto state-level medical privacy rules and information fiduciary duties of healthcare providers creates a civil rights framework that is surprisingly well-tailored to the major challenges we face in an age of AI-enabled health care. See Evans LSRP 21-36, at pages 4-5.

This framework is, however, at times misunderstood. The HIPAA Privacy Rule is often criticized based on the (erroneous) perception that it is weaker than the European Union’s General Data Protection Regulation (GDPR). In the clinical healthcare contexts where the HIPAA Privacy Rule applies, it is in many respects stronger than GDPR. See Evans LSRP 21-36, at page 8, discussing how EU Member States apply GDPR in clinical healthcare settings. It will be important not to set policy based on a misunderstanding of the protections GDPR provides.

Health equity is the major unresolved ethical and civil rights challenge with AI/ML medical software

See Evans LSRP 21-36, at pages 8-10, noting that: “Training datasets for AI/ML CDS tools tend to overrepresent men of European ancestry while underrepresenting members of other racial and ethnic groups and women. Empirical studies of how CDS tools perform for transgender patients do not even appear to exist, but it is known these patients face special health risks (such as elevated incidence of aortic aneurism in transgender women). Those risks can be obscured if AI/ML training datasets force-fit these patients into gender-binary categories without further nuancing to highlight special medical needs within those categories. AI/ML tools that perform well in high-resource, well-staffed academic medical centers often underperform at lower-resourced community hospitals where much of the American population receives care. To be blunt, much of the AI/ML CDS software developed to date is racist, misogynistic, trans-oblivious, and dispenses recommendations that vary in quality depending on your socioeconomic status.”
See Evans RP 21-36, at pages 10-19, attributing much of this problem to structural and systemic inequities in U.S. health care. However, part of the problem traces to 1970s-era information privacy norms that prevail both in bioethical discourse and in information privacy theory more generally. These norms can have a disparate impact that fuels inequity in medical AI software. Eliminating those inequities is the defining ethical challenge for medical AI.

Strengthening privacy, safety, and civil rights protections for medical AI will require a carefully integrated state, federal, and non-governmental effort

The HIPAA Privacy Rule offers a powerful toolkit for addressing three defining bioethical challenges in the age of AI-enabled clinical care. Those challenges are to protect individual privacy, to keep patients safe by enabling data flows to regulators, scientists, and others charged with ensuring software safety, and to combat inequity and injustice in AI/ML medical software. See Evans RP 21-36, at pages 24-35, discussing regulatory pathways for assembling more inclusive, equitable training data for medical AI.

For this to be successful, however, the HIPAA Privacy Rule has certain gaps that need to be filled, and doing so will require coordination among state and federal policymakers as well as non-governmental actors. Crafting a “Bill of Rights” will require an interactive rather than top-down, federal effort. Perhaps you already have taken that into account, but it bears re-emphasis.

The HIPAA Privacy Rule was the product of careful consultations between federal and state privacy regulators to accommodate their joint roles in medical privacy. The Privacy Rule’s preemption provisions, like those of the HIPAA statute, grant the States the power to improve its civil rights protections. Additionally, the 21st Century Cures Act of 2016 tasked the U.S. Food and Drug Administration (FDA) with overseeing the safety of AI/ML CDS tools. The FDA’s proposed regulatory approach for CDS software would assess its performance using flows of real-world clinical health data, which the Privacy Rule enables. A one-size-fits-all approach to medical and non-medical AI privacy might impede this data-driven safety oversight.

See Evans RP 21-36, suggesting specific measures to enhance safety, privacy, and equity for medical AI. These measures include:

A. Recognize that informed consent and safe-harbor de-identification (stripping away specific identifiers from the data) do not provide effective privacy protection. Even when consent seems ethically necessary, it may not be sufficient to protect privacy.

B. Adopt policies to nudge software developers and users toward greater reliance on statistical de-identification techniques (i.e., computational privacy protections, privacy-by-design), which can provide more reliable, measurable privacy protection.

C. Educate the public that, in an age of AI-enabled medical software, having your data included in AI/ML training data helps ensure that the resulting software will provide well-informed health recommendations for you, and for people like you.

D. Require ethics review bodies (and other gatekeepers charged with overseeing access to training data for AI/ML medical software) to include members having the technical expertise necessary to oversee strong, modern computational privacy protections.

E. Strengthen “information fiduciary” requirements for parties who control AI/ML CDS tools, whether as developers, vendors, or users.

F. Implement “public benefit” requirements to ensure that any non-consensual uses of people’s data will serve socially beneficial purposes, such as reducing inequities in health care.
G. Promote legal accountability for privacy violations and for inequitable, unsafe AI/ML medical software through appropriate allocation of legal liabilities.

Thank you for this opportunity to provide comments.

Sincerely,

Barbara J. Evans, Ph.D., J.D., LL.M.
Professor of Law and Stephen C. O’Connell Chair
University of Florida Levin College of Law
Professor of Engineering
University of Florida Wertheim College of Engineering
Spessard L. Holland Law Center
PO Box 117620
Gainesville FL 32611-7620
The HIPAA Privacy Rule at Age 25:
Pushing Past Boomer Bioethics to Promote Equity in AI-enabled Health Care

Barbara J. Evans, Ph.D., J.D., LL.M.
THE HIPAA PRIVACY RULE AT AGE 25: PUSHER PAST BOOMER BIOETHICS TO PROMOTE EQUITY IN AI-ENABLED HEALTH CARE
Barbara J. Evans*

INTRODUCTION

I. COMPETING DATA ACQUISITION NORMS FOR AI/ML MEDICAL SOFTWARE

   A. The Privacy Rule and its discontents
   B. Invidious discrimination in AI/ML CDS software
   C. Systemic bias in medical AI
   D. The systemic element of consent bias
   E. The disparate impact of informed consent norms
   F. The rise of boomer data ethics after 1970
   G. The bioethics of human sameness
   H. Biomedicine confronts human diversity after 1990
   I. The Privacy Rule reasserts traditional medical privacy norms
   J. Traditional informational norms of clinical health care
   K. Translating traditional norms to modern health care

II. PATHWAYS TO DIVERSE, INCLUSIVE AI/ML TRAINING DATA

   A. Disclosure-friendly Norms and Alternative Privacy Protections
   B. AI/ML CDS software as a treatment use of data
   C. Diversion of health data from healthcare operational uses
   D. Two pathways of access for AI/ML research
   E. Access to data by FDA-regulated software developers
   F. Creating Common Data Infrastructure for Equitable AI/ML Medical Software

III. ACHIEVING STATE-OF-THE-ART PRIVACY PROTECTION IN THE AGE OF MEDICAL AI

   A. Notice-and-consent norms as bioethical misinformation
   B. Remessaging consent in the age of AI-enabled health care
   C. Staffing for state-of-the-art privacy protection
   D. Addressing the Privacy Rule's Lingering Privacy Gaps

CONCLUSION
THE HIPAA PRIVACY RULE AT AGE 25: PUSHING PAST BOOMER BIOETHICS TO PROMOTE EQUITY IN AI-ENABLED HEALTH CARE

INTRODUCTION

President Bill Clinton signed the Health Insurance Portability and Accountability Act (HIPAA) into law on August 21, 1996. Its 25th birthday passed largely unnoticed last August in an America wracked by contagion and a rough exit from Afghanistan. HIPAA was mainly an insurance statute best known in medical circles for its annoying offshoot, the HIPAA Privacy Rule, which took effect in 2003-2004 after a long and contentious rulemaking. Rarely in the nation’s history has a regulation been so widely reviled.

An alternative view, advanced here, is that the Privacy Rule was ahead of its time. Its drafters foresaw an increasingly diverse American population served by 21st-century health systems that, increasingly, would derive general medical knowledge from informational as well as clinical research. In that faraway future, rigid requirements to obtain informed consent before scientific use of people’s health data might block critical data flows and exacerbate healthcare disparities, inadvertently abetting injustice in health care. That future is here now, as health systems grow dependent on artificial intelligence and machine learning (AI/ML) medical software. Long scorned, the Privacy Rule might be just what the doctor ordered to advance equitable, justice-serving medical AI.

In October 2021, the White House Office for Science and Technology Policy (OSTP) launched a study of AI-enabled biometric technologies. Two OSTP officials later called for a new “Bill of Rights for an AI-Powered World” and OSTP is working to develop it. The Bill of Rights analogy presumes a single, overarching set of principles could suffice for AI/ML software of all types in all contexts.

This article expresses grave doubt about a one-size-fits-all approach. A cautionary example is AI/ML clinical decision support (CDS) tools that offer recommendations to healthcare professionals

---

* Professor of Law and Stephen C. O’Connell Chair, University of Florida Levin College of Law; Professor of Engineering, University of Florida Wertheim College of Engineering.


2 45 C.F.R. pts. 160, 164.


5 See Kayte Spector-Bagdady, Governing Secondary Research Use of Health Data and Specimens: The Inequitable Distribution of Regulatory Burden Between Federally Funded and Industry Research, J. L. AND THE BIOSCIENCES 1, 4 (2021) (discussing the shift from human-subjects clinical research that studies people’s bodies to informational research “research with all the stuff [such as data and biospecimens] derived from them.”)


on how to diagnose, treat, or predict the course of a patient’s disease.⁹ CDS tools are designed for use in clinical healthcare settings where patients’ contact with the software is mediated by human actors. Its recommendations might be challenged and rejected (or accepted and implemented) by a clinician, genetic counselor, nurse, or other healthcare professional.

AI/ML CDS tools have distinct features that set them apart from large-scale data collection and processing by retailers, credit-scoreers, social media providers, law enforcement, and other non-medical actors in modern “surveillance societies.”¹⁰ One distinct feature is that CDS software implicates domains of regulation for which longstanding norms of federalism allocate oversight responsibilities to both state and federal authorities (e.g., state medical practice regulators vs. federal medical product regulators).¹¹ Protecting the safety and civil rights of patients and others whose data is used in AI/ML CDS software requires a careful interplay of state, federal, and non-governmental authorities already involved with these matters.¹² More broadly, medical and non-medical AI differ in ways that may justify different civil rights protections, including for data privacy.¹³ There is no harm in exceptionalism, as long as you can put your finger on what, precisely, warrants an exception. This article tries to do that for AI/ML CDS software.

For non-medical AI/ML tools, the United States has glaring gaps in privacy and other civil rights protections that are a worthy focus for OSTP’s policymaking efforts. In clinical healthcare settings, however, the Privacy Rule is not ‘broken’ and does not need to be ‘fixed,’ at least not at the federal level.¹⁴ The Privacy Rule was the product of careful consultations between federal and state privacy regulators to accommodate their joint roles in medical privacy.¹⁵ The Privacy Rule’s preemption provisions, like those of the HIPAA statute, grant the States power to improve its civil rights protections.
Additionally, the 21st Century Cures Act of 2016 tasked the U.S. Food and Drug Administration (FDA) with overseeing the safety of AI/ML CDS tools. The FDA’s proposed regulatory approach for CDS software would assess its performance using flows of real-world clinical health data, which the Privacy Rule enables. A one-size-fits-all approach to medical and non-medical AI privacy might impede this data-driven safety oversight.

The Privacy Rule, like most 25-year-olds, is deeply misunderstood by boomer bioethicists, the postwar generation born between 1946 and 1964 that came of age as scholars in the 1970s and 1980s. The Privacy Rule laid a strong cornerstone for a clinical AI Bill of Rights, but only if policymakers, regulated institutions, and gatekeepers that control access to real-world clinical data understand its rationale and embrace the socially beneficial data practices it promotes.

I. COMPETING DATA ACQUISITION NORMS FOR AI/ML MEDICAL SOFTWARE

A. The Privacy Rule and its discontents

Since the 1970s, bioethicists have pressed for people to have a right of informed consent before their identifiable health information moves into secondary uses – that is, uses other than the one for which they intended the data. Equivalent notice-and-consent norms are favored by the more recent “Information Privacy Law Project” examining the ethics of data flows in the broader surveillance society where personal information is routinely collected, stored, and made visible to others and then algorithmically transformed “in the active production of categories, narratives, and norms” that can land us on no-fly lists, earn us a discount, tag us as risky or at-risk human beings, or cause a prospective employer to rule us out. The phrase “de-identify or get consent” (DOGC) encapsulates what such norms typically require: get consent if the data are in a format that identifies the individual the data describe.

The Privacy Rule is a medical privacy law aimed at players in the chain of payments for clinical health care. It regulates “covered entities” – basically, private-sector actors that provide or finance clinical healthcare services (clinics, hospitals, and insurers), plus business associates that obtain identifiable data from them while supplying professional or informational services to them. This leaves out many businesses commonly thought of as health-related, such as companies selling fitness trackers and consumer health applications, or pharmaceutical or medical device companies that sell medical products as opposed to medical services. The Privacy Rule governs what covered entities can

---

16 See 45 C.F.R. § 160.202-.203 (Privacy Rule preemption provisions); 42 U.S.C. § 1320d-7(b) (HIPAA statutory preemption provisions).
18 See infra Table 1, Norms 15, 16 and Part II.E, F.
19 See Privacy Protection Study Commission, Personal Privacy in an Information Society 280 (1977), available at https://www.epic.org/privacy/ppsc1977report/c13.htm (finding, in a study authorized under the Privacy Act of 1974 see 5 U.S.C. § 552(a)(d), that health data were widely used without consent in medical research and public health studies during the 1970s, and recommending that it would be ethical to seek consent before such uses). For an example of a regulation implementing this view, see, e.g., Federal Policy for the Protection of Human Subjects of Biomedical Research (“Common Rule”), 45 C.F.R. §§ 46.101–124.
22 See 45 C.F.R. § 160.102 (2018) (providing that the HIPAA regulations, including the Privacy Rule, apply to healthcare providers such as physicians, clinics, hospitals, laboratories and various other entities, such as insurers, that transmit “any health information in electronic form in connection with a transaction covered by this subchapter [the Administrative Simplification provisions of HIPAA]” and to their business associates); see also id. § 160.103 (defining the terms “covered entity” and “business associate”).
do with protected health information (PHI), which is a class of data, defined in the HIPAA statute, that the Privacy Rule protects.23

Bioethicists’ major discontent with the Privacy Rule is that it is not a DOGC privacy scheme. The Privacy Rule allows covered entities to use or disclose PHI with individual authorization (HIPAA’s name for consent) or if the data have been de-identified.24 This lulls casual observers into thinking the Privacy Rule is a DOGC privacy scheme. Then comes the betrayal: the Privacy Rule goes on to list 25 additional ways patients’ PHI can be shared, usually without consent and potentially in identifiable form (Table 1). “Even if the Privacy Rule allows nonconsensual access to data, is it ethical and is it trustworthy?” ethicists ask.

The Privacy Rule is what law scholar Martha Nissenbaum calls a contextual privacy scheme. It lists “informational norms” – a set of data flows considered appropriate and necessary in and around one specific context (in this case, clinical health care).25 Information sharing that is appropriate in one context might be highly inappropriate in other contexts. Thus, inquiring about people’s annual income is appropriate when they apply for a home loan, but not when asking them out on a first date.

When crafting the norms in Table 1, the U.S. Department of Health and Human Services (HHS) was “aware of the concerns of privacy and consumer advocates” about controlling access to their data, but HHS determined that “[t]he allowable disclosures and corresponding restrictions we recommend reflect a balancing of privacy and other social values.”26 The Privacy Rule was never all about your individual autonomy; it is about the contextual ends and values of clinical health care.27 It is about making health care work and, I argue, about making healthcare work more equitably – something that, to date, American health care has failed to do.

23 See 45 C.F.R. § 160.103 (defining “protected health information” (the information that the HIPAA Privacy Rule protects) as “individually identifiable health information” and defining the term “health information” for purposes of the HIPAA Privacy Rule). See 42 U.S.C. § 1320d(4) (reflecting the original 1996 HIPAA statute’s definition of “health information” as “any information, whether oral or recorded in any form or medium, that: (A) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual”). See also, Genetic Information Nondiscrimination Act of 2008 § 105(a), 42 U.S.C. § 1320d-9(a) (expanding the definition of “health information” that HIPAA protects to include genetic information). See also, 42 U.S.C. § 1320d-9(b)(1) (stating, in a new section introduced by GINA, that Congress deems “genetic information,” as broadly defined by GINA at 42 U.S.C. § 300gg-91, to be health information, for purposes of making it subject to HIPAA’s privacy protections).

24 See 45 C.F.R. § 164.502(a)(1)(iv) (allowing PHI to be released with individual authorization); id. § 164.508 (describing requirements for a valid individual authorization, which is HIPAA’s term for a consent). See id § 164.502(d) (allowing de-identified data to be used and disclosed without individual authorization).


27 See discussion infra Parts I.I – I.K.
### Table 1. The Privacy Rule’s 27 Norms Allowing PHI to be Used and Disclosed

<table>
<thead>
<tr>
<th>Can disclose or use data</th>
<th>Fifteen norms allowing unconsented disclosure and use, subject to the minimum necessary standard*</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. with individual authorization</td>
<td>13. with waiver approved by IRB/privacy board</td>
</tr>
<tr>
<td>2. if deidentified</td>
<td>14. for payment and healthcare operations/QI</td>
</tr>
<tr>
<td>a. safe-harbor deidentification</td>
<td>15. to public health authorities and their contractors</td>
</tr>
<tr>
<td>b. statistical deidentification</td>
<td>16. to FDA-regulated entities for activities that FDA requires them to do.</td>
</tr>
<tr>
<td>3. MUST disclose designated record set to the individual upon request, under HIPAA’s individual right of access to one’s own data</td>
<td>17. to health oversight agencies</td>
</tr>
<tr>
<td>4. Can disclose additional data to the individual</td>
<td>18. limited data set subject to data use agreement</td>
</tr>
<tr>
<td>5. Disclosures to legal representative after death</td>
<td>19. to people exposed to communicable disease</td>
</tr>
<tr>
<td>Seven norms allowing unconsented disclosure and use, not subject to minimum necessary standard but subject to alternative protections</td>
<td>20. to employers for workplace safety/exposures</td>
</tr>
<tr>
<td>6. to a healthcare provider for use in treating a patient – any patient</td>
<td>21. to facilitate a dignified burial of the deceased</td>
</tr>
<tr>
<td>7. to HHS for regulatory compliance purposes</td>
<td>22. to facilitate organ transplants</td>
</tr>
<tr>
<td>8. as required for HIPAA compliance</td>
<td>23. for fundraising with an opt-out</td>
</tr>
<tr>
<td>9. to agencies for detecting abuse and neglect</td>
<td>24. for certain insurance underwriting purposes</td>
</tr>
<tr>
<td>10. for judicial and regulatory proceedings</td>
<td>25. to avert serious threats to health or safety</td>
</tr>
<tr>
<td>11. for law enforcement purposes</td>
<td>26. for special governmental functions (military)</td>
</tr>
<tr>
<td>12. if required by law</td>
<td>27. for workers’ compensation cases</td>
</tr>
</tbody>
</table>

* Minimum necessary disclosures can include identifiers if they are necessary to fulfill the purpose of the disclosure

A second discontent is that the HIPAA statute defines PHI narrowly. It includes data related to people’s health or to their health care if the information is “created or received by a health care provider.”

That leaves out what might be termed “health-related information outside clinical contexts” (HIPOCs), such as data from personal fitness trackers, commercial ancestry genomic testing, or from AI tools lenders use to predict who is likely to live long enough to repay a loan. It

---

28 See 45 C.F.R. § 164.502(a)(1)(iv) and see id. § 164.508 (describing requirements for a valid authorization) [Norm 1]; id. §§ 164.502(d), 164.514(a) and see id. § 164.514(b)(1) (statistical de-identification), id. § 164.514(b)(2)(i) (safe-harbor de-identification) [Norm 2]; id. § 164.524 (providing an individual access right) and id. § 164.501 (defining the “designated record set” that is subject to mandatory disclosure to the individual or to a third party the individual specifies) [Norm 3]; id. §§ 164.502(a)(1), (b)(2)(i) [Norm 4]; id. §§ 160.103, 164.502(e) and see HHS, FAQ 512-Under the HIPAA Privacy Rule, may a health care provider disclose protected health information about an individual to another provider, when such information is requested for the treatment of a family member of the individual?, at https://www.hhs.gov/hipaa/for-professionals/faq/512/under-hipaa-may-a-health-care-provider-disclose-information-requested-for-treatment/index.html (clarifying that, except for psychotherapy notes, a HIPAA-covered doctor may disclose a patient’s information to another doctor without individual authorization for use in treating “another patient” – not necessarily a family member of the person whose data is disclosed) [Norm 6]; id. § 164.502(b)(2)(iv) [Norm 7]; id. § 164.502(b)(2)(vi) [Norm 8]; id. § 164.512(e) [Norm 9]; id. § 164.512(e) [Norm 10]; id. § 164.512(f) [Norm 11]; id. § 164.512(a) [Norm 12]; id. § 164.512(i) [Norm 13]; id. §§ 164.502(a)(1)(ii), 164.506. But see Proposed Modifications to the HIPAA Privacy Rule To Support, and Remove Barriers to, Coordinated Care and Individual Engagement (Notice of Proposed Rulemaking), 86 Fed. Reg. 6446 [January 21, 2021] (controversially proposing to exclude these disclosures from HIPAA’s minimum necessary standard) [Norm 14]; id. § 164.512(b)(1)(i),(ii), 164.514(d)(3)(ii)(A), 164.514(b)(2)(ii), (iii) [Norm 15]; id. § 164.512(b)(iii) [Norm 16]; id. § 164.512(d) and see id. § 164.501 (defining oversight agencies) [Norm 17]; id. §§ 164.514(c)(3)(i), 164.514(e)(4) [Norm 18]; id. § 164.512(b)(iv) [Norm 19]; id. § 164.512(b)(v) [Norm 20]; id. § 164.512(g) [Norm 21]; id. § 164.512(h) [Norm 22]; id. § 164.514(f) [Norm 23]; id. § 164.514(g) [Norm 24]; Id. § 164.512(j) [Norm 25]; id. § 164.512(k); id. § 164.512(l) [Norm 27].

29 Supra Note 23.
strikes many observers as crazy that HIPAA protects the inference that Sally is pregnant if it came from a test her clinician ordered, but not if a retailer’s AI algorithm mined Sally’s recent purchasing data and concluded she must be pregnant. A contrarian view, explored here, is that this is not crazy and, in fact, is a sensible policy that is just poorly understood.

A third discontent is the perception that Privacy Rule is weaker than the European Union’s (EU) General Data Protection Regulation (GDPR), often touted as the putative privacy Ideal to which the United States should aspire. In the clinical healthcare context where the Privacy Rule applies, it is in many respects stronger than GDPR. The Privacy Rule sets a federal floor of clinical data protection: states are free to set higher standards but cannot go lower. In contrast, GDPR grants the 27 EU Member States leeway to go higher or lower than GDPR’s baseline consent standard. A 2021 report for the European Commission details the many ways Member States enable unconsented flows of health data. In clinical healthcare contexts, many Member States allow unconsented data flows functionally equivalent to those in Table 1. Where clinical data privacy is concerned, the perceived GDPR privacy Ideal exists only in the ill-informed American imagination.

B. Invidious discrimination in AI/ML CDS software

Law considers discrimination “invidious” when people are treated in damaging ways because of race, gender, or class, without a rational reason to do so (for example, there could be a good reason to disadvantage a historically privileged group to correct past injustices). AI/ML CDS tools show great promise for improving health care but recent empirical studies reveal their ominous side: they can serve as instruments of invidious healthcare discrimination.

Training datasets for AI/ML CDS tools tend to overrepresent men of European ancestry while underrepresenting members of other racial and ethnic groups and women. Empirical studies of how