Interoperability MATTERS
an initiative of The Sequoia Project

DRAFT

Operationalizing Automated Consent:

Actionable Guidance for Health Care Providers, Payors, and Other Health Care Organizations

Legal Elements of Consent (HIPAA & 42 CFR Part 2)

Draft for Public Comment

Send your feedback to interopmatters@sequoiaproject.org by March 13, 2026

the sequoia project

Contents

1. Introduction

The U.S. health information ecosystem continues to struggle with a widening gap between policy expectations for seamless data exchange and the operational realities of collecting, managing, and honoring patient consent. *Moving Toward Computable Consent: A Landscape Review* (The Sequoia Project, April 2025) (hereinafter, the "**2025 Landscape Review**") traced this disconnect to a series of persistent chokepoints:

- A tangled web of federal and state consent rules that even seasoned compliance teams interpret differently, each of which may require or waive consent for different purposes;
- The absence of mature, computable-consent infrastructure capable of capturing granular choices and carrying them across disparate electronic health records (EHRs), health information networks (HINs), and payer systems;
- Widely divergent consent forms and workflows that force each organization to invent its own "dialect" of consent and then train staff to speak it;
- Daily friction points, literacy hurdles, signature collection, revocation tracking, limited staffing, that turn consent into a resource drain competing with clinical care;
- Ongoing challenges in identity matching and data segmentation that break the connection between a patient's expressed wishes and the records circulating in the network; and
- The constant tension between obtaining consent and avoiding information blocking, leaving providers, payers and other stakeholders uncertain which rule should prevail.

This guidance document builds upon the 2025 Landscape Review and translates its findings into practical, operational considerations. It also includes a suite of sample "operational resource documents," business requirements, model policies, and workflow templates that stakeholders can readily adapt based on their own circumstances. Collectively, these resources are intended to help prepare the industry for a future in which computable, standards-based consent is routine.

This guidance document and its related appendices directly answer the Landscape Review's call for a "practical playbook." Its purpose is to equip health care providers, health systems, payers, and their partners with actionable tools to collect, manage, and honor patient consent confidently, efficiently, and in a computable manner. Paper and other nonautomated consent mechanisms are out of scope; the aim of this document is

to help stakeholders move toward automated processes that support interoperability. The tools and frameworks presented here are designed to operationally support electronic, standards-driven consent capture, management, and exchange, laying the groundwork for scalable, automated consent operations across the health information ecosystem.

2. Computable Consent

The 2025 Landscape Review traced many of the interoperability and data-sharing barriers in health care to the fragmented and manual ways patient consent is collected and managed today. It found that paper and scanned authorizations, static PDFs, and manual "release of information" workflows have created inconsistent, resource-intensive processes that cannot scale in a digital health ecosystem. The report concluded that these legacy methods, while legally valid, have become an obstacle to seamless, trustworthy data exchange.

To address this problem, the Landscape Review introduced the concept of computable consent as a transformative solution. It defined computable consent as a machine-readable, standards-based representation of an individual's privacy and data-sharing preferences that can be automatically adjudicated and enforced across electronic systems. In practice, computable consent involves encoding a person's directives in a structured, interoperable format, such as the HL7 Fast Healthcare Interoperability Resource (FHIR) Consent Resource, so that EHR, HIN and payer systems can record, transmit, and apply a patient's choices about what information may be shared, with whom, and for what purposes. When implemented properly, these directives generally can be executed automatically, without human interpretation or manual intervention. However, realizing this level of automation requires more than technical capability; it demands coordinated organizational readiness. Therefore, implementing automated consent requires alignment across legal, technical, and governance domains.

Computable consent evolved from the concept of granular consent, which allows patients to authorize or restrict specific data elements or purposes rather than relying on broad "all-or-nothing" models. The Landscape Review emphasized that computable consent enables legal and policy rules governing data exchange to be expressed in machine-readable form, allowing those rules to be adjudicated and enforced consistently across organizations and technologies. Foundational standards efforts such as the HL7 FHIR Consent Resource, the IHE Privacy Consent on FHIR (PCF) Profile, and the ONC LEAP Consent Project were identified as the building blocks for operationalizing this capability at scale.

Equally important, the Landscape Review clarified what does not constitute computable consent. It excludes:

- Traditional paper, scanned, or PDF authorizations that cannot be parsed or executed by electronic systems;
- Manual "release-of-information" or deferred approval workflows that depend on staff intervention;
- Simple, binary, or blanket opt-in/opt-out models that lack granular control; and
- Legacy or other data that lack metadata, sensitivity tagging, or other approaches to sensitivity determination that can be operationalized.

Because computable privacy and consent standards are still emerging, any consent process that cannot be represented and exchanged in a consistent, machine-interpretable format are currently outside its scope. Building on the Landscape Review, this guidance focuses on the real-world operationalization of automated consent via digital tools, interoperable standards, and technical workflows. The goal is to prepare the health information ecosystem to move beyond those legacy approaches toward automated, standards-driven consent management that can support secure, patient-directed information sharing "at scale."

3. Scope of Guidance

Automated consent must be operationalized across a wide spectrum of use cases, each involving distinct legal authorities, data flows, and technical challenges. In practice, consent transactions may occur in many different configurations, for example:

Examples of Consent Transactions (non-exhaustive)

- Provider → Payer (for payment adjudication or utilization management);
- Payer → Payer (for coordination of benefits or continuity of coverage);
- Provider → Patient (for patient-directed access or disclosure to personal software applications); and
- Health Information Network (HIN) or Health Information Exchange (HIE) acting as an intermediary or facilitator of the consent transaction between recipients.

- Consent may be captured at multiple points, by the disclosing entity, the requesting entity, or a trusted third party operating as a business associate under HIPAA or a Qualified Service Organization (QSO) under 42 C.F.R. Part 2.

- In some circumstances, consent may not be required at all, such as in bona fide medical emergencies or other legally recognized exceptions.
- Additional complexity arises when consent involves special categories of individuals, such as minors, legally incapacitated adults, or personal representatives, where distinct state and federal standards apply. See the 2025 Landscape Review for a discussion of the regulatory variability and operational barriers in implementing computable consent at scale.

Because the operational terrain is so broad, this guidance document cannot address every permutation. It was therefore necessary to narrow the scope of this first phase to a single, high-impact use case, one that provides a realistic foundation for defining the operational building blocks of automated consent. This approach produced tangible, reusable tools while testing the interoperability and governance elements that will ultimately support broader expansion.

Accordingly, this guidance document addresses a timely and legally consequential scenario:

> **Sharing substance use disorder ("SUD") information for treatment under the newly aligned 42 C.F.R. Part 2 ("Part 2") Final Rule, which becomes enforceable in February 2026.**

More specifically, this guidance focuses on those specific entities which are subject to Part 2 ("Part 2 Programs") disclosing Part 2 records pursuant to an automated, computable consent through a health information network (HIN) to a HIPAA-covered provider that is not itself a Part 2 Program.

This scenario was selected because it represents a legally significant exchange pattern under the newly aligned HIPAA-Part 2 framework. It allows "modeling" of the end-to-end operational steps, legal, technical, and governance that must be in place before broader adoption across other consent contexts (e.g., payment, public health, or research) can occur.

This guidance document excludes from scope:

- Consents involving **minors** or individuals represented by parents, guardians, or legal representatives;
- Consents governing **SUD counseling notes**, which require distinct, standalone authorization under 42 C.F.R. § 2.31(a)(2); and

- Consents for **non-treatment purposes**, such as marketing, fundraising, public health reporting, research, or other disclosures outside HIPAA's treatment framework.

These areas involve additional legal requirements, differing consent standards, or workflow variations that merit separate analysis. Once the foundational framework for automated consent has been validated, this guidance document may be supplemented with additional resources tailored to these other use cases, prioritizing those of greatest urgency or strategic importance to stakeholders.

3.1. Use Case 1: Consent to Share Patient Information from a Part 2 Program for a Treatment Purpose

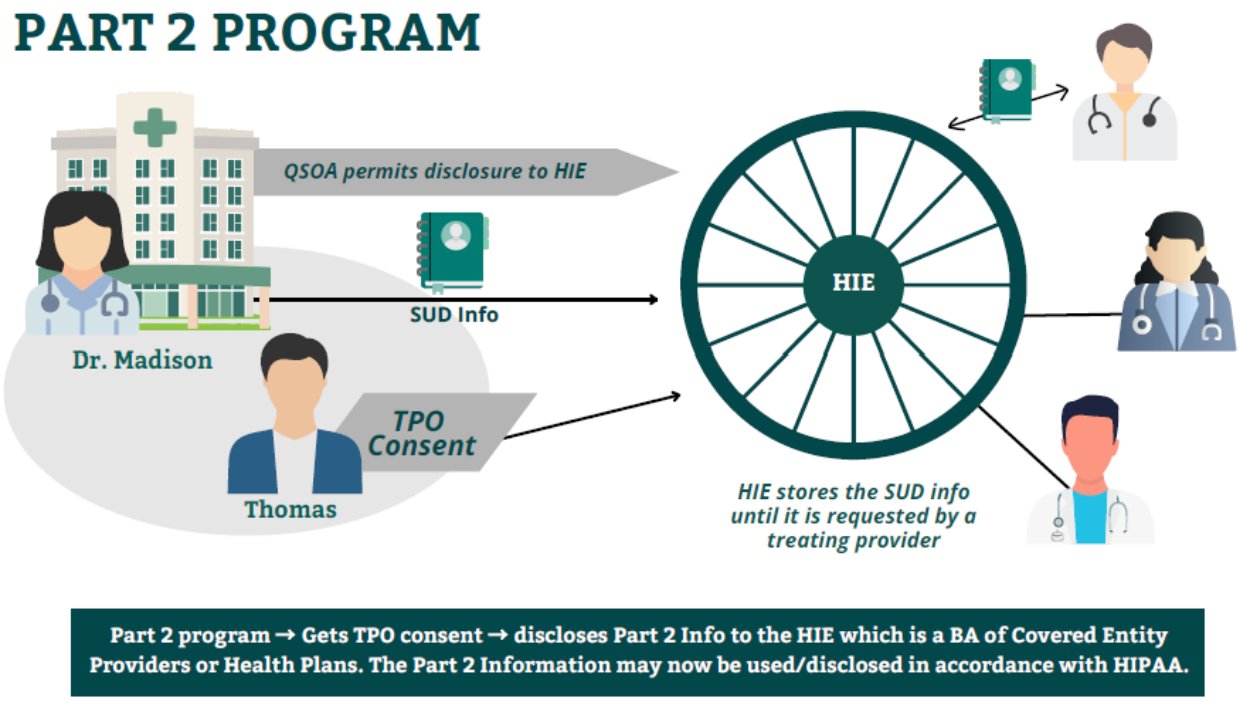

Image independently adapted from the Disclosure of Substance Use Disorder Patient Records: "How Do I Exchange Part 2 Data?" resource from SAMHSA by The Sequoia Project. It is not endorsed or reviewed by any federal agency. It is for educational purposes only. https://www.samhsa.gov/sites/default/files/how-do-i-exchange-part2.pdf

Scenario:

A substance-use-disorder clinic governed by Part 2 (the "**Part 2 provider**") must send a patient's medication list and recent progress notes to the orthopedic surgery department of the Regional Medical Center, where the patient is scheduled for a knee-replacement

procedure. The Regional Medical Center is a general hospital and a HIPAA covered entity health care provider. The Part 2 provider is also a HIPAA covered entity health care provider. Part 2 requires the Part 2 provider to obtain the patient's written consent before sharing this information with Regional Medical Center.

Although Regional Medical Center itself is not a Part 2 Program, its orthopedic surgeons will rely on the information requested from the Part 2 provider for pre-operative planning and post-surgical pain-management coordination. The request for the Part 2 provider's records is initiated by the Regional Medical Center through the state HIE and routed across its TEFCA-designated Qualified Health Information Network (QHIN) to the Part 2 provider. This Use Case seeks to support the Part 2 provider in order for it to disclose the patient's Part 2 protected information to Regional Medical Center for a Treatment purpose.

4. Operationalizing Automated Consent

To enable a Part 2 Program to respond effectively to a request for Part 2-protected information under the Treatment Use Case described above, a structured operational foundation must be established. Implementing automated consent requires alignment across ***legal***, ***technical***, and ***governance*** domains. The following foundational components define the core building blocks necessary to operationalize automated consent in a consistent and scalable manner:

1. **Use Case Selection**
2. **Legal Requirements Identification**
3. **Automated Consent Tool Selection**
4. **Operational Workflow & RACI[1], encompassing:**
    - **Identity Verification**
    - **Consent Collection**
    - **Compliance Satisfaction**
    - **Data Segmentation**
    - **Consent Management**

[1] **RACI stands for: R – Responsible** (the person(s) who performs the work);
A – Accountable (the single individual ultimately answerable for the task's success and who signs off on decisions or deliverables);
C – Consulted (stakeholders who provide input, expertise, or guidance);
I – Informed Individuals or groups who must be kept updated but are not active participants.

5. **Patient Education**
6. **Governance & Oversight**

Each component builds upon the last, forming an iterative framework through which organizations can design, implement, and sustain computable consent operations that are compliant, technically interoperable, and patient centered.

4.1. Use Case Selection

The first step in operationalizing automated consent is to identify and clearly define the use case the organization intends to support. Because automated consent processes are inherently context-dependent, each use case, whether provider-to-payer, provider-to-provider, or patient-directed exchange, presents unique policy and workflow considerations. The data flow, the actors involved, the applicable legal authorities, and the technical requirements all influence how consent must be structured, encoded, and adjudicated.

For the purposes of this guidance document, the use case has been pre-defined as described in Section 3.1 to ensure a common focus and anchor development of reusable tools: a HIPAA –covered entity provider requesting Part 2-protected information from a Part 2 Program via a HIN, using a computable, automated consent to authorize the disclosure for a treatment purpose.

4.2. Legal Requirements Identification

The next critical step in operationalizing automated consent is to identify the federal and state legal requirements that define and control what type of consent must be collected for the use case at issue. For example, these requirements dictate whether consent may be verbal or in writing, and what elements must be included in a consent document. Each consent use case, whether for treatment, payment, research, or another purpose, is shaped by a distinct set of statutory and regulatory obligations. Before deploying an automated consent tool or launching a use case, an organization must carefully analyze these requirements to ensure that any consent captured will be legally valid and enforceable.

Consent requirements vary depending on the governing law and the nature of the data being shared. Not all scenarios demand the same level of consent or the same informational elements. To help frame these distinctions, consent standards can generally be understood through four principal categories:

- **Simple Consent:** A binary choice—such as "yes/no" or "opt-in/opt-out"—is sufficient to meet the applicable legal standard. Example: a patient agreeing to participate in a health information exchange where no additional consent elements are mandated by law.
- **Specific Consent:** A simple binary response is not sufficient. The legal standard requires that specific consent elements be collected, such as identification of the disclosing party, recipient, description of the information, purpose, and expiration, and inclusion of mandatory statements. HIPAA and 42 C.F.R. Part 2 are both examples of Specific Consent frameworks. (See **Appendix 1: Legal Elements of Consent Matrix for HIPAA & 42 C.F.R. Part 2**.)
- **Informed Consent:** Requires the individual to be given meaningful information about the nature, purpose, and potential risks or benefits of authorizing the disclosure. A consent obtained without adequate disclosure of this information may be invalid because it was not made "knowingly" or "voluntarily."
- **Regulated Consent:** Refers to circumstances in which the law or a regulatory agency prescribes an exact form or format that must be used. For example, several states mandate specific pre-approved forms for HIV/AIDS testing or mental health record disclosures, which may not be altered or substituted.

For the current use case, the applicable consent is a Part 2 consent for treatment purposes. Such consent must satisfy all elements required under 42 C.F.R. § 2.31, including the patient's identification, the name of the disclosing program and recipient, a description of the information to be disclosed, the purpose of the disclosure, expiration parameters, signature requirements and mandatory statements. It is also important to note that the elements required for a consent under 42 C.F.R. § 2.31 will vary depending on both the purpose of the disclosure and the intended recipient. In addition, although separate from the consent form, 42 C.F.R. § 2.32 requires that a mandatory redisclosure notice and either a copy of the executed consent or an explanation of the scope of the executed consent accompany all disclosures of Part 2-protected information. When a Part 2 Program is also a HIPAA covered entity, it must additionally comply with HIPAA; however, because HIPAA does not require a signed authorization for disclosures made for treatment, payment, or health care operations (TPO), the Part 2 Program need only meet the Part 2 consent requirements for this use case.

To assist organizations in identifying and confirming the 42 CFR Part 2 required consent elements, a resource, **"Legal Elements of Consent Matrix: HIPAA & 42 C.F.R. Part 2"** (Appendix 1), is provided with this guidance document. This matrix provides a detailed crosswalk that maps every consent component required under Part 2 and highlights distinctions among standard Part 2 consents, TPO consents, and intermediary consents.

Each element, such as patient identification, purpose, expiration, and redisclosure notice, is assigned a unique *Consent Element ID*. These IDs serve as reusable reference points that can be applied across jurisdictions and translated into system logic or data fields, creating a consistent structure for compliance and technical implementation.

In addition, for an organization to fully understand the legal requirements for consent to disclose SUD information, it is necessary to identify the specific laws in the state where the SUD information originates from and confirm whether a state imposes additional or stricter requirements for entities that maintain, create or receive SUD information. These laws may affect consent elements and requirements for consent. Some states directly incorporate Part 2 by reference; others layer additional consent elements; and a few have less stringent provisions.

To help evaluate these differences, organizations may consult the ***50-State SUD Resource*** developed by the George Washington University Hirsch Health Law and Policy Program and the Robert Wood Johnson Foundation, available at www.healthinfolaw.org/comparative-analysis/disclosure-substance-use-records-patient-consent-50-state-comparison-0 (last updated October 4, 2019). That resource compares state SUD consent laws against Part 2, showing which states impose stricter or supplementary requirements and which are governed entirely by Part 2. Users should note that the resource has not been updated since 2019 and certain citations may now be outdated.

To complement the federal matrix in Appendix 1, Appendix 2 includes **"Legal Elements of Consent Matrix: State Law Template",** which mirrors the structure and Consent Element IDs of Appendix 1, enabling users to layer state-specific rules and requirements without losing consistency. By using the two tools together, organizations can maintain a unified compliance framework that satisfies both federal and state law. The recommended approach is to begin with Appendix 1 to establish the baseline HIPAA and Part 2 consent elements, then populate Appendix 2 with any additional state-specific elements. Once completed, the combined matrix serves as a jurisdiction-ready compliance reference that can be directly mapped to workflow logic, system fields, and HL7 FHIR Consent Resources. Together, these matrices provide a structured way for organizations to complete a *risk evaluation* of automated consent tools and electronic workflows against all required legal elements prior to any disclosure, and to confirm that those elements can be validated, transmitted, and enforced in a computable, interoperable format.

4.3. Automated Consent Tool Selection

As the health information ecosystem shifts toward automated consent processes, a growing number of computable consent tools are emerging in the marketplace. Much like

the early wave of EHR systems, these products vary widely in scope, design, and compliance maturity. Because consent functionality is not regulated, certified, or standardized under any federal program, there is currently no assurance that a given tool will meet all applicable legal or interoperability requirements. Consequently, organizations must approach selection and implementation with diligence, ensuring that any automated consent solution they adopt can fully support the chosen use case and comply with the federal and state legal requirements identified in the preceding steps.

The importance of conducting this due diligence cannot be overstated. Without confirming that a tool can capture and express the required consent elements, encode them in a computable form, and enforce them accurately across systems, organizations risk deploying technology that produces invalid or incomplete consent artifacts. This may lead to regulatory non-compliance, data-sharing failures, or patient-trust erosion. For this reason, the first two preparatory steps, *Use Case Selection* and *Legal Requirements Identification***,** are prerequisites to any tool evaluation. Only after those steps are complete should an organization begin assessing technical platforms and vendor products.

To support this evaluation, Appendix 3 provides another practical resource, **"Modular Part 2 Consent: TPO Purposes** (Appendix 3). This tool deconstructs the core legal and operational requirements of a valid 42 CFR Part 2 consent for treatment, payment, and health care operations. It lists each required consent element in modular form, allowing organizations to test whether an automated consent tool can capture, store, and transmit those elements in accordance with applicable law.

When evaluating automated consent tools, organizations should also conduct an assessment that includes, at minimum, the following questions:

1. **Does the tool capture all required consent elements** for the selected use case, both federal and state, and can it represent them in a machine-interpretable format?
2. **Does it implement recognized technical standards**, such as HL7 FHIR Consent, IHE Privacy Consent on FHIR (PCF), or comparable APIs that support interoperability?
3. **Can it accommodate granular consent choices**, allowing patients to authorize or restrict specific data types, recipients, or purposes rather than relying solely on global "all-or-nothing", location or encounter-based permissions?
4. **Does it support consent lifecycle management**, including real-time updates, expiration, and revocation, and can it propagate those changes automatically to all systems holding the data?

5. **Does the tool provide auditable records** of when and how a consent was created, modified, or acted upon, ensuring accountability and compliance traceability?
6. **Can it integrate with existing identity-verification and authentication mechanisms**, confirming that the consent was executed by the correct individual or authorized representative?
7. **Does it include safeguards against unauthorized secondary use or redisclosure**, particularly when interfacing with external data networks or intermediaries?
8. **Can it support data segmentation and tagging**, such that the consent directives remain linked to the appropriate records through the exchange process?
9. **Does the tool enable interoperability with downstream systems**, including HINs, EHRs, and payer platforms, without requiring manual re-entry or translation of consent data?
10. **Is there a governance or validation framework** for how the vendor maintains compliance with updates to HIPAA, 42 CFR Part 2, and state privacy laws?

These questions are not exhaustive but provide a baseline for vetting readiness and maturity. The goal is to ensure that an automated consent solution can (1) translate legal consent elements into structured, machine-readable data, (2) communicate those elements across networks using recognized standards, and (3) enforce consent preferences consistently throughout the data-sharing lifecycle.

In essence, the selection of an automated consent tool is not a purely technical procurement, it is also a compliance and governance decision. The tool chosen must operationalize the organization's legal obligations, reflect the patient's intent with precision, and maintain the fidelity of those directives across every point of exchange. A rigorous evaluation process grounded in the legal matrices (Appendices 1 and 2) and the modular requirements tool (Appendix 3) provides a defensible, repeatable framework for making that determination.

4.4. Operational Workflow & RACI

With the legal foundations established, the next step is to operationalize automated consent through a structured, end-to-end workflow. A practical implementation resource, **"Operational Workflow & RACI for Use Case 1" (Appendix 4),** is provided with this guidance document to guide this process. This tool breaks down each operational task

associated with executing a computable consent for the defined scenario, namely, a Part 2 Program disclosing Part 2-protected information for treatment purposes to a non-Part 2 HIPAA-covered provider through a HIN.

The exhibit organizes implementation into five major process areas:

- **Identity Verification** – Confirming that both the requesting entity and the patient (or authorized representative) are ***correctly identified*** before any disclosure occurs. This includes validating the requestor's credentials through the National Provider Identifier (NPI), HIN, or QHIN participant directories; matching patient identity attributes across systems; and maintaining audit trails to demonstrate due diligence.
- **Consent Collection** – Capturing, validating, and storing the computable consent and its accompanying mandatory redisclosure notice in accordance with 42 C.F.R. §§ 2.31 and 2.32, and the associated HL7 FHIR Consent Resource. The workflow outlines which party (Part 2 Program, HIN, or Business Associate) is *Responsible*, *Accountable*, *Consulted*, and *Informed* (RACI) for each step, from presenting the consent to the patient, through electronic execution, to secure transmission and storage.
- **Data Segmentation** – Tagging the Part 2-protected records so that downstream systems can automatically recognize and honor the patient's consent directives. The workflow references segmentation using ***Data Segmentation for Privacy*** (DS4P) or comparable metadata standards to maintain linkage between the consent artifact and the data it governs.
- **Compliance Satisfaction** – Ensuring all regulatory obligations are met at the time of disclosure. This includes appending the required ***redisclosure notice*** under § 2.32, providing the patient with a copy of the executed consent, providing the recipient with a copy of the executed consent or an explanation of the scope of the executed consent, and confirming that any technical system logs capture evidence of compliance.
- **Consent Management and Revocation** – Maintaining the ***consent lifecycle*** after initial disclosure. The workflow details how revocation requests must be authenticated, logged, and propagated through the HIN and receiving systems so that further use or disclosure ceases automatically upon expiration or withdrawal.

Each of these steps is addressed in detail within the Workflow & RACI Tool, which assigns operational accountability across key roles such as the Part 2 Provider, HIN Operator, Receiving Provider, and, where applicable, Qualified Service Organization (QSO) or

Business Associate. The RACI framework — *Responsible, Accountable, Consulted, Informed* — clarifies who must take action, who must verify completion, and who should be notified at each stage of the process. This ensures clear delineation of responsibilities and reduces the risk of compliance gaps or duplicated effort.

Organizations implementing automated consent can use Appendix 4 as both a blueprint and a project-management tool. By mapping the workflow to existing operational systems, policies, and vendor interfaces, teams can identify where new functionality, governance checkpoints, or technical integrations are required. The exhibit's structure allows each organization to tailor the steps to its internal environment while preserving the standardized sequencing and accountability that underpin compliant Part 2 data exchange.

In summary, the Workflow & RACI for Use Case 1 operationalizes how computable consent moves from concept to execution, detailing *who does what, when, and how*, so that a Part 2 Program can confidently disclose Part 2 records for treatment purposes to a non-Part 2 provider in a manner that is secure, auditable, and fully compliant with federal requirements.

4.5. Patient Education

As the industry transitions toward automated and computable consent, patient education will be one of the most significant and complex challenges. The concept of "automated consent" is not intuitive for most individuals, and confusion about what it means, how it differs from traditional paper forms, how it operates behind the scenes, and how it protects their rights, can quickly undermine trust and participation. Many patients may equate "automation" with loss of control, fearing that their health information will flow without their knowledge or ongoing involvement. Others may assume that electronic consent automatically means broader data sharing, without understanding the precision and safeguards that computable consent enables.

During a recent workgroup for consent which took place during the Civitas Networks for Health conference, numerous stakeholders identified this educational gap as one of the most pressing barriers to adoption, noting that clear, accessible, and consistent communication materials for patients and consumers are urgently needed. Without these resources, even the most well-designed technical and legal frameworks will struggle to gain traction, because effective consent depends on comprehension and trust at the individual level.

Patient education for automated consent must therefore go beyond simply explaining "what consent is." It should aim to help individuals understand:

- How their consent choices are recorded and enforced electronically;
- What rights they retain to revoke or modify consent at any time;
- How computable consent improves accuracy, privacy, and accountability compared to manual paper processes;
- What safeguards and security measures prevent unauthorized access or redisclosure; and
- How automated consent contributes to safer, more coordinated care by ensuring that data flows only as authorized by the individual or permitted by applicable laws.

Developing such educational materials will require multidisciplinary collaboration among legal, technical, and patient-engagement experts to ensure both accuracy and accessibility. The content should be designed for varied literacy levels, available in multiple languages, and delivered in user-friendly formats such as infographics, short videos, FAQs, or patient-portal modules. Ideally, education should occur at multiple points in the care continuum, before, during, and after consent execution, so that patients have repeated opportunities to understand and manage their choices.

At present, no standardized national resources exist to fill this need. The health care community will need to collaborate to develop tools that focus specifically on patient education and engagement. Possible deliverables could include:

- A **"Patient Education Toolkit"** containing model scripts, brochures, and FAQs for use by providers, HINs, and health plans;
- **Plain-language templates** explaining the meaning and implications of computable consent;
- **Digital content modules** that can be embedded into patient portals or HIE interfaces; and
- **Best practice guidance** for providers on how to communicate consent options during clinical or registration workflows.

By prioritizing education as an integral component of implementation, not an afterthought, the health information ecosystem can build patient confidence in automated consent systems and ensure that digital innovation advances alongside informed, voluntary participation.

4.6. Governance & Oversight

Governance and oversight are the mechanisms that ensure automated consent processes operate in a lawful, consistent, and accountable manner once deployed. Even the most sophisticated technical tools require a clear organizational framework to define who is responsible for compliance, how consent policies are enforced, and how risks are identified and mitigated over time. Governance provides that structure; oversight ensures that it is working as intended.

In the context of automated consent, governance refers to the internal policies, procedures, and role assignments that guide how an organization will collect, store, manage, and rely on computable consents. Oversight involves the continuous monitoring and evaluation of those processes to verify that they remain compliant with applicable laws, including 42 C.F.R. Part 2, HIPAA, and relevant state privacy rules, and that they align with the organization's privacy and security posture.

Strong governance begins with the adoption of written policies and procedures that define:

- The legal authorities under which automated consent will be used;
- The roles and responsibilities of staff, Business Associates ("BAs"), and Qualified Service Organizations ("QSOs");
- The technical and administrative safeguards for managing computable consent artifacts;
- The technical processes for verifying consent validity prior to any disclosure;
- How consent revocations and expirations are recognized and acted upon; and
- The documentation and audit mechanisms for demonstrating compliance.

Much like HIPAA requires Business Associate Agreements be entered into between covered entities and their BAs, Part 2 requires that any entity performing functions or services on behalf of a Part 2 Program enter into a Qualified Service Organization Agreement (QSOA). Therefore, governance policies must also address how automated consent workflows are extended to or performed by QSOs and BAs. This includes ensuring that those entities:

- Act strictly "on behalf of" the Part 2 Program;
- Are bound by contractual obligations to comply with Part 2, HIPAA, and all redisclosure prohibitions;

- Maintain technical and procedural controls for safeguarding Part 2 data; and
- Participate in regular oversight or auditing to confirm compliance.

To assist organizations in establishing this foundation, the Workstream developed a model policy titled "**Policy Template: Automated Part 2 Consent (Part 2 Provider**)" (Appendix 5). This template provides a structured framework that Part 2 Programs can use to begin formalizing their internal governance for automated consent. It includes sample policy statements, procedures for validating electronic consent forms, QSOA alignment language, and key decision points for integrating automated consent processes into existing privacy and security programs.

Organizations can adapt this template to reflect their operational realities, technical environments, and contractual relationships. Over time, governance policies should evolve alongside the organization's implementation maturity, moving from initial deployment toward continuous compliance monitoring, workforce training, and periodic policy review.

As automated consent becomes more widespread, future efforts may develop additional governance tools to support multi-party coordination, QSOA/BA oversight, and cross-organizational accountability frameworks. These resources will help ensure that automated consent does not simply function as a technical innovation, but as a legally sound, auditable, and ethically managed process embedded within each organization's compliance ecosystem.

4.7. Future Guidance

This guidance document and its corresponding resources lay the foundation for operationalizing automated consent. This document focuses on treatment disclosures from a Part 2 program to a non-Part 2 HIPAA health care provider; however, additional guidance and resources, including technical, will be needed to address other high-impact areas where legal standards and workflows differ. A near-term needed deliverable is guidance that shows how workflow steps, form fields, and required legal elements translate into the structured data necessary to generate a computable consent artifact for this specific use case. This includes demonstrating how those elements map directly into an HL7 FHIR Consent Resource, creating a clear bridge between operational processes and the technical implementation of computable consent.

Near-term priorities include public health and emergency disclosures, where HIPAA and 42 C.F.R. Part 2 contain specialized provisions and time-critical, multi-party coordination. Guidance should show how computable systems represent and enforce such exceptions while safeguarding privacy.

Other priority areas include individual access services (IAS); access by personal representatives and caregivers (HIPAA's professional-judgment standard vs. Part 2's explicit consent); and research, which needs standardized computable consent models aligned with IRB and privacy requirements.

This phase establishes the operational groundwork. The community will need to work collaboratively to extend these principles across additional use cases and policy domains over time, building a cohesive, interoperable framework so that automated consent can operate confidently, lawfully, and at scale.

5. Appendices

- Appendix 1: Legal Elements of Consent - Part 2 & HIPAA
- Appendix 2: Legal Elements of Consent - State Law Template
- Appendix 3: Modular Part 2 Consent - TPO Purposes
- Appendix 4: Workflow & RACI for Use Case: Part 2 → Non-Part 2 HIPAA Provider (TPO via HIN)
- Appendix 5: Policy Template: Automated Part 2 Consent (Part 2 Provider)

DISCLAIMER NOTE: ALL TOOLS, TEMPLATES, AND INSTRUCTION SHEETS THAT FOLLOW ARE PROVIDED SOLELY FOR INFORMATIONAL AND EDUCATIONAL PURPOSES AS SAMPLES AND EXAMPLES; THEY MAY NOT BE COMPLETE, CURRENT, OR ACCURATE FOR ANY PARTICULAR JURISDICTION OR USE CASE. THEY DO NOT CONSTITUTE LEGAL ADVICE, ARE NOT A SUBSTITUTE FOR INDEPENDENT LEGAL JUDGMENT, AND DO NOT CREATE AN ATTORNEY–CLIENT RELATIONSHIP. ORGANIZATIONS SHOULD CONSULT QUALIFIED LEGAL COUNSEL ABOUT THEIR SPECIFIC CIRCUMSTANCES AND APPLICABLE STATE AND FEDERAL LAW BEFORE RELYING ON OR IMPLEMENTING ANY TOOL, TEMPLATE, OR RELATED MATERIALS. NO REPRESENTATIONS OR WARRANTIES OF ANY KIND (EXPRESS OR IMPLIED) ARE MADE REGARDING THE CONTENT, AND ANY USE IS SOLELY THE RESPONSIBILITY OF THE USER.

Appendix 1:
Legal Elements of Consent – Part 2 & HIPAA

INSTRUCTIONS

Purpose of the Tool

The Legal Elements of Consent tool (the "Tool") is a practical reference that translates the legal requirements for valid patient consent under HIPAA and 42 CFR Part 2 ("Part 2") into clear, structured elements that can be operationalized in electronic consent processes. It is designed to help organizations understand and implement the specific elements needed for compliant consent for uses and disclosures of health information, including consents that involve treatment, payment, health care operations, and information sharing organizations such as HIEs and other health information networks.

What the Tool Provides

The Tool organizes consent requirements into a series of core "consent elements" (for example, C1 through C15) and shows how each element is treated under:

- HIPAA standard authorization elements and requirements
- 42 CFR Part 2 standard consent elements and requirements
- 42 CFR Part 2 consent requirements for treatment, payment, and health care operations
- 42 CFR Part 2 intermediary requirements (i.e., when a legally defined intermediary is the recipient)

For each element, the Tool identifies specific information that must appear in a consent, such as the name of the patient, a description of the information, who may disclose and who may receive the information, the purpose of the disclosure, the expiration, signature, and date. It highlights where HIPAA and Part 2 requirements are the same or materially similar and where they differ, and it flags special rules, including requirements when the recipient is an "intermediary" and when a general designation is used, when the expiration may be stated as "none" or "end of treatment" for treatment, payment, and health care operations purposes, required statements about revocation, consequences of refusal to sign, and redisclosure, as well as additional procedural requirements that accompany use of the consent, such as providing copies of the consent or a clear explanation of its scope to recipients and including the Part 2 redisclosure notice. The Tool also confirms that

electronic documents and electronic signatures can satisfy “in writing” and “signature” requirements where not prohibited by other law.

How the Tool Can Be Used

Organizations can use the Tool in multiple ways, with a particular focus on supporting automated, digital consent. It can serve as a checklist when drafting or updating consent and authorization forms so that each required element under HIPAA and Part 2 is addressed in accordance with regulatory standards, and it can be used to translate those legal elements into data fields for electronic forms, patient portals, and automated or computable consent solutions, ensuring that required content, recipients, purposes, and expiration logic are captured in a structured and reliable way. The Tool can be used to evaluate and validate consent solutions, whether in third-party platforms or as consent functionalities embedded within EHRs, by providing a rigorous reference to confirm that all required Part 2 consent elements are being captured correctly. It can also act as a check against any digital consent workflow under consideration. It can support drafting or updating policies on obtaining, documenting, revoking, and honoring consent, and can be used to train staff on what must be present in a valid consent for different use cases. It can also be used for gap analysis and compliance reviews by comparing existing forms and workflows against legal requirements and quickly identifying missing elements, conflicting terms, or incorrect handling of Part 2 consents, including those involving intermediaries and general designations. In addition, the Tool can inform contracting and due diligence with health IT vendors, HIEs, and other intermediaries by helping to ensure that their systems can honor consent elements and procedural requirements, including redisclosure notices and any copy-to-recipient obligations.

Types of Organizations That May Use the Tool

The Tool is suitable for a wide range of organizations that create, receive, use, or disclose Personal Health Information (PHI) and Part 2 information, including substance use disorder programs and behavioral health providers subject to Part 2, hospitals, health systems, clinics, and physician practices, health information exchanges, health information networks, and other data intermediaries, health plans and other third-party payers that receive or use data under consent, health IT, EHR, and consent management vendors that need to design compliant forms and workflows, as well as compliance officers, privacy officers, security officers, and in house or outside legal counsel supporting HIPAA and Part 2 compliance.

Excluded Topics

The current version of the Tool is focused on core HIPAA and Part 2 consent elements and does not address certain specialized consent scenarios. The following is a non-

exhaustive list of topics that **ARE EXCLUDED** from this Tool and require separate analysis, additional forms, or tailored workflows:

1. Minors
2. Individuals lacking mental capacity and situations involving legal or personal representatives
3. Marketing purposes
4. Research purposes
5. Fundraising purposes
6. Psychotherapy notes
7. SUD counseling notes

Users should **not** rely on this Tool for these excluded topics and should consult additional guidance, forms, and legal advice before designing or implementing consents in those areas.

Note: Cited references in the table below can be found in the endnotes at the end of this document.

ELEMENTS OF CONSENT						
CONSENT ELEMENT	**ELEMENT ID**	**HIPAA** (Core Elements & Requirements)[i]	**42 C.F.R. Part 2** (Standard Requirements)	**42 C.F.R. Part 2** (Consent for TPO)	**42 CFR Part 2** (Intermediary Requirements)	***Notes & Comments***
NAME	**C1**	**Name** of the subject of the PHI.	**Name** of the patient.[ii]	**Name** of the patient.[iii]	☐ **Name** of the patient.[iv]	☑ *The element requirement is the same for HIPAA & Part 2.*
WHAT	**C2**	**Description of the Information** to be used or disclosed identified in a *specific* and *meaningful* fashion.[v]	**Description of the Information** to be used or disclosed identified in a *specific* and *meaningful* fashion.[vi]	**Description of the Information** to be used or disclosed identified in a *specific* and *meaningful* fashion.[vii]	☐ **Description of the Information** to be used or disclosed identified in a *specific* and *meaningful* fashion.[viii]	☑ *The element requirement is the same for HIPAA & Part 2.*
FROM WHO (the Disclosing Party)	**C3**	**Discloser Name** OR other **Specific Identification** of the person(s), or class of persons, authorized to make the requested use or disclosure.[ix]	**Discloser Name** OR other **Specific Identification** of the person(s), or class of persons, authorized to make the requested use or disclosure.[x]	**Discloser Name** OR other **Specific Identification** of the person(s), or class of persons, authorized to make the requested use or disclosure.[xi]	☐ **Discloser Name** OR other **Specific Identification** of the person(s), or class of persons, authorized to make the requested use or disclosure.[xii]	☑ *The element requirement is the same for HIPAA & Part 2.*
TO WHO (the Receiving Party)	**C4.1**	**Recipient - Name** OR other **Specific Identification** of the person(s), or **class of persons**, to whom the covered entity may make the requested use or disclosure.[xiii]	**Recipient - Name(s)** of the person(s), or **class of persons**, to which a disclosure is to be made.[xiv]	For a single consent for all future uses & disclosures for treatment, payment, and health care operations (TPO Consent), the **Recipient** may be described as "***my treating providers, health plans, third-party payers, and people helping to operate this program***" or a similar statement).[xv]	See C4.2	☑ *The element requirement is materially the same for HIPAA & Part 2, including Part 2 consents for treatment, payment, and/or Health Care Operations (HCO) purposes,* ***EXCEPT*** *when the Recipient is an Intermediary.*

ELEMENTS OF CONSENT						
CONSENT ELEMENT	**ELEMENT ID**	**HIPAA** (Core Elements & Requirements)[i]	**42 C.F.R. Part 2** (Standard Requirements)	**42 C.F.R. Part 2** (Consent for TPO)	**42 CFR Part 2** (Intermediary Requirements)	***Notes & Comments***
	C4.2	N/A	N/A	N/A	☐ **Recipient - Intermediary Name** is required[xvi] **PLUS:** ☐ **Name(s)** of the member participants of the Intermediary[xvii] **-OR-** ☐ **General Designation** of a participant(s) or class of participants, which **must be limited** to a participant(s) who has a ***treating provider relationship*** with the patient whose information is being used or disclosed.[xviii]	⊗ *This element is **different** when the Recipient is an **Intermediary**.*[xix]
PURPOSE	**C5**	**Purpose** must be described for each purpose of the requested use or disclosure.[xx]	**Purpose** must be described for each purpose of the requested use or disclosure.[xxi] *Note: A statement **"at the request of the patient"** is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to,*	**Purpose** must be described for each purpose of the requested use or disclosure.[xxiii] *Note: The statement, "**for treatment, payment, and health care operations**" is a sufficient description of the purpose when a patient provides consent once for all such future*	**Purpose** must be described for each purpose of the requested use or disclosure.[xxv] *Intermediary & General Designation Exception: If a General Designation is used to describe the Recipient(s), the purpose(s) for which the Part 2 Information may be used must be limited to*	☑ *Requirement is materially the same for HIPAA & Part 2, including Part 2 consents for treatment, payment, and/or HCO purposes and Intermediaries, **EXCEPT** for Intermediaries when the General Designation is used to*

ELEMENTS OF CONSENT						
CONSENT ELEMENT	**ELEMENT ID**	**HIPAA** (Core Elements & Requirements)[i]	**42 C.F.R. Part 2** (Standard Requirements)	**42 C.F.R. Part 2** (Consent for TPO)	**42 CFR Part 2** (Intermediary Requirements)	***Notes & Comments***
			provide a statement of the purpose.[xxii]	*uses or disclosures for those purposes.*[xxiv]	*only such purposes allowed for a Treating Provider (e.g., Treatment).*	*describe the Recipient(s).*
END DATE	**C6.0**	**Expiration Date** or **expiration event** that relates to the individual or the purpose of the use or disclosure.[xxvi]	An **expiration date** or an **expiration event** that relates to the individual patient or the purpose of the use or disclosure.[xxvii]	An **expiration date** or an **expiration event** that relates to the individual patient or the purpose of the use or disclosure.[xxviii]	An **expiration date** or an **expiration event** that relates to the individual patient or the purpose of the use or disclosure.[xxix]	☑ *Requirement is materially the same for HIPAA & Part 2.*
	C6.1	*N/A. Note: a HIPAA Authorization is not required for TPO purposes. When a HIPAA Authorization is required, "none" is not a permitted End Date.*	⊗ An expiration statement, like "***none***," is only permitted when the purpose of the use or disclosure is for TPO purposes.	The expiration statement may be "end of the treatment" **or "None"** or similar language IF the consent is for a use or disclosure for **treatment, payment, or health care operations.**[xxx]	The expiration statement may be "**end of the treatment**" or "**None**" or similar language IF the consent is for a use or disclosure for **treatment, payment, or health care operations.**[xxxi]	⊗ An expiration statement of "**None**" or similar statement is permitted **only** for **TPO purposes.**
SIGNATURE	**C7.0**	**Signature of Individual required.**[xxxii]	**Signature** of **patient required.**[xxxiii]	**Signature** of **patient required.**[xxxiv]	**Signature** of **patient required.**[xxxv]	☑ *Requirement is materially the same for HIPAA & Part 2.*
	C7.1	**Signature** of a **personal representative** (PR) *permitted* if legally authorized to sign on the Individual's behalf. If signed by a PR, the authorization must also include the PR's **Description of Authority** to act for the Individual.[xxxvi]	**Signature** of (a) a **personal representative** (PR) permitted **only if** the patient has been adjudicated as *lacking the capacity* to make their own health care decisions *or* (b) signature of the Part 2 Program Director is permitted **only if** (i) the patient has NOT been adjudicated as lacking the capacity to make their own health care decisions, and	**Signature** of (a) a **personal representative** (PR) permitted **only if** the patient has been adjudicated as *lacking the capacity* to make their own health care decisions *or* (b) signature of the Part 2 Program Director is permitted **only if** (i) the patient has NOT been adjudicated as lacking the capacity to make their own health care decisions, and	**Signature** of (a) a **personal representative** (PR) permitted **only if** the patient has been adjudicated as *lacking the capacity* to make their own health care decisions *or* (b) signature of the Part 2 Program Director is permitted **only if** (i) the patient has NOT been adjudicated as lacking the capacity to make their own health care decisions, and	⊗ Part 2 and HIPAA are materially different here. A personal representative may only sign on behalf of a patient under Part 2 if the patient has been adjudicated as lacking the capacity to make their own health care decisions.

ELEMENTS OF CONSENT						
CONSENT ELEMENT	**ELEMENT ID**	**HIPAA** (Core Elements & Requirements)[i]	**42 C.F.R. Part 2** (Standard Requirements)	**42 C.F.R. Part 2** (Consent for TPO)	**42 CFR Part 2** (Intermediary Requirements)	***Notes & Comments***
			(ii) the patient for any period suffers from a medical condition that prevents knowing or effective action on their own behalf, and (iii) consent to a use or disclosure is for the sole purpose of obtaining payment for services from a payer or health plan.[xxxvii]	(ii) the patient for any period suffers from a medical condition that prevents knowing or effective action on their own behalf, and (iii) consent to a use or disclosure is for the sole purpose of obtaining payment for services from a payer or health plan.[xxxviii]	(ii) the patient for any period suffers from a medical condition that prevents knowing or effective action on their own behalf, and (iii) consent to a use or disclosure is for the sole purpose of obtaining payment for services from a payer or health plan.[xxxix]	
SIGNATURE DATE	**C8**	**Date** the authorization is signed.[xl]	**Date** on which the consent is signed.[xli]	**Date** on which the consent is signed.[xlii]	**Date** on which the consent is signed.[xliii]	☑ *Requirement is materially the same for HIPAA & Part 2.*
REQUIRED STATEMENTS:						
RIGHT TO REVOKE	**C9**	A statement regarding the Individual's **right to revoke** the Authorization in writing and either: ☐ (A) the ***exceptions*** to the right to revoke and a ***description of how*** the Individual may revoke the HIPAA Authorization; **OR** ☐ (B) to the extent that such right to revoke information is included in the Covered Entity's Notice of Privacy Practices, a ***reference***	A statement regarding the patient's **right to revoke** the consent in writing, except to the extent that the Part 2 program or other Lawful Holder of patient identifying information that is permitted to make the disclosure has already acted in reliance on it, and how the patient may revoke consent.[xlv]	A statement regarding the patient's **right to revoke** the consent in writing, except to the extent that the Part 2 program or other Lawful Holder of patient identifying information that is permitted to make the disclosure has already acted in reliance on it, and how the patient may revoke consent.[xlvi]	A statement regarding the patient's **right to revoke** the consent in writing, except to the extent that the Part 2 program or other Lawful Holder of patient identifying information that is permitted to make the disclosure has already acted in reliance on it, and how the patient may revoke consent.[xlvii]	☑ *Requirement is materially the same for HIPAA & Part 2. HIPAA additionally requires a description of how the Individual may revoke the HIPAA Authorization, which Part 2 does not.*

ELEMENTS OF CONSENT						
CONSENT ELEMENT	**ELEMENT ID**	**HIPAA** (Core Elements & Requirements)[i]	**42 C.F.R. Part 2** (Standard Requirements)	**42 C.F.R. Part 2** (Consent for TPO)	**42 CFR Part 2** (Intermediary Requirements)	***Notes & Comments***
		to the Covered Entity's HIPAA NPP.[xliv]				
RIGHT TO REFUSE	**C10.0**	A statement that the Covered Entity **may <u>not</u>** condition **treatment, payment, enrollment** or **eligibility** for benefits on whether the Individual signs the HIPAA Authorization when HIPAA's prohibition on conditioning of Authorizations applies (see 164.508(b)(4))[xlviii]	N/A	N/A	N/A	⊗ Part 2 does not prohibit conditioning, whereas, if HIPAA requires an Authorization, the covered entity may not condition treatment, payment, enrollment or eligibility on signing such Authorization (Reminder, HIPAA does not require an Authorization for TPO).
		-OR-				
	C10.1	A statement of the ***consequences*** to the Individual of a **refusal to sign** the Authorization when the covered entity can condition treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain such Authorization, when allowed under HIPAA to do so (see 164.508(b)(4)).[xlix]	N/A	A statement of the **consequences** to the patient of a refusal to sign the consent when it is being sought to use or disclose records for treatment, payment, or health care operations.[l]	N/A unless for TPO purposes. in which case it must include a statement of the consequences to the patient of a refusal to sign the consent.	☑ *Requirement to include a statement describing the consequences of refusal to sign is materially <u>the same</u> for HIPAA & Part 2.*
REDICLOSURE NOTICE	**C11**	**<u>Redisclosure Notice</u>.** A statement must be included regarding the potential for information	**<u>Redisclosure Statement</u>.** A patient's written consent to use or disclose Part 2 records/information **<u>must</u>**	**<u>Redisclosure Statement</u>.** A patient's written consent to use or disclose Part 2 records/information for	N/A	⊗ **This requirement is different for HIPAA and Part 2.** Further, the statement

ELEMENTS OF CONSENT						
CONSENT ELEMENT	**ELEMENT ID**	**HIPAA** (Core Elements & Requirements)[i]	**42 C.F.R. Part 2** (Standard Requirements)	**42 C.F.R. Part 2** (Consent for TPO)	**42 CFR Part 2** (Intermediary Requirements)	***Notes & Comments***
		disclosed pursuant to the Authorization to be subject to redisclosure by the recipient and **no longer be protected by HIPAA**.[li]	include a statement regarding the potential for the records used and disclosed to be subject to redisclosures by the Recipient and **no longer protected by 42 CFR Part 2.**[lii]	Treatment, Payment, OR Health Care Operations **must** include a statement if the Recipient is a covered entity or business associate regarding the potential for the records uses and disclosed pursuant to the TPO consent to be subject to redisclosures by the Recipient as permitted by HIPAA, except for uses and disclosures for civil, criminal, administrative, and legislative proceedings against the patient. [liii]		required by Part 2 depends upon the Recipient and whether the consent is a TPO consent or a standard consent.
OTHER REQUIRED STATEMENT(S)	**C12**	N/A	N/A	N/A	N/A	See applicable State law requirements, if any. For example, disclosures of genetic information could require additional notice statements.
ADDITIONAL PROCEDURAL REQUIREMENTS:						
COPY OF CONSENT	**C13**	**Copy to Individual.** *If the covered entity is the one seeking* an Authorization to be signed by the Individual for a use or disclosure of PHI, the covered entity must	**Copy to Recipient. Each** disclosure made with the patient's written consent must be accompanied by a copy of the consent **OR** a clear explanation of the	**Copy to Recipient. Each** disclosure made with the patient's written consent must be accompanied by a copy of the consent **OR** a clear explanation of the	**Copy to Recipient. Each** disclosure made with the patient's written consent must be accompanied by a copy of the consent **OR** a clear explanation of the	⊗ **This requirement is different for HIPAA and Part 2.** HIPAA requires a copy **to the Individual** (Part 2 does NOT) when the covered entity is the

ELEMENTS OF CONSENT						
CONSENT ELEMENT	**ELEMENT ID**	**HIPAA** (Core Elements & Requirements)[i]	**42 C.F.R. Part 2** (Standard Requirements)	**42 C.F.R. Part 2** (Consent for TPO)	**42 CFR Part 2** (Intermediary Requirements)	***Notes & Comments***
		provide the Individual with a copy of the signed Authorization.[liv]	scope of the consent provided.[lv]	scope of the consent provided. [lvi]	scope of the consent provided. [lvii]	one requesting the Authorization to be signed. Part 2 requires a copy of the consent *OR* an explanation of the scope of consent to be provided **to the Recipient** with each disclosure (HIPAA does not).
ELECTRONIC SIGNATURES & DOCUMENTS	**C14**	A valid HIPAA authorization *must be in* ***writing*** *in* ***plain language*** and contain specific elements and statements as required by the HIPAA Privacy Rule.[lviii] Electronic documents, including electronic signature, are sufficient to satisfy the 'in writing' and 'signature' requirements of HIPAA; however, verbal authorizations are not. [lix]	Electronic signatures are permitted to the extent that they are not prohibited by any applicable law.[lx]	Electronic signatures are permitted to the extent that they are not prohibited by any applicable law.[lxi]	Electronic signatures are permitted to the extent that they are not prohibited by any applicable law.[lxii]	☑ *Requirement is materially the same for HIPAA & Part 2.*
OTHER PROCEDURAL REQUIREMENT(S)	**C15**	N/A	**Part 2 Notice to Recipient**: Each disclosure made with the patient's written consent must be ***accompanied by*** one of two statements. The short form statement	**Part 2 Notice to Recipient**: Each disclosure made with the patient's written consent must be ***accompanied by*** one of two statements. The short form statement	**Part 2 Notice to Recipient**: Each disclosure made with the patient's written consent must be ***accompanied by*** one of two statements. The short form statement	⊗ **This requirement is different for HIPAA and Part 2.** HIPAA does not require a Notice to Recipient.

ELEMENTS OF CONSENT						
CONSENT ELEMENT	**ELEMENT ID**	**HIPAA** (Core Elements & Requirements)[i]	**42 C.F.R. Part 2** (Standard Requirements)	**42 C.F.R. Part 2** (Consent for TPO)	**42 CFR Part 2** (Intermediary Requirements)	***Notes & Comments***
			permitted is: "***42 CFR part 2 prohibits unauthorized use or disclosure of these records***."[lxiii]	permitted is: "***42 CFR part 2 prohibits unauthorized use or disclosure of these records***." [lxiv]	permitted is: "***42 CFR part 2 prohibits unauthorized use or disclosure of these records***." [lxv]	

Appendix 2
Legal Elements of Consent – State Law Template

INSTRUCTIONS

The State Law Template tool is designed to help organizations determine how their state's laws governing substance use disorder (SUD) treatment and other sensitive health information overlay and, where applicable, go beyond the federal requirements of 42 CFR Part 2 and HIPAA. For each consent element (e.g., who may disclose, who may receive, description of the information, purpose, expiration, signature, and requirement statements) and each category of sensitive information, users should review state statutes, regulations, and additional steps. In particular, this tool may be used to flag any state law conditions that narrow who may disclose or receive information, and more specific descriptions of the information or purpose, impose different expiration or revocation rules, mandate warnings or notices, or add procedural requirements such as copies, writing, or special signature standards. Those additional state-law requirements may then be incorporated into an organization's evaluation and configuration of automated consent solutions for that state, whether through a third-party consent management tool, a health information exchange solution, or consent functionality embedded within an EHR, so that digital consent workflows capture not only the rigorous federal Part 2 elements, but also any more protective obligations imposed under state law.

ELEMENTS OF CONSENT														
CONSENT ELEMENT	ELEMENT ID	Consent Element Assessment Question	SUD	Mental/ Behavioral Health	Communicable Disease	HIV AIDS	Genetic Tests	Reproductive Care	Gender Affirming Care	Developmental Disabilities	Immunization Records	*Licensed Facility Type*	*Licensed Provider Types*	*Other*
NAME	C1	*Is the Name of the subject of the Information required?*												
WHAT	C2	*Is a specific or general Description of the Information to be used or disclosed required? This can include restrictions like limiting the Information to be used/disclosed to only a specific range of dates, and to only a specific set of providers.*												
FROM WHO (DISCLOSING PARTY)	C3	*Is the Discloser's Specific Name required OR can the Discloser be described as part of a group of person(s), or class of persons, authorized to make the requested use or disclosure?*												

ELEMENTS OF CONSENT														
CONSENT ELEMENT	ELEMENT ID	Consent Element Assessment Question	SUD	Mental/ Behavioral Health	Communicable Disease	HIV AIDS	Genetic Tests	Reproductive Care	Gender Affirming Care	Developmental Disabilities	Immunization Records	*Licensed Facility Type*	*Licensed Provider Types*	*Other*
TO WHO (RECEIVING PARTY)	C4	*Is the Recipient's Specific Name required OR can the Recipient be described as part of a group of person(s), or class of persons, authorized to receive the requested Information?*												
PURPOSE	C5	*Is a description of the Purpose of the requested use or disclosure required? Must each purpose of the requested use or disclosure be described?*												
END DATE	C6	*Is an Expiration Date or expiration event allowed or specifically dictated?*												
SIGNED	C7	*Is the Subject's Signature required? Are there any specific restrictions or requirements regarding signatures, such as when a personal representative may sign?*												
SIGN DATE	C8	*Is a signature Date required?*												

ELEMENTS OF CONSENT														
CONSENT ELEMENT	ELEMENT ID	Consent Element Assessment Question	SUD	Mental/ Behavioral Health	Communicable Disease	HIV AIDS	Genetic Tests	Reproductive Care	Gender Affirming Care	Developmental Disabilities	Immunization Records	*Licensed Facility Type*	*Licensed Provider Types*	*Other*
REQUIRED STATEMENTS:														
RIGHT TO REVOKE	C9	*Is there a requirement to include a statement regarding the Individual's right to revoke the consent?*												
RIGHT TO REFUSE	C10	*Is there a requirement to include a statement in the consent or otherwise notify the Individual regarding the Individual's right to refuse to sign the consent?*												
REDICLOSURE NOTICE	C11	*Is there a requirement to include a statement in the consent or otherwise notify the Individual that this Type of Information is subject to redisclosure by the Recipient and no longer protected by the applicable State Law?*												
OTHER REQUIRED STATEMENT(S)	C12	*Any other specific statements required under State Law?*												

ELEMENTS OF CONSENT														
CONSENT ELEMENT	ELEMENT ID	Consent Element Assessment Question	SUD	Mental/ Behavioral Health	Communicable Disease	HIV AIDS	Genetic Tests	Reproductive Care	Gender Affirming Care	Developmental Disabilities	Immunization Records	*Licensed Facility Type*	*Licensed Provider Types*	*Other*
PROCEDURAL REQUIREMENTS:														
COPY	C13	*Is there a requirement to provide a Copy of the signed consent to the Individual?*												
WRITING	C14	*Is there a requirement that the consent must be in writing?* *Does State Law prohibit the consent from being captured:* - *Electronically?* - *Verbal?* - *Verbal + reduced to writing?*												
OTHER PROCEDURAL REQUIREMENT(S)	C15	*Any other specific requirements under State Law?*												

Appendix 3
Modular Part 2 Consent – TPO Purposes

INSTRUCTIONS

This tool provides a modular 42 C.F.R. Part 2 ("Part 2") patient consent form specifically for disclosures of Part 2 records for treatment, payment, and health care operations (TPO) and is not intended for any other purposes. It organizes each required consent element (C1, C2, C3, etc.) into clearly labeled fields so it can be implemented on paper or translated directly into an electronic or computable consent format. It can be adopted as-is or customized with a specific Part 2 program's name, state law overlays, and branding, and then used as the primary design blueprint when building or configuring digital consent workflows in an EHR, patient portal, HIE or HIN solution, or a third party consent platform, ensuring that each required Part 2 TPO element (such as the description of information, disclosing entity, recipient or recipients, purpose, expiration, revocation rights, redisclosure statement, and Part 2 notice) is captured in a structured way and available for automated enforcement. This tool provides a practical bridge between the legal requirements and the actual consent fields to be implemented for TPO and can be used as a checklist to evaluate whether any proposed automated consent solution fully and accurately reflects the rigorous consent content required for Part 2 TPO disclosures.

ID	Element	Description / Language	Field / Response
C1	Patient Name	Full Legal Name of Patient:	First Name: Last Name:
C2	Description of Information to Be Disclosed ("Shared")	I agree that records about my care can be used and shared as checked:	☐ All my drug and alcohol records that the Disclosing Entity has that are protected by 42 C.F.R. Part 2 ☐ Specific drug and alcohol records only (list records to be shared):
C3	Disclosing Entity	Name of Part 2 Program or Provider that can use and share my records:	_____ ("Disclosing Entity")
C4	Recipient(s)	I agree the Disclosing Entity can share my records with:	☐ My treating providers, health plans, third-party payers, and persons helping to operate this program (for TPO purposes) ☐ Specific person(s) or entity: _____ ("Recipient(s)")
C5	Purpose of Disclosure	The purposes ("reasons") my records can be shared are:	☑ Treatment ☑ Payment ☑ Health Care Operations
C9	Right to Revoke Statement	**I can revoke this consent (change my mind) at any time in writing, except to the extent that the Disclosing Party has already used this Consent to share my records. I can change my mind by writing to:** _____	
C10.1	Consequences of Refusal	**I do not have to sign this Consent. If I do not sign this Consent, the Disclosing Party might not be able to care or get care for me, get paid or carry out certain health care activities.**	
C.11	Part 2 Redisclosure Statement	**When my drug and alcohol records are used and shared with the Recipient(s), my records could be redisclosed (shared again) by the Recipient(s). This means they could no longer be protected by 42 C.F.R. Part 2, a federal law that protects some drug and alcohol records. If the Recipient(s) is a covered entity or a business associate under a federal law called HIPAA, the Recipient could share my records if allowed by HIPAA, except for uses and disclosures for civil, criminal, administrative, and legislative proceedings against me.**	

C6.1	Expiration Date or Event	This Consent will last until:	☐ Until the end of my treatment ☐ Until I change my mind by writing to the address above ☐ Other date or event: _____
C7	Signature	Signature of Patient:	
C8	Date Signed	Date consent is executed:	_____/_____/20_____
C13	Copy of Consent	A copy of this consent or a clear explanation of the scope of the consent must be provided to the Recipient.	
C15	Part 2 Notice to Recipient	**NOTICE TO RECIPIENT: 42 CFR Part 2 prohibits unauthorized use or disclosure of these records.**	

Appendix 4
Workflow & RACI for Use Case

Health System Workflow:

Part 2 Program → Non-Part 2 HIPAA Provider (TPO via a HIN)

1 Intake & Verification (Performed by Part 2 Program or HIN/HIE)

- Patient/Member Consent Verification: Confirm the identity/authority of the patient or personal representative providing consent. Document verification in the system of record. Note: This step may be performed by the HIN/HIE.
- Recipient Verification: Confirm the identity and authority of the receiving organization/provider requesting PHI. Validate participation in the HIN and role credentials. Note: This step may be performed by the HIN/HIE.

2 Consent Management

- Capture Part 2-compliant consent (written or electronic, per 42 CFR §2.31).
- Store in an enterprise consent service (preferably as a FHIR Consent resource).
- Map consent to the HIN security model to enforce query/response restrictions.
- Include all required attributes: description of PHI, recipient, purpose, expiration (if applicable), patient signature/date.
- Note: Reference Appendix 3 for Part 2 TPO Consent

3 Pre-Disclosure Validation

- Request through HIN is logged and routed to Part 2 program.
- Validate:
  - Consent is active and covers the recipient and purpose.
  - Requested data aligns with consent scope and minimum necessary.

4 Data Segmentation & Packaging

- Label Part 2 records with:
  - HL7 confidentiality code (42CFRPart2) or FHIR security Label.
  - Consent identifier for audit linkage.
- Apply segmentation so only permitted fields leave the system.
- Package in agreed HIN exchange format (FHIR, CCD, IHE).

5 Secure Transmission

- Use HIN-approved secure protocols (FHIR REST, IHE XDS.b, Direct).
- Authenticate with HIN federation (UDAP/OAuth, SAML).
- Transmit with every disclosure:
  1. Copy of the consent or explanation of consent (either or)
  2. Part 2 Notice to Recipient (exact required language).

6 Receipt & Use by Non-Part 2 Provider

- Recipient verifies:
  - Sender's authentication and integrity.
  - Attached consent metadata.
- Store data with Part 2 tags preserved.
- Display redisclosure notice using exact prescribed language:
  - "42 CFR part 2 prohibits unauthorized use or disclosure of these records."
- Enforce redisclosure restrictions in workflows and downstream systems. This includes uses and disclosures for civil, criminal, administrative, and legislative proceedings against the patient.

7 Logging & Accounting

- Both sender and HIN log: patient, purpose, recipient, dataset, timestamp.
- Link disclosure logs to consent ID.
- Make logs available to patient upon request.
- Retain disclosures for 6 years.
- Retain consents/authorizations for 6 years from the date of expiration or revocation.

8 Ongoing Oversight

- Revocation: Enforce immediate removal/termination of access when revoked.
- Expiration: Treat separately from revocation.
- TPO consents may be designed without expiration (per 42 CFR §2.31(a)(7)); valid unless revoked.
- If expiration dates are used, enforcement may be shared between Part 2 staff and the HIN/HIE consent engine/software.
- **Auditing:**
  - Audit both disclosures and consents/authorizations periodically.
  - Confirm compliance and detect misuse (e.g., that only TPO consents are being applied).

RACI: Health System Workflow

Part 2 → Non-Part 2 Disclosure via HIN

Roles

- **Part 2 Program Staff (P2P)** – staff managing SUD treatment records & disclosure
- **HIN/HIE Operator (HIN)** – network services handling routing, authentication, consent engine
- **Non-Part 2 Provider (NPP)** – receiving HIPAA-covered entity/provider
- **Privacy/Compliance Officer (PCO)** – oversight, audits, regulatory compliance

Workflow Step	Part 2 Program Staff	HIN/HIE Operator	Non-Part 2 Provider	Privacy/Compliance Officer
1. Intake & Verification	R (verify patient consent authority; verify sending program identity)	A/R (verify recipient identity & HIN participation)	I	C (ensure verification policy in place)
2. Consent Management	A/R (capture, document, and store Part 2-compliant consent)	C (enforce consent rules in consent engine/security model)	I	C (verify compliance with §2.31 requirements)
3. Pre-Disclosure Validation	A/R (validate consent scope, purpose, minimum necessary)	R (log and route request)	I	C (confirm compliance in process design)

Workflow Step	Part 2 Program Staff	HIN/HIE Operator	Non-Part 2 Provider	Privacy/Compliance Officer
4. Data Segmentation & Packaging	A/R (apply Part 2 confidentiality tags, segment data)	C (enforce HIN formatting rules, enforce consent-linked queries)	I	C (validate tagging & segmentation procedures)
5. Secure Transmission	R (prepare disclosure, apply metadata)	A/R (secure delivery, authentication, ensure redisclosure notice + consent copy/explanation transmitted)	I	C (ensure protocols align with policy)
6. Receipt & Use by Non-Part 2 Provider	I	I	A/R (verify consent metadata, store with tags, display redisclosure banner with required language)	C (audit provider compliance periodically)
7. Logging & Accounting	R (log disclosures, link to consent ID)	A/R (maintain system logs, support accounting requests)	I	C (audit logs, ensure 6-year retention from expiration/revocation)

Workflow Step	Part 2 Program Staff	HIN/HIE Operator	Non-Part 2 Provider	Privacy/Compliance Officer
8. Ongoing Oversight	R (track revocations, coordinate on expirations if applicable)	A/R (enforce revocation and expiration rules in consent engine/software)	I	A (audit disclosures & consents; verify compliance and misuse prevention)

Appendix 5
Policy Template

INSTRUCTIONS:

This Automated Part 2 Consent Policy is a sample governance framework that a Part 2 Program can adopt or adapt to guide its transition to computable, automated consent for disclosures of SUD information. It explains how the organization will select, validate, and use a computable consent tool so that every electronic consent captured (for example via HL7 FHIR Consent) includes all legal elements required under 42 C.F.R. Part 2 and applicable state law, is linked to the data it governs, and can be reliably enforced, revoked, audited, and monitored across systems and partners. By adopting this policy, a Part 2 Program can clearly define roles and responsibilities (such as privacy, security, clinical, and IT functions), set expectations for QSOs, HIEs, and other vendors, and ensure that any automated consent solution, whether part of an EHR or a third party platform, is evaluated and operated in a way that preserves patient confidentiality while supporting lawful treatment, payment, and health care operations.

Automated Part 2 Consent Policy
(for Part 2 Programs)

1. Purpose

The purpose of this policy is to establish the framework by which **[ORGANIZATION NAME]** ("**the Program**") implements, manages, and oversees **automated or computable consent processes** for the disclosure of substance use disorder ("SUD") information under 42 C.F.R. Part 2 ("SUD Consents").

This policy ensures that the Program's use of automated consent tools complies with all applicable federal and state confidentiality requirements, supports lawful data exchange for treatment, payment, and health care operations ("TPO"), and preserves the privacy rights of patients receiving SUD services.

2. Scope

This policy applies to all workforce members, contractors, vendors, Qualified Service Organizations (QSOs), and Business Associates (BAs) who create, maintain, receive, or transmit Part 2 records or related consent artifacts on behalf of the Program. It governs every activity involving the creation, execution, storage, validation, transmission, or revocation of automated or computable SUD Consents.

3. Definitions

"Automated (Computable) Consent" means a machine-readable, standards-based representation of an individual's consent that can be electronically adjudicated and enforced across systems (e.g., HL7 FHIR Consent Resource).

"Part 2 Program" means an individual or entity that holds itself out as providing, and provides, SUD diagnosis, treatment, or referral for treatment as defined in 42 C.F.R. § 2.11.

"Qualified Service Organization" or "QSO" means a person or entity providing services to a Part 2 Program under a written QSO Agreement meeting 42 C.F.R. § 2.11 and § 2.12(c)(4). This includes, but is not limited to, entities such as Health Information Exchanges (HIEs) and Health Information Networks (HINs) that receive, maintain, use, or transmit Part 2 records on behalf of one or more Part 2 Programs to facilitate lawful data exchange or interoperability services (e.g., consent management, secure data routing, or patient-matching) consistent with Part 2 and HIPAA.

"Computable Consent Tool" means an electronic platform capable of capturing, encoding, and managing patient consents in a machine-interpretable form consistent with 42 C.F.R. Part 2 and applicable state law.

4. Policy Statement

[ORGANIZATION NAME] will obtain and manage patient consent for disclosure of Part 2-protected information using secure, automated, and computable consent mechanisms that:

1. Capture every consent element required under 42 C.F.R. §§ 2.31 – 2.33 and applicable state law;
2. Are executed by the patient or authorized personal representative;
3. Are stored and transmitted in structured, interoperable, and machine-readable formats using recognized standards (e.g., HL7 FHIR Consent);
4. Maintain a persistent link between each consent artifact and the data it governs through metadata tagging or data segmentation;
5. Provide the ability to verify, expire, or revoke consents automatically; and
6. Generate an auditable record of all consent-related actions for compliance and quality assurance.

5. Roles and Responsibilities

Role	Responsibilities
Privacy Officer / Compliance Officer	Approves automated consent tools before use; oversees compliance with Part 2 and HIPAA; oversees audits and workforce training.
Information Security Officer	Confirms that technical systems meet required safeguards; validates secure transmission, storage, and access controls for consent data.
Clinical and Intake Staff	Present and explain consent options to patients; use the approved consent tool; verify patient identity before consent execution.
Health Information Network (HIN) / Exchange Partner	Disclose or receive Part 2 data only when supported by valid computable consent; honor redisclosure restrictions.
Qualified Service Organizations / Business Associates	Perform consent-related functions strictly "on behalf of" the Program under a QSOA or BAA; maintain required safeguards and cooperate in audits.

6. Procedures

6.1 Tool Selection and Validation

- The Program will evaluate any automated consent tool to confirm that it captures all required legal elements, supports HL7 FHIR Consent standards, and provides revocation and audit functionality.
- Validation results will be documented and approved by the Privacy Officer before implementation.

6.2 Consent Collection

- A valid computable consent must be obtained prior to any disclosure of Part 2 records except in medical emergencies and other exceptions permitted by Part 2.
- The consent must include all required elements (§ 2.31) and be linked to the specific records disclosed.
- The Program will verify patient identity and authorization before accepting or transmitting consent.

6.3 Redisclosure Notice and Documentation

- Every disclosure of Part 2 information shall include the Part 2 Notice to Recipient required by § 2.32.
- An electronic copy of each executed consent will be retained for a minimum of six (6) years or as required by state law.

6.4 Revocation and Expiration

- Revocations will be processed promptly upon receipt, verified for authenticity, and propagated to all systems and partners holding the data.
- Expired consents will be automatically flagged, and no further disclosures will be permitted under them.

6.5 Audit and Monitoring

- The Privacy Officer will conduct periodic audits to ensure that all disclosures are supported by valid, unexpired consents.
- Audit logs will be reviewed to confirm revocations and redisclosure notices are properly managed.

7. Qualified Service Organization Agreement (QSOA) Provisions

When engaging a QSO to perform functions such as consent management, storage, or identity verification, the QSOA must include language that:

1. Binds the QSO to full compliance with 42 C.F.R. Part 2;
2. Prohibits independent use or redisclosure of Part 2 records or consent artifacts;
3. Requires the QSO to maintain appropriate technical and administrative safeguards;
4. Confirms that the QSO acts solely “on behalf of” the Program and under its direction; and
5. Requires prompt notification to the Program of any breach or unauthorized disclosure involving Part 2 data or consent records.

8. Training and Awareness

All workforce members who access Part 2 records or use automated consent systems must complete initial and annual training on:

- Legal requirements under Part 2 and applicable state laws;
- Proper use of the computable consent tool;
- Revocation and redisclosure procedures; and
- Incident reporting and compliance escalation.

Completion records shall be maintained for audit purposes.

9. Oversight and Review

The Privacy Officer shall review this policy at least annually or earlier if there are material changes to law, regulation, or technology. Revisions must be approved by Program leadership and communicated to all affected personnel.

Periodic audits, incident reports, and patient feedback will inform continuous improvement of automated consent operations.

10. Future Development

Recognizing that standards and technologies for automated consent continue to evolve, **[ORGANIZATION NAME]** may develop additional policies, procedures, and technical guidance to enhance its governance framework over time. Potential future resources include:

- Detailed technical specifications for consent system interoperability;
- Patient education materials explaining automated consent in plain language; and
- Periodic risk assessments to evaluate compliance with emerging federal and state requirements.

Effective Date: ____ / ____ / _____
Approved By: _____
Version: 1.0

ENDNOTES (*Note: the following endnotes correspond to Appendix 1):*
[i] 45 C.F.R. 164.508(c).
[ii] 42 C.F.R. 2.31(a)(1).
[iii] 42 C.F.R. 2.31(a)(1).

[iv] 42 C.F.R. 2.31(a)(1).
[v] 45 C.F.R. 164.508(c)(1)(i).
[vi] 42 C.F.R 2.31(a)(3).
[vii] 42 C.F.R 2.31(a)(3).
[viii] 42 C.F.R 2.31(a)(3).
[ix] 45 C.F.R. 164.508(c)(1)(ii).
[x] 42 C.F.R. 2.31(a)(2).
[xi] 42 C.F.R. 2.31(a)(2).
[xii] 42 C.F.R. 2.31(a)(2).
[xiii] 45 C.F.R. 164.508(c)(1)(iii).
[xiv] 42 C.F.R. 2.31(a)(4)(i).
[xv] 42 C.F.R. 2.31(a)(4)(i).
[xvi] 42 C.F.R. 2.31(a)(4)(ii).
[xvii] 42 C.F.R. 2.31(a)(4)(ii)(A).
[xviii] 42 C.F.R. 2.31(a)(4)(ii)(B).
[xix] 42 C.F.R. 2.11. An "Intermediary" is defined as a person, other than a Part 2 Program, HIPAA Covered Entity, or HIPAA Business Associate, who has received records under a ***general designation*** in a written patient consent to be disclosed to one or more of its member participant(s) who has a treating provider relationship with the patient.
[xx] 45 C.F.R. 164.508(c)(1)(iv). A statement "*at the request of the individual*" is a sufficient description of the purpose when an individual *initiates* the authorization and does not, or elects not to, provide a statement of the purpose.
[xxi] 42 C.F.R. 2.31(a)(5).
[xxii] 42 C.F.R. 2.31(a)(5)(i).
[xxiii] 42 C.F.R. 2.31(a)(5).
[xxiv] 42 C.F.R. 2.31(a)(5)(ii).
[xxv] 42 C.F.R. 2.31(a)(5).
[xxvi] 45 C.F.R. 164.508(c)(1)(v). The statement "end of the research study," "none," or similar language is sufficient if the authorization is for a use or disclosure of protected health information for research, including for the creation and maintenance of a research database or research repository.
[xxvii] 42 C.F.R. 2.31(a)(7).
[xxviii] 42 C.F.R. 2.31(a)(7).
[xxix] 42 C.F.R. 2.31(a)(7).
[xxx] 42 C.F.R. 2.31(a)(7).
[xxxi] 42 C.F.R. 2.31(a)(7).
[xxxii] 45 C.F.R. 164.508(c)(1)(vi).
[xxxiii] 42 C.F.R. 2.31(a)(8). NOTE: Under this provision, if a person other than the patient is signing on the patient's behalf, the patient must first be "adjudicated" as lacking the capacity to make their own health care decisions.
[xxxiv] 42 C.F.R. 2.31(a)(8). NOTE: Under this provision, if a person other than the patient is signing on the patient's behalf, the patient must first be "adjudicated" as lacking the capacity to make their own health care decisions.
[xxxv] 42 C.F.R. 2.31(a)(8). NOTE: Under this provision, if a person other than the patient is signing on the patient's behalf, the patient must first be "adjudicated" as lacking the capacity to make their own health care decisions.
[xxxvi] 45 C.F.R. 164.508(c)(1)(vi).
[xxxvii] 42 C.F.R. 2.15(a) and 2.31(a)(8). A Personal Representative means a person who has authority under applicable law to act on behalf of a patient who is an adult or an emancipated minor in making decisions related to health care. 42 C.F.R. 2.11.
[xxxviii] 42 C.F.R. 2.15(a) and 2.31(a)(8). A Personal Representative means a person who has authority under applicable law to act on behalf of a patient who is an adult or an emancipated minor in making decisions related to health care. 42 C.F.R. 2.11.

[xxxix] 42 C.F.R. 2.15(a) and 2.31(a)(8). A Personal Representative means a person who has authority under applicable law to act on behalf of a patient who is an adult or an emancipated minor in making decisions related to health care. 42 C.F.R. 2.11.
[xl] 45 C.F.R. 164.508(c)(1)(vi).
[xli] 42 C.F.R. 2.31(a)(9).
[xlii] 42 C.F.R. 2.31(a)(9).
[xliii] 42 C.F.R. 2.31(a)(9).
[xliv] 45 C.F.R. 164.508(c)(2)(i).
[xlv] 42 C.F.R. 2.31(a)(6).
[xlvi] 42 C.F.R. 2.31(a)(6).
[xlvii] 42 C.F.R. 2.31(a)(6).
[xlviii] A covered entity **may NOT condition the provision to an individual of treatment, payment, enrollment in the health plan, or eligibility for benefits** on the provision of an Authorization, **except**:(i) A covered health care provider may condition the provision of research-related treatment on provision of an Authorization for the use or disclosure of PHI for such research under this section; (ii) A health plan may condition enrollment in the health plan or eligibility for benefits on provision of an Authorization requested by the health plan prior to the Individual's enrollment in the health plan, if: (A) The Authorization sought is for the health plan's eligibility or enrollment determinations relating to the Individual or for its underwriting or risk rating determinations; and (B) The Authorization is not for a use or disclosure of psychotherapy notes pursuant to a specific Authorization for such specific PHI (i.e., psychotherapy notes). 45 C.F.R. 164.508(b)(4)(i) & (ii). Additionally, a covered entity may condition the provision of health care that is solely for the purpose of PHI for disclosure to a third party on provision of an Authorization for the disclosure of the PHI to such third party. 45 C.F.R. 164.508(b)(4)(iii).
[xlix] A covered entity **may NOT condition the provision to an individual of treatment, payment, enrollment in the health plan, or eligibility for benefits** on the provision of an Authorization, **except**:(i) A covered health care provider may condition the provision of **research-related treatment** on provision of an Authorization for the use or disclosure of PHI for such research under this section; (ii) A health plan may condition enrollment in the health plan or eligibility for benefits on provision of an Authorization requested by the health plan prior to the Individual's enrollment in the health plan, if: (A) The Authorization sought is for the health plan's eligibility or enrollment determinations relating to the Individual or for its **underwriting or risk rating** determinations; **and** (B) The Authorization is not for a use or disclosure of psychotherapy notes pursuant to a specific Authorization for such specific PHI (i.e., psychotherapy notes). 45 C.F.R. 164.508(b)(4)(i) & (ii). Additionally, a covered entity may condition the provision of health care that is solely for the purpose of PHI for disclosure to a third party on provision of an Authorization for the disclosure of the PHI to such third party. 45 C.F.R. 164.508(b)(4)(iii).
[l] 42 C.F.R. 2.31(a)(10)(ii).
[li] 45 C.F.R. 164.508(c)(2)(iii).
[lii] 42 C.F.R. 2.31(a)(10)(i).
[liii] 42 C.F.R. 2.31(a)(4)(ii).
[liv] 45 C.F.R. 164.508(c)(4).
[lv] 42 C.F.R. 2.32(b).
[lvi] 42 C.F.R. 2.32(b).
[lvii] 42 C.F.R. 2.32(b).
[lviii] 45 C.F.R. 164.508(b)(1).
[lix] See 65 Fed. Reg. 82,462, 82,660 (Dec. 28, 2000). In the HIPAA Privacy Rule preamble, HHS clarifies: "Response: All authorizations must be in writing and signed. **We intend e-mail and electronic documents to qualify as written documents. Electronic signatures are sufficient**, provided they meet standards to be adopted under HIPAA. In addition, we do not intend to interfere with the application of the Electronic Signature in Global and National Commerce Act. Comment: Some commenters requested that we permit covered entities to use and disclose protected health information pursuant to verbal authorizations. Response: To ensure compliance and mutual understanding between covered entities and individuals, we require all authorizations to be in writing."
[lx] 42 C.F.R. 2.31(a)(8).

[lxi] 42 C.F.R. 2.31(a)(8).
[lxii] 42 C.F.R. 2.31(a)(8).
[lxiii] 42 C.F.R. 2.32(a)(2).
[lxiv] 42 C.F.R. 2.32(a)(2).
[lxv] 42 C.F.R. 2.32(a)(2).