PATIENT SAFETY ORGANIZATION (PSO) LISTING GUIDE

What is the PSO Listing Guide?

The PSO Listing Guide is an informal educational resource to help readers locate and learn about the requirements for PSO listing under the Patient Safety and Quality Improvement Act of 2005 (Patient Safety Act) and its implementing regulation (Patient Safety Rule). This Guide does not represent the only possible approach to thinking about the requirements, and AHRQ may revise it over time. This Guide does not constitute legal advice, and is not law, regulation, or official policy. It does not establish standards or requirements beyond those incorporated in the text of the Patient Safety Rule and does not confer any rights on any person or entity.

Who is the PSO Listing Guide for?

The PSO Listing Guide is intended to help prospective and listed PSOs understand the requirements underlying their attestations and their related compliance obligations. The individual who signs a Certifications for Initial or Continued Listing Form on behalf of a prospective or listed PSO is certifying that the attestations made on the form were made in good faith and are true, complete, and correct to the best of their knowledge and belief. It may also be of interest to contractors that work with PSOs, healthcare providers who either currently work with a PSO or are considering doing so, and entities that have organizational relationships with PSOs.

What will you find in this Guide?

This Guide contains links to references, tools, and self-assessment resources helpful to understanding the PSO listing requirements in the Patient Safety Act and Rule.

Technical Assistance is Available

AHRQ administers the provisions of the Patient Safety Rule relating to listing and operation of PSOs that are the focus of this Guide. The AHRQ PSO team provides technical assistance free of charge to PSOs and entities interested in becoming a PSO. A number of helpful resources, including some in this Guide, are available at: https://pso.ahrq.gov/.

The HHS Office for Civil Rights (OCR) is responsible for interpretation and enforcement of the confidentiality provisions that protect patient safety work product (PSWP) and the exceptions to confidentiality. AHRQ can arrange technical assistance with OCR for PSOs and entities interested in becoming a PSO that have specific questions about the confidentiality requirements.

Agency for Healthcare Research and Quality

PATIENT SAFETY

AHRQ encourages PSOs and entities interested in becoming PSOs to request technical assistance as early and as often as needed. Technical assistance can help both new and experienced PSOs avoid compliance pitfalls, especially when undertaking a new activity or business relationship. While AHRQ has the authority to delist a PSO for failure to correct a deficiency and OCR has the authority to impose a civil money penalty for knowing or reckless violations of the confidentiality requirements, the Patient Safety Rule authorizes both AHRQ and OCR to work with PSOs to help them comply voluntarily and avoid the need for enforcement action. To request technical assistance, send an e-mail to the AHRQ PSO email box at pso@ahrq.hhs.gov.

PSO Listing Guide Sections

The Section numbers are for reference only. The content may be reviewed in any order.

1. **Organizations and Relationships**
2. **Resources Related to the Patient Safety and Quality Improvement Act of 2005**
3. **Become a PSO**
4. **Maintain a PSO Listing**
5. **Listing Self-Assessment Questions and Compliance Resources**

Section 1. Organizations and Relationships

Introduction

Congress authorized the Secretary of the U.S. Department of Health and Human Services (HHS) to implement and enforce the Patient Safety and Quality Improvement Act of 2005 (Patient Safety Act). HHS carries out these responsibilities through the HHS Agency for Healthcare Research and Quality and its contractors and the HHS Office for Civil Rights. This section describes the roles of these agencies and contractors in relation to Patient Safety Organizations (PSOs).

Agency for Healthcare Research and Quality (AHRQ)

AHRQ is the lead Federal agency charged with improving the safety and quality of healthcare. The AHRQ PSO Program is a Division within the AHRQ Center for Quality Improvement and Patient Safety. It implements the Patient Safety Act and Patient Safety Rule provisions related to PSOs and the network of patient safety databases (NPSD). The PSO Program oversees the PSO listing process, development and maintenance of the AHRQ Common Formats and the NPSD, and provides technical assistance to PSOs, providers and the public. Widespread use of the AHRQ Common Formats and voluntary contributions of data by PSOs to the NPSD make it possible to aggregate and analyze patient safety information from healthcare providers across the country, which can accelerate national learning about patient safety.

Contractors provide support to the PSO Program for some tasks related to the Common Formats and NPSD:

- **PSO Privacy Protection Center (PSOPPC)**
  The PSOPPC receives Common Formats data voluntarily submitted by PSOs and ensures it is nonidentifiable as required by the Patient Safety Act and Patient Safety Rule before submitting it to the NPSD. The PSOPPC also maintains AHRQ's Common Formats. The PSOPPC is developing a tool on the PSOPPC website that any member of the public can use to submit comments on the Common Formats beginning with the release of each new or updated version and continuing thereafter. The PSOPPC convenes an Expert Panel to review the public comments and provide feedback for AHRQ's consideration.

- **Network of Patient Safety Databases (NPSD)**
  The NPSD is an interactive evidence-based data management resource for national learning about patient safety authorized by the Patient Safety Act. It launched in June 2019. The NPSD receives nonidentifiable patient safety data from the PSOPPC and makes it available to the public on the NPSD website.

The HHS Office for Civil Rights (OCR)

The Secretary delegated responsibility for interpreting and enforcing the confidentiality provisions of the Patient Safety Act to the HHS Office for Civil Rights (OCR). The AHRQ PSO Division can arrange for technical assistance with OCR for PSOs that have questions about the Patient Safety Act confidentiality requirements. Patient Safety Act confidentiality complaints can be filed with OCR. OCR also interprets and enforces the HIPAA Privacy, Security, and Breach Notification Rules.

Section 2. Resources Related to the Patient Safety and Quality Improvement Act of 2005

Introduction

This section includes information about the Patient Safety and Quality Improvement Act of 2005; its implementing regulation; formal guidance documents issued by the U.S. Department of Health and Human Services (HHS); informal guides (other than this PSO Listing Guide); and other educational materials developed by AHRQ to assist patient safety organizations (PSOs) with understanding various concepts in the Act and the regulation.

A. The Act and the Regulation

Patient Safety and Quality Improvement Act of 2005

On July 29, 2005, the President signed the Patient Safety and Quality Improvement Act of 2005 (Patient Safety Act, codified at 42 U.S.C. sections 299b-21 to 299b-26) into law. The Patient Safety Act amended Title IX of the Public Health Service Act to provide for the improvement of patient safety and to reduce the incidence of events that adversely affect patient safety by authorizing the creation of PSOs. PSOs work with providers to improve quality and safety through the collection, aggregation, and analysis of confidential patient safety data.

- Access a copy of the Patient Safety Act (Public Law 109–41—JULY 29, 2005)
- Access the Patient Safety Act in an online version of the United States Code (42 U.S.C. sections 299b-21 to 299b-26).

Patient Safety and Quality Improvement Rule (Patient Safety Rule)

To implement the Patient Safety Act, the HHS issued the Patient Safety Rule.

The rulemaking process for the Patient Safety Rule included a Notice of Proposed Rulemaking (NPRM) published in the Federal Register (FR) at 73 FR 8112 (February 12, 2008). Discussions in the first part of the NPRM, called the preamble, may be helpful to understanding provisions in the NPRM that were later incorporated unchanged into the final Patient Safety Rule.

The Patient Safety Final Rule was published on November 21, 2008 (73 FR 70732). The preamble to the Final Rule (73 FR 70732–70796) addresses each provision of the rule, providing a summary and brief discussion of public comments received and how HHS responded to those comments in the Final Rule. The second part (73 FR 70796–70814) is the final regulatory text that serves as the legal basis on which the Department will interpret and enforce the provisions of the Patient Safety Act. This is the regulatory text that is published in the official version of the Code of Federal Regulations (CFR) as 42 CFR Part 3 and in the Electronic Code of Federal Regulations (eCFR), the web version of the Code of Federal Regulations (CFR) that is updated regularly.

eCFR link to 42 CFR Part 3

- Subpart A defines essential terms, such as patient safety work product (PSWP), patient safety evaluation system, and PSO. The definitions apply to all of the other Subparts.
- Subpart B provides the requirements to become and remain listed as a PSO and related agency procedures.
- Subpart C describes the privilege and confidentiality protections that attach to PSWP and lists the only circumstances in which PSWP can be permissibly disclosed.
- Subpart D establishes a framework to enable HHS to monitor and ensure compliance with the confidentiality provisions, a process for imposing a civil money penalty for breach of the confidentiality provisions, and hearing procedures.

B. HHS Guidance

Patient Safety and Quality Improvement Act of 2005 - HHS Guidance Regarding Patient Safety Work Product and Providers' External Obligations (May 2016)

This notice sets forth guidance for PSOs and providers regarding questions that have arisen about the Patient Safety Act and Patient Safety Rule. In particular, this guidance is intended to provide clarity in response to recurring questions about what information that a provider creates or assembles can become patient safety work product (PSWP). It also clarifies how providers can satisfy external obligations related to information collection activities consistent with the Patient Safety Act and Patient Safety Rule.

Access the May 2016 Guidance (Federal Register) (PDF, 0.2 MB)

Additional Resource: AHRQ presentation on the May 2016 HHS Guidance

This presentation is intended to provide general information regarding the AHRQ PSO program and should not be construed as official HHS or AHRQ policy or guidance, nor should it be relied upon as a substitute for familiarity with the Federal laws and regulations applicable to PSOs, including the Patient Safety Act and the Patient Safety Rule. The information presented is not legal advice, is not to be acted on as such, may not be current, and is subject to change without notice.

Access the AHRQ presentation on the May 2016 HHS Guidance (PDF, 0.2 MB)

Patient Safety and Quality Improvement Act of 2005—HHS Guidance Regarding Patient Safety Organizations' Reporting Obligations to the Food and Drug Administration (FDA) (December 2010)

The purpose of this guidance is to address questions that have arisen regarding the obligations of PSOs where they or the organization of which they are a part are legally obligated under the Federal Food, Drug, and Cosmetic Act (FDCA), 21 U.S.C. §301 et seq., and its implementing regulations to report certain information to the Food and Drug Administration (FDA) and to provide FDA with access to its records, which may contain patient safety work product.

This guidance applies to all entities that seek to be or are PSOs that:

- have mandatory FDA-reporting obligations under the Food, Drug and Cosmetic Act (FDCA) or
- are organizationally related to such FDA-regulated reporting entities (e.g., parent organizations, subsidiaries, sibling organizations).

  Access the HHS Guidance Regarding Patient Safety Organizations' Reporting Obligations to the FDA (PDF, 0.4 MB)

C. AHRQ Guides

Guide for PSOs and Providers for Determining Parent Organization and Affiliated Providers

This Guide addresses how the Patient Safety Rule determines a parent organization of a PSO or a provider, and how the Patient Safety Rule determines an "affiliated provider." The terms "parent" and "component", which are used in the Rule, differ from traditional legal interpretation. The Guide explains how to apply these concepts to more complex organizational and corporate structures.

- Access Guide for PSOs and Providers for Determining Parent Organizations and Affiliated Providers (PDF, 0.2 MB)

PSO Policies and Procedures – Topics to Address

This Guide provides entities with topics to consider when developing their Policies and Procedures.

- Access PSO Policies and Procedures - Topics to Address (PDF, 0.5 MB)

What is the Role of the PSO Authorized Official

This Guide addresses the role of the PSO Authorized Official.

- Access What is the Role of the PSO Authorized Official (PDF, 0.2 MB)

Working with a PSO: One Approach (Video and Flow Chart)

"Working with a PSO: One Approach," was developed in response to numerous inquiries from PSOs and providers alike on how a provider should set up a Patient Safety Evaluation System (PSES) when working with a PSO. The video addresses how the concept of a PSES is flexible to meet varying needs of providers. The model this video reviews is intended to raise many - but certainly not all - of the issues that a provider should consider.

- Access the Video: Working with a PSO: One Approach (34 minutes)
- Access the Diagram: Working with PSO: One Approach Diagram (PDF, 0.2 MB)

AHRQ PSO Frequently Asked Questions (FAQ)

This is a list of frequently asked questions and corresponding answers related to the following topics:

- Common Formats
- Component PSOs and Shared Staffing Agreements
- HHS Agency Roles
- Listing Process and Requirements
- Privacy and Confidentiality Requirements
- PSO General Information
- PSO Workforce
- Purpose of a PSO

Access the Frequently Asked Questions

D. Brochure, Webinars And Other Educational Materials

Choosing a PSO Brochure

This brochure includes questions and information that providers should consider when choosing a PSO.

- Access the Choosing a PSO Brochure (PDF, 0.8 MB)

Webinars

November 5, 2020: Working With Patient Safety Organizations (PSOs): The Value for Hospitals During COVID-19 and Beyond

This webinar, recorded November 5, 2020, informs hospital leaders and others who are not familiar with PSOs about the unique advantages of working with PSOs to improve patient safety and healthcare quality. It provides an introduction to the PSO program, insights on perceived value of PSOs from participating hospitals, examples of how PSOs have helped hospitals during COVID-19, and a demonstration of how PSO participation can improve patient safety.

- Access the November 5, 2020 Webinar (1 hour, 2 minutes): https://www.youtube.com/watch?v=gU-2545W6Dg

- Access the slides from the November 5, 2020 Webinar (PDF, 2.6 MB) https://pso.ahrq.gov/sites/default/files/wysiwyg/working-with-pso-webinar-value-hospitals.pdf

June 10, 2015: Benefits of AHRQ Patient Safety Organizations (PSOs): Success Stories from Hospital PSO Members

This June 10, 2015 Webinar highlights the AHRQ PSO program and presents success stories from hospitals that are members of one or more PSOs. Hospitals shared how their organizations worked with their PSOs for meaningful improvements in patient safety and quality.

- Access the June 10, 2015 Webcast (1 hour): https://www.youtube.com/watch?v=sJ-OpMTa3Pw&t=4s

- Access the slides from the June 10, 2015 Webinar: https://pso.ahrq.gov/sites/default/files/wysiwyg/OnDemand%20Webinar%20Slides%20-%20June%2010%202015.pdf (PDF, 1.5 MB)

PSO Program: Common Terms and Acronyms

This is a quick reference of PSO Program common terms and acronyms. These terms are used in the Patient Safety Act, Rule and Notice of Proposed Rulemaking as well as the HHS Guidance and guides. The reader should always rely on the actual definitions in these documents when making any determination.

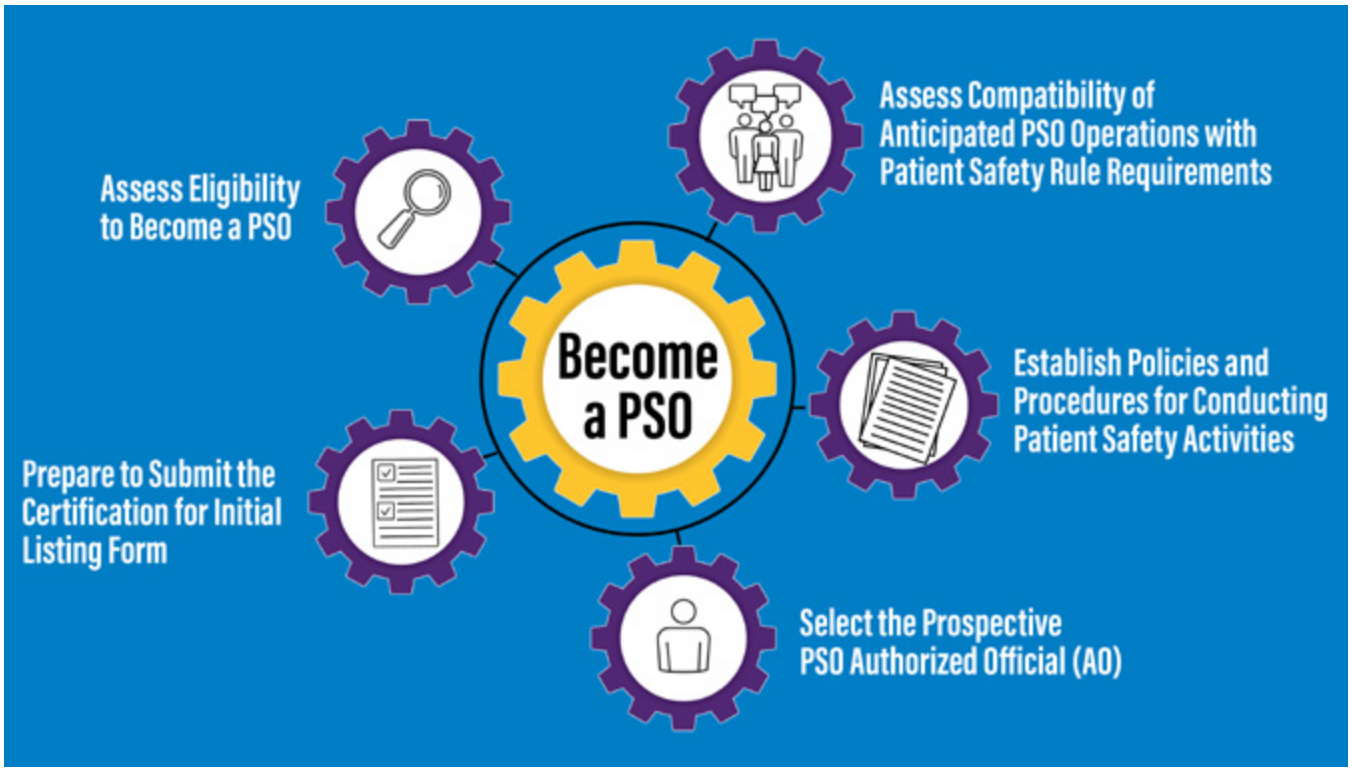
- Access the PSO Program: Common Terms and Acronyms (PDF, 0.3 MB)

Quiz

These quiz questions are provided to promote understanding about PSOs and the requirements of the Patient Safety Act and Rule. The questions have been gathered from AHRQ's experience in providing technical assistance to PSOs, providers, and the public. New questions may be added periodically.

- Access the Quiz Questions (PDF, 0.3 MB)
- Access the Quiz Answers (PDF, 0.3 MB)

Section 3. Become a Patient Safety Organization



This section provides an overview of some points to consider when preparing to pursue PSO listing.

- Assess Eligibility to Become a PSO (page 13)
- Assess Compatibility of Anticipated PSO Operations with Patient Safety Rule Requirements (page 15)
- Establish Policies and Procedures for Conducting Patient Safety Activities (page 17)
- Select the Prospective PSO Authorized Official ("AO") (page 18)
- Prepare to Submit the Certification for Initial Listing Form (page 19)

The AHRQ PSO Program can offer informal, individualized technical assistance for entities interested in pursuing a PSO listing free of charge. There are no fees to apply for listing. Contact us at pso@ahrq.hhs.gov.

Assess Eligibility to Become a PSO

Words that are *italicized* in this section are all defined in Section 3.20 of the Patient Safety Rule.

If an *entity's* mission and primary activity is to conduct activities that are to improve patient safety and the quality of healthcare delivery, it may be eligible to become a PSO.

Some entities are explicitly prohibited from becoming a PSO.

- A *health insurance issuer* cannot be a PSO; nor can a unit or division of a health insurance issuer; nor an entity that is owned, managed, or controlled by a health insurance issuer.
- The following types of "excluded entities" cannot themselves become a PSO, but they may be able to form a PSO as a *component organization*:
  - An entity that accredits or licenses healthcare providers
  - An entity that oversees or enforces statutory or regulatory requirements governing the delivery of healthcare services
  - An agent of an entity that oversees or enforces statutory or regulatory requirements governing the delivery of healthcare services
  - An entity that operates a Federal, State, local, or Tribal patient safety reporting system to which healthcare providers (other than members of the entity's workforce or healthcare providers holding privileges with the entity) are required to report information by law or regulation.

Component organizations of excluded entities that are eligible to apply for PSO listing (section 3.102(a)(2)(ii)) are subject to certain operational restrictions. They must also make additional attestations and provide related information when applying for listing (sections 3.102(c)(1)(ii) and (c)(4)). The following sections provide more information about the requirements for listing as a component PSO and some related considerations.

Listing as a "Full Entity PSO" vs. "Component PSO" and Determining "Parent Organization(s)"

For purposes of the Patient Safety Rule, a parent organization is one that, in relation to a component organization,

- owns a controlling interest or a majority interest in a component organization;
- has the authority to control or manage agenda setting, project management, or day-to-day operations; or

- has the authority to review and override decisions of a component organization.

The Patient Safety Rule uses the terms component and parent organizations broadly. For example, if the entity that will apply for PSO listing is owned, managed, or controlled by one or more legally separate parent organizations, it is considered a component organization for purposes of the Patient Safety Rule and would need to apply for listing as such. For more information, see the section on "Determining a PSO's Parent Organization(s)" in "Guide for PSOs and Providers for Determining Parent Organization and Affiliated Providers (July 2021)."

A component organization does not have to be a legal entity to apply for listing as a PSO if it has a parent organization that is a legal entity. For example, the component organization may be a unit or division of its parent organization.

One consideration in deciding whether to form a component organization to apply for PSO listing is that the mission and primary activity of the PSO must be to conduct activities that are to improve patient safety and the quality of healthcare delivery. Although many organizations have quality and safety in their mission statement, few will meet the primary activity criterion and be able to seek listing as a "full entity PSO." For example, a healthcare facility's primary activity is the delivery of care, not the conduct of activities to improve care.

Requirements Specific to Component PSOs

In addition to the 15 general PSO certification requirements (section 3.102(b)), component organizations have further criteria to meet (section 3.102(c)). Essentially, there must be a firewall between the component PSO and the parent organization so that:

- Patient safety work product (PSWP) is maintained separately from and cannot be accessed by the parent organization.
- The workforce of the component PSO does not make unauthorized disclosures of PSWP to the parent organization or anyone who works there.
- The pursuit of the mission of the PSO cannot create a conflict of interest for the parent organization.
- If any individuals or units of the parent organization will assist the component PSO with patient safety activities requiring access to PSWP, written agreements with specific content are required (see FAQ category "Component PSOs and Shared Staffing Agreements.")

There are additional requirements and restrictions on such arrangements if the PSO is a component of an excluded entity:

- With each certification for listing, the entity must include a statement describing its parent organization's role and scope of authority with respect to any excluded activities described in section 3.102(c)(4). A summary must be prominently posted on the PSO's website and published in any promotional materials for dissemination to providers.

- Each certification for listing must include an attestation that: 1) the parent organization has no policies or procedures that would require or induce providers to report PSWP to their component organization once listed as a PSO; and 2) the component PSO will notify AHRQ within 5 calendar days of the day on which the component organization has knowledge of the adoption by the parent organization of such policies or procedures. The certifications must also acknowledge that the adoption of such policies or procedures by the parent organization during the component PSO's period of listing will result in the initiation of an expedited revocation process in accordance with §3.108(e).

- The component organization may not share staff with its parent organization(s). It may, however, enter into written agreements with individuals or units of the parent organization, for assistance with patient safety activities if their responsibilities do not involve any of the excluded activities.

Assess Compatibility of Anticipated PSO Operations with Patient Safety Rule Requirements

The individual who signs the Certification for Initial Listing Form must be able to accurately attest that the entity will comply with all requirements in the Patient Safety Act and Rule if listed. To prepare, it is important to assess plans for the prospective PSO's operations and services in relation to each requirement in the Certification for Initial Listing Form.

Below are examples of just a few of the Patient Safety Rule requirements that need to be considered when developing plans for a prospective PSO.

Examples of Requirements Related to Security, Confidentiality, and Limitations on the Disclosure of PSWP

Words that are *italicized* in this section are all defined in Section 3.20 of the Patient Safety Rule.

Start by reviewing the definitions of *PSWP* and *disclosure*; the exceptions to confidentiality (section 3.206(b) and related requirements in section 3.212); and the security requirements (section 3.106). Identify and carefully consider all anticipated PSO operations that may involve any access to, transfer or release of PSWP. PSWP must remain confidential unless there is an applicable exception to confidentiality (also referred to as a "disclosure permission") in the Patient Safety Rule. PSWP may only be permissibly disclosed if the contemplated disclosure fits all of the requirements of an applicable exception to confidentiality in section 3.206(b).

Read carefully, as each exception/disclosure permission is very specific about who can make the disclosure, who can receive the PSWP and under what circumstances, and whether the PSWP must meet specific anonymization or non-identification requirements before it can be disclosed.

When planning for the security of PSWP, remember that the requirements in section 3.106 must be met at all times and at any location (physical and virtual) at which the PSO, its workforce members, or its contractors receive, access, or handle PSWP. Handling PSWP includes its processing, development, use, maintenance, storage, removal, disclosure, transmission, and destruction. The PSO must also address the requirement to physically separate PSWP from non-PSWP or, if co-located with non-patient safety work product, to make it distinguishable so that the appropriate form and level of security can be applied and maintained.

It is also helpful to be aware of the requirements for disposition of PSWP when a PSO is delisted (section 3.108(b)(3)) to be sure they would not preclude any aspects of anticipated PSO operations.

Examples of Requirements That Must Be Met by a PSO Within Certain Timeframes

Words that are *italicized* in this section are all defined in Section 3.20 of the Patient Safety Rule.

When developing plans for a prospective PSO, consider how long it is likely to take before the plans can be fully implemented. Once listed, the PSO must meet certain requirements within the specified timeframes in order to remain listed. For example:

- Within the first 2 years after listing, the PSO must have *bona fide contracts* with two different providers for the purpose of receiving and reviewing PSWP.
- Before the end of the first 3-year continued listing period, the PSO must have performed all eight *patient safety activities* and be able to attest that it will continue to do so.
- If the PSO has a relationship with a provider fitting the description in section 3.102(d)(2) and enters into a Patient Safety Act contract with the same provider, the PSO must complete and submit the required disclosure statement by the deadlines specified in the Patient Safety Rule.

FDA Reporting Requirements

Another issue to consider is whether the entity seeking listing is subject to any Federal Food, Drug, and Cosmetic Act (FDA) reporting requirements. The Patient Safety Act works in concert with FDA laws promoting patient safety. FDA reporting responsibilities do not change when an entity becomes listed as a PSO or becomes the parent organization of a component PSO. Being an FDA-regulated reporting entity or organizationally related to an FDA-regulated reporting entity may have implications for the confidentiality of PSWP collected and developed as a listed PSO. (see "Department of Health and Human Services Guidance Regarding Patient Safety Organizations' Reporting Obligations and the Patient Safety and Quality Improvement Act of 2005").

Requirements Related to the HIPAA Privacy and Security Rules

If anticipated PSO operations will involve receipt from providers of PSWP that includes patient information, consider obligations that may arise under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules. For example, the PSO may need to enter into a business associate agreement with its reporting providers. A PSO is considered a business associate of a healthcare provider if the relationship meets two conditions: (1) the provider meets the HIPAA definition of a covered entity; and (2) the PSO performs a function (such as patient safety activities) on behalf of a covered healthcare provider that requires the PSO to receive and use PSWP that contains protected health information (PHI) as defined in the HIPAA Privacy Rule.

To learn more about the obligations of a PSO that is also a HIPAA business associate and the definitions of related HIPAA terms, consult the website maintained by the Office for Civil Rights. Additional business associate security provisions under the HIPAA Security Rule apply to electronic patient health information held by business associates. Review information about the HIPAA Security Rule requirements on the OCR website.

Establish Policies and Procedures for Conducting Patient Safety Activities

Before completing and submitting the Certification for Initial Listing Form, the entity seeking listing must have in place written policies and procedures needed to perform the eight required patient safety activities specified in the Patient Safety Rule. The policies and procedures should outline the "what" (i.e., the Policy) and "how" (i.e., the Procedure) specific to the anticipated PSO's own operations. The entity should provide a systematic, step-by-step outline of the activities that will take place in the PSO including the workforce positions responsible for each activity. Merely re-stating general text from the rule does not fulfill this requirement. For more information, see Policies and Procedures—Topics to Address (PDF, 375 KB).

Please note that AHRQ does not create, approve, or endorse any model PSO policies and procedures or any other template documents for use by PSOs in their operations.

The eight required patient safety activities are:

1. Efforts to improve patient safety and the quality of healthcare delivery;

2. The collection and analysis of patient safety work product;

3. The development and dissemination of information with respect to improving patient safety, such as recommendations, protocols, or information regarding best practices;

4. The utilization of patient safety work product for the purposes of encouraging a culture of safety and of providing feedback and assistance to effectively minimize patient risk;

5. The maintenance of procedures to preserve confidentiality with respect to patient safety work product;

6. The provision of appropriate security measures with respect to patient safety work product;

7. The utilization of qualified staff; and

8. Activities related to the operation of a patient safety evaluation system and to the provision of feedback to participants in a patient safety evaluation system.

With respect to Patient Safety Activities (5) and (6) regarding confidentiality and security, the policies and procedures must include and provide for compliance with the confidentiality and security requirements in the Patient Safety Rule as well as notification to each provider if patient safety work product or data they submitted was subject to an unauthorized disclosure or security breach.

The Certification for Initial Listing also requires the applicant to certify that, if listed as a PSO, it will also comply with the seven requirements listed below. The entity may choose to address aspects of these in its policies and procedures but is not required to do so:

1. The mission and primary activity of the PSO must be to conduct activities that are to improve patient safety and the quality of healthcare delivery.

2. The PSO must have appropriately qualified workforce members, including licensed or certified medical professionals.

3. The PSO, within the 24-month period that begins on the date of its initial listing as a PSO, and within each sequential 24-month period thereafter, must have 2 bona fide contracts, each of a reasonable period of time, each with a different provider for the purpose of receiving and reviewing patient safety work product.

4. The PSO is not a health insurance issuer and is not a component of a health insurance issuer.

5. The PSO must make disclosures as required under section 3.102(d), in accordance with section 3.112 of this subpart.

6. To the extent practical and appropriate, the PSO must collect patient safety work product from providers in a standardized manner that permits valid comparisons of similar cases among similar providers.

7. The PSO must utilize patient safety work product for the purpose of providing direct feedback and assistance to providers to effectively minimize patient risk.

Select the Prospective PSO Authorized Official (AO)

Decide who will serve as the PSO's AO and, if desired, select another individual to serve as the PSO point of contact. The AO must have full authority to sign the certification for listing forms containing

the attestations. The AO is responsible for the veracity of all of the attestations and all aspects of PSO compliance.

AHRQ will want to communicate directly with the AO in technical assistance calls and in the event of a compliance assessment. For this reason, consider whether the AO will—or will not—be a member of the PSO workforce as that term is defined in the Patient Safety Rule and any implications that may have for the AO in performing their responsibilities for the PSO. For example, if an AO is not a workforce member and needs access to PSWP to perform these responsibilities, the PSO will need to determine how PSWP can be permissibly disclosed to the AO. Similarly, a component PSO that designates a senior executive of its parent organization as AO should determine how the PSO will meet its attestations to maintain PSWP securely from, and prevent unauthorized disclosures to, its parent organization in light of such an arrangement.

For more information, see the Guide entitled "What is the Role of the PSO Authorized Official?" (PDF, 466 KB).

Prepare to Submit the Certification for Initial Listing Form

The Certification for Initial Listing Form requires the name, address, and other administrative information about the entity applying for listing as a PSO and any parent organization(s), if applicable (including their alternate legal names, if any). The applicant must also disclose in the Certification for Initial Listing Form if the entity (under its current name or any other) has previously been denied listing, or if listed, was delisted; and if any of the applicant entity's officials or senior managers held comparable positions of responsibility in such an entity.

The Certification for Initial Listing Form may be submitted whenever the prospective AO is able to accurately make the required attestations and certification. The individual who will serve as the PSO's AO if the PSO is listed must be legally authorized to complete the Certification for Initial Listing Form on behalf of the entity seeking listing as a PSO and must certify that the "statements on this form, and any submitted attachments or supplements to it, are made in good faith and are true, complete, and correct to the best of my knowledge and belief. I understand that a knowing and willful false statement on this form, attachments or supplements to it, can be punished by fine or imprisonment or both (United States Code, Title 18, Section 1001)."

There are no fees to apply for listing. AHRQ will acknowledge the form upon receipt and will contact the applicant shortly thereafter to begin the initial listing process.

Technical Assistance

Technical assistance calls with the AHRQ PSO team provide an informal opportunity to discuss specific questions about the requirements. Calls can be arranged at no charge before and after completing and submitting the Certification for Initial Listing Form and at any time after listing. Contact us at pso@ahrq.hhs.gov.

Section 4. Maintain a PSO Listing

When a PSO is listed by AHRQ, it should be ready to carry out its mission and primary activity: conducting activities with providers to improve patient safety and the quality of healthcare delivery. By the time the PSO is due to submit its first Certification for Continued Listing, it must be able to accurately certify that it is currently performing, and will continue to perform, all eight required patient safety activities.

The forms containing the certifications needed to maintain a PSO listing are available for online submission, which is encouraged. Once a PSO is listed, online forms pre-populate with the PSO's administrative information. PSO Authorized Officials can access online forms for their PSO by logging in to their 'My PSO Account' page. If necessary, forms can be downloaded from AHRQ's PSO website, completed, and submitted by email or regular mail.

The AHRQ PSO Division is readily available to respond to PSO questions and technical assistance needs and will facilitate technical assistance specific to the confidentiality requirements with the HHS Office for Civil Rights (OCR).

Overview of PSO Filing Timeline and Forms

***During* each three-year listing period, PSOs must:**

Submit the Two Bona Fide Contracts Form within each 24-month period.

PSOs must have at least two bona fide contracts with two different providers for the purpose of receiving and reviewing patient safety work product. The PSO is required to notify AHRQ that it meets this requirement by submitting the Two Bona Fide Contracts Requirement Form no later than 45 days before the end of each succeeding 24-month period following its initial period of listing. Only the completed form (not the contracts) is required as long as it is submitted before the deadline. If the PSO fails to submit the form by the deadline, it will receive a notice of a preliminary finding of deficiency and will be required to provide copies of contracts to AHRQ that demonstrate compliance.

Submit the Change of Listing Information Form whenever listing information changes

A PSO must promptly notify AHRQ whenever there are changes in the accuracy of the information submitted for listing and provide the pertinent changes. This includes any changes to any information in the last Certification of Listing Form the PSO submitted to AHRQ, including but not limited to information about the PSO's Authorized Official and Point of Contact (if applicable), changes to addresses, telephone numbers, and websites for the PSO, and any changes related to new or existing parent organization(s) to the PSO, if applicable. The Change of Listing Information Form is an administrative form that can be used by the PSO's Authorized Official to comply with this notification requirement.

Submit a Disclosure Statement whenever a relationship with a provider arises that requires disclosure

The PSO must submit a Disclosure Statement to AHRQ within 45 days whenever it has begun, or begins, with respect to the same provider, both a Patient Safety Act contract and a relationship that meets one or more of the criteria in subsection 3.102(d)(2) of the Patient Safety Rule. If a PSO believes this requirement may apply, the Authorized Official is encouraged to contact AHRQ for technical assistance before beginning work on a Disclosure Statement.

To *prepare* for continued listing for another three years, PSOs must:

Submit the Certification for Continued Listing Form

Each PSO must submit the Certification for Continued Listing Form no later than 75 days before expiration of its current three-year listing period. The Certification for Continued Listing Form includes a series of attestations regarding the current activities of the PSO. The PSO may find it helpful to review its operations in relation to the questions on the Continued Listing Form as it enters the third year of each listing period to ensure that it understands and will be able to accurately attest to all of the required certifications. For example, the PSO must be performing all of the eight required patient safety activities. It must also have policies and procedures specific to its own operations that address the confidentiality and security requirements, including a provision to notify providers if their information was subject to an unauthorized disclosure or security breach.

***Throughout* listing, PSOs are encouraged to:**

Submit and update the PSO Profile Form

The PSO Profile Form is voluntary and unrelated to required certifications for listing, but AHRQ encourages all PSOs listed during any part of the previous calendar year to submit a PSO Profile Form to the PSO Privacy Protection Center (PSOPPC) by February 28 of each year. For example, data reflecting the 2021 reporting period (i.e., 2021 calendar year) should be submitted no later than February 28, 2022. The information from the PSO Profile Form makes it possible, for example, for AHRQ to accurately populate the selection tool on the AHRQ PSO website, provide PSOs with aggregate information at the PSO Annual Meeting, and develop content for the AHRQ National Healthcare Quality and Disparities Report. The PSO Profile Form information should be completed electronically at the PSO Privacy Protection Center website. Please contact support@psoppc.org for information about registering for an account and/or for more information about how to submit the PSO Profile Form.

Periodically review this PSO Listing Guide

PSOs may find helpful to review the self-assessment questions in this PSO Listing Guide periodically, when preparing for continued listing, or prior to a compliance review by AHRQ (which may be announced or unannounced). Check the Guides page on the AHRQ PSO website for the latest version.

Take advantage of AHRQ's patient safety and quality improvement resources

AHRQ's main website and its Patient Safety and Quality Improvement page contain a wealth of resources that may be of interest to PSOs and the providers they work with. These include educational resources and learning opportunities about safety science and strategies for improving patient safety; tools that focus on safety culture, teamwork, and patient engagement as well as specific clinical topics in patient safety; the Making Healthcare Safer series, which includes reviews and/or updates of the evidence base for many patient safety practices and strategies; and announcements of funding opportunities.

Online subscriptions to the following AHRQ electronic newsletters can help PSOs and providers keep up with the latest patient safety literature and AHRQ resources. Sign up for these and others here.

- AHRQ News Now is a weekly newsletter that highlights AHRQ's research and program activities.
- PSNet and WebM&M (Combined resource - sign up for email updates here)
  - PSNet features the latest news and essential resources on patient safety, including weekly literature updates, news, tools, and meetings; patient safety primers; and annotated links to important research and other information on patient safety.
  - WebM&M (Morbidity & Mortality Rounds on the Web) features expert analysis of patient safety events, Spotlight Cases that include interactive learning modules available for CME, and Commentaries written by patient safety experts.

Know where to find information about the HIPAA Privacy & Security Rules

The HHS Office for Civil Rights (OCR) interprets and enforces the confidentiality provisions of the Patient Safety Act and Rule as well as the HIPAA Privacy and Security Rules. OCR's website, "HIPAA for Professionals" and its Privacy and Security Listservs may be of interest to PSOs. Since PSOs may receive and use patient safety work product that contains protected health information (PHI), every PSO should determine at the outset when establishing a working relationship with a provider its obligations with respect to HIPAA, if any, and whether it is required by the HIPAA Privacy Rule to enter into a business associate agreement with the provider.

LISTED PSO LOGO

The "Listed PSO" logo is available for use by PSOs that are currently listed by the HHS Secretary. PSOs that choose to use the AHRQ PSO logo should only use it in relation to information pertaining specifically to the PSO (e.g., on the listed PSO's website or web pages, but not on websites or web pages related to any other organization, including the PSO's parent organization and/or affiliated organizations). If the PSO ceases to be listed by AHRQ, it will be expected to promptly remove all uses of the logo.

Section 5: Listing Self-Assessment Questions and Compliance Resources

Introduction

There are two parts to this section:

A. Sample self-assessment questions and links to resources related to the eligibility, listing, and operational requirements in section 3.102 of the Patient Safety Rule.

B. Sample self-assessment questions related to the requirements for the security of patient safety work product in section 3.106 of the Patient Safety Rule.

Some of the sample self-assessment questions may apply to all PSOs, while others may be relevant only to specific types of PSOs. The questions do not establish new standards and are not intended to indicate the only way to meet the regulatory standards. An individual PSO—given its mission, the services and expertise it offers providers, and its operational model for carrying out patient safety activities—should use these sample questions as a starting point for assessing whether its approach to compliance has taken into account issues relevant to its operation.

The other sections in this PSO Listing Guide contain helpful information about the listing requirements. The preambles to both the proposed (73 FR 8111, February 12, 2008) and final (73 FR 70731, November 21, 2008) versions of the Patient Safety Rule may also be helpful to understanding many of these requirements. These preambles are not included among the resources in the tables below. For more information about the preambles, see the section entitled "Patient Safety and Quality Improvement Rule (Patient Safety Rule)" in Section 2 of this Listing Guide (Patient Safety Act Resources).

A. Section 3.102 of the Patient Safety Rule: Requirements for Initial and Continued Listing

INTRODUCTION

This Table addresses the requirements in section 3.102 of the Patient Safety Rule for PSO eligibility, listing, and operations.

Rows #1–#8: Listing Requirements Regarding the Patient Safety Activities (Section 3.102(b)(1) of the Patient Safety Rule):

An entity seeking listing as a PSO must attest that, at the time it seeks listing, it has **policies and procedures in place** to perform the eight patient safety activities defined in section 3.20. The sample Self-Assessment questions below framed in terms of **implementation of the policies and procedures** are not applicable at the time of initial listing.

Once listed and throughout its period of listing, a PSO must be able to demonstrate at all times that it performs all of the patient safety activities that are not dependent upon a relationship with a provider or receipt of patient safety work product. These include utilizing qualified staff, having effective policies and systems to protect the security and confidentiality of patient safety work product, undertaking efforts to improve the quality of health care delivery and patient safety, and developing and disseminating information to improve patient safety. A new PSO may not be ready to conduct all of the other required patient safety activities immediately upon listing, as some of them can only be performed when the PSO is working with a provider and receiving patient safety work product (i.e., the collection and analysis of patient safety work product; the utilization of patient safety work product for the purposes of encouraging a culture of safety and of providing feedback and assistance to effectively minimize patient risk; and activities related to the operation of a patient safety evaluation system and to the provision of feedback to participants in a patient safety evaluation system). However, the PSO must have conducted all eight patient safety activities at some point before its three-year period of listing has concluded. A PSO seeking continued listing must attest that it has performed, and will continue to perform, all eight patient safety activities.

Rows # 9–#15: Requirements Pertaining to the PSO Criteria (Section 3.102(b)(2) of the Patient Safety Rule):

Initial listing requires certification that, if listed, the PSO, will comply with the seven criteria that all PSOs must meet that are specified in section 3.102(b)(2)(i)(A) through (G). To continue listing, the PSO must certify that it is complying and will continue to comply with them.

Rows #16–#19: Additional Requirements for Component Organizations (Section 3.102(c)(1)-(3) of the Patient Safety Rule):

Additional requirements must be met by entities that become listed as component PSOs.

Rows #20–#24: Operational Limitations Required of Component Organizations of Excluded Entities (Section 3.102(c)(4) of the Patient Safety Rule):

Additional requirements must be met by component PSOs with parent organizations that are excluded from listing (i.e., accreditation or licensure entities, regulatory entities or agents of regulatory entities, or entities that administer mandatory reporting systems).

A. Listing Requirements Regarding the Patient Safety Activities

(Section 3.102(b)(1) of the Patent Safety Rule)

Row	Patient Safety Activities	Sample Self-Assessment Questions	Resources
1	Section 3.20, definition of Patient Safety Activities: (1) Efforts to improve patient safety and the quality of health care delivery	How can the PSO document the activities it will offer or has conducted with providers are for the improvement of patient safety and health care quality? For example, does the PSO have descriptive materials or records of patient safety and quality improvement activities it conducted?	FAQ on AHRQ PSO Website: • What is a PSO? • What are "patient safety activities"? • What are the benefits to health care providers who work with a PSO?

Row	Patient Safety Activities	Sample Self-Assessment Questions	Resources
2	Section 3.20, definition of Patient Safety Activities: (2) The collection and analysis of patient safety work product	Has the PSO documented how it will (does) collect patient safety work product from providers? For example, will (does) the PSO accept patient safety work product from providers through paper submissions, secure electronic transmission, use of a secure portal system, or a combination of approaches? Has the PSO documented the range of analytic services that it offers health care providers? Does the documentation address the methods, tools, and analytic approaches the PSO will employ to address specific types of problems or tasks? If the PSO has already undertaken such analyses, can the PSO provide specific examples of the analytic techniques used for specific data? If a PSO enters into a contract with another organization to assist it with the collection or analysis of patient safety work product, are the activities, methods, or approaches used by the contractor(s) consistent with the attestations of the contracting PSO? If the PSO is currently receiving and analyzing patient safety work product, can the PSO provide specific examples that demonstrate or document how the PSO is complying with this requirement?	FAQ on AHRQ PSO Website: What Is Patient Safety Work Product? ▪ What Is Patient Safety Work Product?

Row	Patient Safety Activities	Sample Self-Assessment Questions	Resources
3	Section 3.20, definition of Patient Safety Activities: (3) The development and dissemination of information with respect to improving patient safety, such as recommendations, protocols, or information regarding best practices.	Has the PSO documented how it meets this requirement? For example: ▪ What is the scope of the PSO's existing and planned dissemination activities (i.e., is it restricted to issues for which it receives patient safety work product or will dissemination address a broader range of patient safety and quality improvement issues)? ▪ How does the PSO evaluate whether the information it plans to disseminate takes into account relevant, current clinical standards and developments in patient safety and safety science? ▪ How does the PSO determine when an intervention or approach constitutes a "best practice" before disseminating the information to providers? If the PSO has already developed and disseminated such information, can the PSO provide specific examples that demonstrate or document how the PSO is complying with this requirement?	FAQ on AHRQ PSO Website: ▪ What are the benefits to healthcare providers who work with a PSO?

Row	Patient Safety Activities	Sample Self-Assessment Questions	Resources
4	Section 3.20, definition of Patient Safety Activities: (4) The utilization of patient safety work product for the purposes of encouraging a culture of safety and of providing feedback and assistance to effectively minimize patient risk.	Has the PSO documented how it will (does) meet this requirement? For example: ▪ How will (does) the PSO seek to foster a culture of safety with the providers with which the PSO works? ▪ How does the PSO provide feedback and assistance that may be used by providers to minimize risk to patients? Note the similar requirement in section 3.102(b)(2)(i)(G): "The PSO must utilize patient safety work product for the purpose of providing direct feedback and assistance to providers to effectively minimize patient risk." If the PSO has undertaken specific activities to comply with this requirement, can the PSO provide specific examples that demonstrate or document how the PSO is complying with this requirement?	

Row	Patient Safety Activities	Sample Self-Assessment Questions	Resources
5	Section 3.20, definition of Patient Safety Activities: (5) The maintenance of procedures to preserve confidentiality with respect to patient safety work product.	What policies and procedures does the PSO (plan to) implement to preserve the confidentiality of patient safety work product? Do the PSO's confidentiality policies meet the requirement in section 3.102(b)(1)(i)(A) to be consistent with Subpart C of the Patient Safety Rule (sections 3.204 through 3.212) regarding confidentiality and privilege of patient safety work product? How does the PSO ensure its (existing and new) workforce and contractors are aware of the policies and procedures? For example, does the PSO require written acknowledgement of the confidentiality protections by members of its staff and contractors with access to patient safety work product? How does the PSO ensure compliance with the policies and procedures by all workforce members and contractors with access to patient safety work product in all locations, including virtual work locations? How does the PSO ensure its contractors are aware of and comply with the limitations on contractor disclosure of patient safety work product in section 3.206(b)(4)(ii)? Do the PSO's policies and procedures specify how the PSO will implement the requirement (section 3.102(b)(1)(i)(B)) to notify affected providers of any unauthorized disclosures or security breaches of submitted patient safety work product? If the PSO has received patient safety work product and has had to implement this procedure, does the PSO have documentation that can demonstrate compliance?	FAQ on AHRQ PSO Website: ▪ What are the privacy and confidentiality protections for PSWP? ▪ What is the importance of the privacy and confidentiality protections for PSWP? ▪ What is the relationship between the Patient Safety Rule and the HIPAA Privacy Rule? HHS Office for Civil Rights (OCR) Website: (https://www.hhs.gov/hipaa/for-professionals/index.html) ▪ Understanding Patient Safety Confidentiality ▪ HIPAA Breach Notification Rule

Row	Patient Safety Activities	Sample Self-Assessment Questions	Resources
6	Section 3.20, definition of Patient Safety Activities: (6) The provision of appropriate security measures with respect to patient safety work product	Section 3.102(b)(1)(i)(A) specifies that a PSO's policies for the security of patient safety work product must meet the requirements of section 3.106. The requirements of section 3.106 and sample self-assessment questions are provided in Table 2.	

Row	Patient Safety Activities	Sample Self-Assessment Questions	Resources
7.	Section 3.20, definition of Patient Safety Activities: (7) The utilization of qualified personnel	How did the PSO assess the types and extent of expertise needed to conduct the patient safety activities it offers to providers and ensure its personnel are qualified to fulfill these needs? Has the PSO documented its policies and procedures for utilization of qualified staff (either as members of the PSO's workforce or as contractors)? For example, is there a linkage between the job descriptions for staff positions and the patient safety/safety science, clinical, analytic, and/or quality improvement expertise needed for the PSO to meet its mission and provide the services the PSO is offering providers? [Note: questions regarding the match between the skills and expertise of the PSO's workforce and contractors and the services offered by the PSO are also raised in #10 below.]	FAQ on AHRQ PSO Website: ▪ Generally, what are the staffing and personnel requirements of a PSO? ▪ What expertise is required of a PSO's appropriately qualified workforce? ▪ Is a PSO required to have licensed or certified medical professionals as part of its workforce? ▪ What is the difference between a PSO's overall workforce and appropriately qualified workforce members? ▪ May a PSO meet the requirement that its appropriately qualified workforce include licensed or certified medical professionals with contracted medical professionals? ▪ Is a PSO required to engage with additional experts if the PSO adjusts its activities or areas of focus? ▪ What is an example of how a PSO's collection and analysis of patient safety work product could change requiring additional expertise? ▪ Is every PSO required to engage a medical doctor to meet the appropriately qualified workforce requirement? ▪ Is a PSO required to meet the appropriately qualified workforce requirement when a PSO is not collecting or analyzing patient safety work product?

Row	Patient Safety Activities	Sample Self-Assessment Questions	Resources
8	Section 3.20, definition of Patient Safety Activities: (8) Activities related to the operation of a patient safety evaluation system and to the provision of feedback to participants in a patient safety evaluation system	Has the PSO documented how it will (does) meet this requirement? For example, how are the components of the PSO's patient safety evaluation system (PSES) and the boundaries between the PSO's PSES and those of its providers made clear to the PSO's workforce? Such documentation might include: • Specifying which information 1) received from providers and 2) developed by the PSO is/is not patient safety work product • How information enters the PSES • Processes, activities, information systems, physical space(s) and equipment comprised or used • Which personnel or categories of personnel need access to patient safety work product to carry out their duties involving operation of, or interaction with, the PSES • The category of patient safety work product to which access is needed and any conditions appropriate to such access • Procedures used to ensure the confidentiality and security of the patient safety work product when providing feedback to providers How does the PSO ensure that its workforce is clear regarding the need for boundaries between activities undertaken within the PSES and outside of the PSES? For example, is there documentation regarding the electronic, virtual, and physical spaces allocated for patient safety evaluation system activities and which staff have access to patient safety work product? How is it possible to determine when staff are performing patient safety evaluation system vs. non-patient safety evaluation system activities? Has the PSO documented how it will (does) communicate with, and provide feedback to, participants in each patient safety evaluation system of the providers with which it works?	Resources on AHRQ PSO Website: • Educational Tools That Support Learning (VIDEO and DIAGRAM "Working With A PSO: One Approach")

Requirements Pertaining to the PSO Criteria
(Section 3.102(b)(2) of the Patient Safety Rule)

Row	PSO Criteria	Sample Self-Assessment Questions	Resources
9	Section 3.102(b)(2)(i)(A): The mission and primary activity of the PSO must be to conduct activities that are to improve patient safety and the quality of health care delivery.	Does the PSO have a mission statement? If so, does it align with this requirement? Can the PSO demonstrate, taking into account all of the activities it performs, that the improvement of patient safety and health care delivery constitute its "primary" activity? Note that many organizations could reasonably claim that improvement of the quality of health care and patient safety are fundamental to their missions, but the statute also requires that such improvement activities must be the entity's primary activity. For example, improving patient safety and the quality of health care delivery are typically part of the core mission of a hospital. However, the primary activity of a hospital is patient care. Two possible ways of meeting this requirement would be to demonstrate that these activities: ▪ Account for the "majority" of activity by its workforce; or ▪ Account for the majority of revenue or expenditures of the entity.	FAQ on AHRQ PSO Website: ▪ What is the primary activity requirement for listing as a PSO? ▪ What can an entity do if it does not meet this primary activity requirement?
10	Section 3.102(b)(2)(i)(B): The PSO must have appropriately qualified workforce members, including licensed or certified medical professionals.	Can the PSO document how the expertise and skills of its PSO workforce members are an appropriate match for the clinical, analytic, and patient safety and/or quality improvement activities that the PSO offers providers? Can the PSO document that its workforce includes licensed or certified medical professionals? Can the PSO document that there is a reasonable relationship between the expertise and skills of its medical professional(s) and the clinical patient safety issues the PSO addresses?	FAQ: See list in Row #7 above

Row	PSO Criteria	Sample Self-Assessment Questions	Resources
11	Section 3.102(b)(2)(i)(C): The PSO, within the 24-month period that begins after the date of initial listing as a PSO, and within each sequential 24- month period thereafter, must have two bona fide contracts, each of a reasonable period of time, each with a different provider for the purpose of receiving and reviewing patient safety work product.	If a PSO has submitted certification that it has two contracts with different providers, do the two contracts cited by the PSO meet the regulatory requirements? Specifically: ▪ Do the contracts meet the definition of bona fide (e.g., the contracts are written and entered in good faith)? ▪ Do the contracts require receipt and review of patient safety work product by the PSO? ▪ Were the contracts entered into with different providers? The Patient Safety Rule focuses on the provider entity entering the contract and not the providers covered by the contract. For example, entering two contracts with the same headquarters of a health system (one covering its hospitals and another covering its nursing homes) would not meet the requirement since the contracts are being entered with the same corporate entity. If the PSO has met the two contract requirement, has the PSO submitted the required notification by the deadline (see section 3.102(d)(1)?	

Row	PSO Criteria	Sample Self-Assessment Questions	Resources
12	Section 3.102(b)(2)(i)(D): The PSO is not a health insurance issuer, and is not a component of a health insurance issuer. Health insurance issuer is defined as follows in section 3.20: Health insurance issuer means an insurance company, insurance service, or insurance organization (including a health maintenance organization, as defined in 42 U.S.C. 300gg-91(b)(3)) which is licensed to engage in the business of insurance in a State and which is subject to State law which regulates insurance (within the meaning of 29 U.S.C. 1144(b)(2)). This term does not include a group health plan.	Can the PSO confirm its attestation that it is not a health insurance issuer or a component of a health insurance issuer? Is a health insurance issuer involved in the governance or financing of the PSO in a manner described in the definition of parent organization in section 3.20?	

Row	PSO Criteria	Sample Self-Assessment Questions	Resources
13	Section 3.102(b)(2)(i)(E): The PSO must make a disclosure to the Secretary as required under section 3.102(d), in accordance with 3.112 of this subpart. Note: Section 3.102(d)(2) requires that a PSO shall fully disclose— (i) any financial, reporting, or contractual relationship between the PSO and any provider that has a Patient Safety Act contract with the PSO; and (ii) if applicable, the fact that the PSO is not managed, controlled, and operated independently from any provider that contracts with the PSO.	Has the PSO documented how it has complied with this requirement, including being able to demonstrate the following: ▪ Every time the PSO entered a Patient Safety Act contract with a provider, did the PSO conduct the required assessment to determine whether the PSO had other relationships with that provider that would require the PSO to complete and submit a disclosure statement? ▪ If the PSO chose not to file a disclosure statement regarding a provider with which it entered a Patient Safety Act contract, can the PSO document that it made the determination that a disclosure statement was not required? ▪ If the PSO developed any other relationships with that contracting provider during the contract period, did the PSO conduct the required re-assessment to determine whether the PSO needed to complete and submit a new or revised disclosure statement? ▪ Did each disclosure statement submitted fully comply with the Patient Safety Rule?	

Row	PSO Criteria	Sample Self-Assessment Questions	Resources
14	Section 3.102(b)(2)(i)(F): To the extent practical and appropriate, the PSO must collect patient safety work product from providers in a standardized manner that permits valid comparisons of similar cases among similar providers. See section 3.102(b)(2)(iii), which establishes a different standard for continued listing, which is summarized here: At continued listing, the PSO must attest that it is using, and will continue to use, either (A) the Secretary's published guidance for common definitions and reporting formats (AHRQ Common Formats) or (B) an alternate system of formats and definitions in its collection of patient safety work product that permits valid comparisons among similar providers. If the PSO cannot make either attestation, it must attest that it is not practical or appropriate to comply with the options A or B by submitting a clear explanation of why it is not practical or appropriate for the PSO to comply with those options.	Can the PSO document its determination that it is collecting patient safety work product in a standardized manner that permits valid comparisons of similar cases among similar providers as required by the Patient Safety Rule? If the PSO is not using AHRQ's Common Formats, can the PSO provide documentation of the system it is using? If it is not using any standardized approach, what is the PSO's rationale? Once a PSO is listed, , the requirement for compliance changes and the PSO should consider: ▪ Can the PSO demonstrate that it is using AHRQ's Common Formats? ▪ If the PSO is using another system, is the PSO prepared to demonstrate that the system it is using permits valid comparisons of similar cases among similar providers? ▪ If the PSO is not collecting patient safety work product in a standardized manner, can the PSO provide a clear explanation for why it is not practical or appropriate to use AHRQ's Common Formats or another standardized system at this time?	Common Formats on AHRQ PSO Website: Common Formats PSOPPC Website: Common Formats Background For PSOs
15	Section 3.102(b)(2)(i)(G): The PSO must utilize patient safety work product for the purpose of providing direct feedback and assistance to providers to effectively minimize patient risk.	Will (or does) the PSO use patient safety work product to provide direct feedback and assistance to providers to effectively minimize patient risk? If so, can the PSO demonstrate or document how it complies with this requirement?	RESOURCES on AHRQ PSO Website: Educational Tools That Support Learning (VIDEO and DIAGRAM "Working With A PSO: One Approach")

Additional Requirements That Apply to All Component PSOs

The following requirements (Rows #16–#19) only apply to PSOs that are component organizations. All component PSOs also must meet requirements applicable to all PSOs (Rows #1–#15). In each case, compliance with these additional requirements is the same at initial and continued listing.

Row	Requirement To Be Met By All Component PSOs	Sample Self-Assessment Questions	Resources
16	Section 3.102(c)(2)(i), Separation of Patient Safety Work Product: A component PSO must maintain patient safety work product separately from the rest of the parent organization(s) of which it is a part, and establish appropriate security measures to maintain the confidentiality of patient safety work product.	Can the component PSO demonstrate compliance with this requirement? For example: ▪ Does the component PSO have written policies and procedures and security measures in place to prevent access to its patient safety evaluation system and patient safety work product by staff of the parent organization? ▪ If the component PSO has a shared information system with its parent organization, can the PSO demonstrate how it maintains PSWP separate from and inaccessible to the rest of the parent organization? ▪ How does the component PSO ensure that all individuals with access to PSWP fully understand the importance of: (1) maintaining patient safety work product separately from the parent organization, and (2) avoiding unauthorized disclosures? Do the PSO's confidentiality and security policies and procedures (Rows #5 and #6 above) adequately and appropriately address these issues? ▪ If the component PSO has experienced any close calls or incidents involving inappropriate disclosure of patient safety work product or security breaches of its patient safety evaluation system, what steps did the PSO taken to assess and mitigate the situation? Did the PSO notify affected providers if required by 3.102(b)(1)(i)(B)? What actions have been taken to prevent a similar situation?	Guides on AHRQ PSO Website: Guide for PSOs and Providers For Determining Parent Organizations and Affiliated Providers FAQ on AHRQ PSO Website: ▪ Under what circumstances may a component PSO allow its parent organization to have access to PSWP? ▪ What are the privacy and confidentiality protections for PSWP? ▪ What is the importance of the privacy and confidentiality protections of PSWP? ▪ What is the relationship between the Patient Safety Rule and the HIPAA Privacy Rule? HHS Office for Civil Rights (OCR) (https://www.hhs.gov/hipaa/for-professionals/index.html) ▪ Understanding Patient Safety Confidentiality

Row	Requirement To Be Met By All Component PSOs	Sample Self-Assessment Questions	Resources
17	Section 3.102(c)(2)(ii), Nondisclosure of Patient Safety Work Product: A component PSO must require that members of its workforce and any other contractor staff not make unauthorized disclosures of patient safety work product to the rest of the parent organization(s) of which it is a part.	If the component PSO uses staff of the parent organization to assist it with conducting patient safety activities, how does the PSO ensure that these individuals fully understand the importance of: (1) maintaining patient safety work product separately from the parent organization, and (2) avoiding unauthorized disclosures? Do the PSO's confidentiality and security policies and procedures (Rows #5 and #6 above) adequately and appropriately address these issues? Note that this requirement would also apply if the parent organization provides IT support. Maintaining procedures to preserve the confidentiality and security of patient safety work product are among the required patient safety activities. How does the PSO ensure that IT personnel understand and acknowledge restrictions regarding patient safety work product? If the parent organization staff have access to locations where patient safety work product is held, how does the component PSO handle physical security and access issues?	
18	Section 3.102(c)(2)(iii), No Conflict of Interest. The pursuit of the mission of a component PSO must not create a conflict of interest with the rest of the parent organization(s) of which it is a part.	Can the component PSO demonstrate how it avoids situations that might create a conflict of interest with its parent organization? For example, a component PSO could create a conflict of interest by sharing patient safety work product with a member of the parent organization whose job responsibilities would involve taking adverse personnel actions against providers. If the PSO plans to use individuals or units from the rest of the parent organization(s) to assist it with patient safety activities can the PSO point to the steps it took to review the responsibilities of such individuals before sharing identifiable patient safety work product with him or her? How does the PSO identify whether their work responsibilities for the parent organization pose potential conflicts with the "culture of safety" the PSO is required to encourage?	FAQ on AHRQ PSO Website: ▪ Are there additional requirements for a component organization?

Row	Requirement To Be Met By All Component PSOs	Sample Self-Assessment Questions	Resources
19	Section 3.102(c)(3), Written Agreements for Assisting a Component PSO in the Conduct of Patient Safety Activities (summarized here): A component PSO may provide access to identifiable patient safety work product to one or more individuals in, or to one or more units of, its parent organization(s) if the component PSO enters into a written agreement with such individuals or units which requires that: (i) Access to patient safety work product is only provided to enable such individuals or units to assist the component PSO in its conduct of patient safety activities, and (ii) Such individuals or units may only use or disclose patient safety work product as specified by the component PSO, will take appropriate security measures to prevent unauthorized disclosures and will comply with the other certifications the component PSO has made regarding unauthorized disclosures and conducting the mission of the PSO without creating conflicts of interest.	If the component PSO plans to allow any individuals or units of its parent organization(s) to have access to identifiable patient safety work product, did the PSO enter into the required written agreements with each individual and/or unit? Do the written agreements meet the requirements of this section? For example: ▪ Are the agreements limited to tasks that assist the PSO in carrying out patient safety activities as required by section 3.102(c)(3)(i)? ▪ Do the agreements contain provisions that address the additional elements in section 3.102(c)(3)(ii), which specify that shared staff : » May only use or disclose patient safety work product as specified by the component PSO » Will take appropriate security measures to prevent unauthorized disclosures » Will comply with the other certifications the component PSO has made regarding unauthorized disclosures and conducting the mission of the PSO without creating conflicts of interest. How will the component PSO ensure that the individuals or units of the parent organization have met, are meeting, and will meet the responsibilities in their written agreements? Has the PSO ensured that the agreements are with individuals or units of the parent organization that will not pose a conflict of interest (see previous Row #18)?	FAQ on AHRQ PSO Website: ▪ What are the requirements if a component PSO wishes to use individuals or units of its parent organization as PSO workforce for assistance in performing patient safety activities? ▪ What is a shared staffing agreement? ▪ What must be included in a shared staffing agreement? ▪ What are the circumstances in which a component PSO may not engage an individual or unit of its parent organization in the work of the PSO?

Operational Limitations Required of Component Organizations of Excluded Entities

Section 3.102(c)(4) contains additional requirements that must be met by PSOs with parent organizations that are excluded from listing but which may form a component PSO (Section 3.102(a)(2)(ii) of the Patient Safety Rule), including entities that: Accredit or license health care providers; oversee or enforce statutory or regulatory requirements governing the delivery of health care services; are an agent of an entity that oversees or enforces statutory or regulatory requirements governing the delivery of health care services; or operate a Federal, state, local or Tribal patient safety reporting system to which health care providers (other than members of the entity's workforce or health care providers holding privileges with the entity) are required to report information by law or regulation.

Such PSOs are also responsible for compliance with all of the requirements listed above (Rows #1–#19). In each case (Rows #20-#24), compliance with these additional requirements is the same at initial and continued listing.

Row	Additional Requirements for a PSO that is a component of an Excluded Entity	Sample Self-Assessment Questions	Resources
20	Section 3.102(c)(4)(i): A component organization of an (excluded) entity must: (i) Submit the following information with its certifications for listing: (A) A statement describing its parent organization's role, and the scope of the parent organization's authority, with respect to any of the following that apply: accreditation or licensure of health care providers, oversight or enforcement of statutory or regulatory requirements governing the delivery of health care services, serving as an agent of such a regulatory oversight or enforcement authority, or administering a public mandatory patient safety reporting system	Does the component PSO have a mechanism (1) to review if there are changes to its parent organization's role or authority as described in the statement submitted to AHRQ, and, if so, (2) to revise the written statement, and submit the updated version to AHRQ?	FAQ on AHRQ PSO Website: ▪ Are any entities excluded from being listed as a PSO?

Row	Additional Requirements for a PSO that is a component of an Excluded Entity	Sample Self-Assessment Questions	Resources
21	Section 3.102(c)(4)(i): A component organization of an (excluded) entity must: (i) Submit the following information with its certifications for listing: (B) An attestation that the parent organization has no policies or procedures that would require or induce providers to report patient safety work product to their component organization once listed as a PSO and that the component PSO will notify the Secretary within 5 calendar days of the date on which the component organization has knowledge of the adoption by the parent organization of such policies or procedures, and an acknowledgment that the adoption of such policies or procedures by the parent organization during the component PSO's period of listing will result in the Secretary initiating an expedited revocation process in accordance with §3.108(e).	Can the PSO document how it determines if its parent organization has prohibited policies or incentives?	The Resources in Row #20 also apply here.
22	Section 3.102(c)(4)(i): A component organization of an (excluded) entity must: (i) Submit the following information with its certifications for listing: (C) An attestation that the component organization will prominently post notification on its Web site and publish in any promotional materials for dissemination to providers, a summary of the information that is required by paragraph (c)(4)(i)(A) of this section. (see Row #20).	Does the PSO periodically review its website and promotional materials to ensure that the required summary statement regarding the role and authority of the parent organization is provided, and is current?	

Row	Additional Requirements for a PSO that is a component of an Excluded Entity	Sample Self-Assessment Questions	Resources
23	Section 3.102(c)(4)(ii), Comply with the following requirements during its period of listing: (A) The component organization may not share staff with its parent organization(s).	Can the component PSO document that it does not share staff with its parent organization(s)? Note the distinction between the prohibition on shared staff and the ability to enter a written agreement for assistance in carrying out patient safety activities pursuant to a written agreement required by the rule text in Row #24.	FAQ on AHRQ PSO Website: ▪ Under what circumstances may a component PSO allow its parent organization to have access to PSWP? ▪ What must be included in a shared staffing agreement?
24	Section 3.102(c)(4)(ii), Comply with the following requirements during its period of listing: (B) The component organization may enter into a written agreement pursuant to paragraph (c)(3) but such agreements are limited to units or individuals of the parent organization(s) whose responsibilities do not involve the activities specified in the restrictions in paragraph (a)(2)(ii) of this section.	If the PSO plans to enter a written agreement with its parent organization for assistance in carrying out patient safety activities, how does it determine whether the individuals or units assigned to provide such assistance are involved with any of the restricted activities specified in section 3.102(a)(2)(ii)? See also the questions in row #19 above.	▪ What are the circumstances in which a component PSO may not engage an individual or unit of its parent organization in the work of the PSO?

B. Section 3.106 of the Patient Safety Rule: Security Requirements

The Patient Safety Rule (42 CFR Part 3) requires all PSOs to have written policies and procedures that address the security requirements specified in section 3.106. While this section of the Patient Safety Rule permits each PSO to develop appropriate and scalable security standards, policies, and procedures suitable for the size and complexity of its organization, the PSO's security framework must address every element set forth in section 3.106, including security management, distinguishing patient safety work product, security control and monitoring, and security assessment. PSOs should note that these policies and procedures must address security at all locations at which patient safety work product is received, accessed, or handled, whether at the PSO's physical location or remotely. Handling patient safety work product includes its processing, development, use, maintenance, storage, removal, disclosure, transmission, and destruction.

In addition to the Patient Safety Rule's confidentiality and security requirements, PSOs that receive patient safety work product or other information containing protected health information (PHI) from a provider that is a covered entity are also subject to certain provisions of the HIPAA Privacy, Security and Breach Notification Rules (HIPAA Rules). The Patient Safety Act clarifies (at 42 U.S.C. 299b-22(i)) that a PSO is to be treated as a business associate of such providers and that the patient safety activities the PSO conducts as a business associate are deemed to be healthcare operations of the

provider. In addition to its obligations under the Patient Safety Rule, a PSO that is a business associate is directly liable for compliance with certain provisions of the HIPAA Rules. For example, if the PSO receives electronic PHI as a business associate, it must meet the HIPAA Security Rule standards in addition to meeting other provisions of the HIPAA Rules. The Office for Civil Rights (OCR) of the U.S. Department of Health and Human Services (HHS) implements and enforces the HIPAA Rules and is also responsible for interpretation and enforcement of the confidentiality provisions of the Patient Safety Rule. The OCR website, Direct Liability of Business Associates | HHS.gov, provides more information about requirements in the HIPAA Rules that would apply to PSOs that serve as business associates to providers.

AHRQ does not have technical assistance materials specific to the security requirements in the Patient Safety Rule. OCR and the Office of the National Coordinator for Health Information Technology (ONC) make available helpful resources pertaining to the HIPAA Security Rule. The resources described below pertain to the HIPAA Rules and/or cybersecurity generally. They are not specific to the Patient Safety Rule security requirements but may be informative.

National Institute of Standards and Technology (NIST):

- General industry resources about managing and reducing cybersecurity risk, such as the voluntary Cybersecurity Framework.

OCR:

- HIPAA for Professionals | HHS.gov - resources about various aspects of the HIPAA Privacy and Security Rules
- Cyber Security Guidance Material
- HIPAA Security Rule Guidance Material
- Sign up for the OCR Privacy (and/or) Security Listserv

ONC:

- Top 10 Myths of Security Risk Analysis
- Security Risk Assessment Videos

B. Security Requirements

(Section 3.106 of the Patient Safety Rule)

Application		
Row	**Security Requirements**	**Sample Self-Assessment Questions**
1	Section 3.106(a) A PSO must secure patient safety work product in conformance with the security requirements of paragraph (b) of this section. These requirements must be met at all times and at any location at which the PSO, its workforce members, or its contractors receive, access, or handle patient safety work product. Handling patient safety work product includes its processing, development, use, maintenance, storage, removal, disclosure, transmission, and destruction.	Has the PSO established security standards that meet the requirements of this section, including the standards that address all locations at which PSO workforce and contractors receive, access, or handle PSWP? Does the PSO have, or expect to have, contracts in place with outside contractors (e.g., consultants and vendors) to whom PSWP will be entrusted? If so, has the PSO: ▪ Established specific security standards that its contractors must meet when they have access to PSWP? ▪ Established a secure mechanism to monitor, control, and protect the security of PSWP during transmission, access, and handling by contractors? ▪ Reviewed with contractors the confidentiality and security requirements for PSWP, including the limitations on further disclosure of patient safety work product (section 3.205(b)(4) of the Patient Safety Rule states that a contractor may not further disclose patient safety work product except to the PSO or provider from which it received the PSWP? ▪ Defined clearly the permissible tasks for which the contractor may use patient safety work product and specified the individual(s) or unit(s) of the contractor(s) that may have access to PSWP? ▪ Required its contractors or vendors to establish an effective mechanism to ensure each member of their workforce (both employees and subcontractors) with access to PSWP understand, acknowledge, and agree to adhere to the protections and limitations regarding its use and disclosure?

Security Framework		
Row	**Security Requirements**	**Sample Self-Assessment Questions**
2	Section 3.106(b) A PSO must have written policies and procedures that address each of the considerations specified in this subsection. In addressing the framework that follows, the PSO may develop appropriate and scalable security standards, policies, and procedures that are suitable for the size and complexity of its organization.	Has the PSO considered the full range and scope of its operations and areas of potential exposure in determining the security standards, policies, and procedures suitable for its size and complexity?

Security Management A PSO must address:		
Row	**Security Requirements**	**Sample Self-Assessment Questions**
3	Section 3.106(b)(1)(i) Maintenance and effective implementation of written policies and procedures that conform to the requirements of this section to protect the confidentiality, integrity, and availability of the patient safety work product that is received, accessed, or handled; and to monitor and improve the effectiveness of such policies and procedures.	Do the PSO's written policies and procedures: ▪ Establish standards for each element of the security framework in section 3.106(b)? ▪ Outline the processes by which the PSO: (1) decides to disclose PSWP; (2) verifies that a proposed disclosure is permitted by an exception in section 3.206(b) in the Patient Safety Rule; (3) ensures that the circumstances of any proposed disclosure meet all elements of the applicable exception and tracks to whom PSWP is disclosed and the specific information that was disclosed; (4) if the disclosure is to be made pursuant to section 3.206(b)(4)(iv), prior to making the disclosure, the PSO ensures the removal of all identifiers required to be removed for providers (individual and institutional, including affiliated organizations, corporate parents, subsidiaries, practice partners, employers, members of the workforce, or household members), reporters, and patients (the direct identifiers listed at 45 CFR 164.514(e)(2)) (5) if the disclosure is to be made pursuant to section 3.206(b)(5), prior to making the disclosure: i. selects the provider and reporter nonidentification process to be used from the two options outlined in 3.212(a); ii. if using the process in 3.212(a)(1), has a procedure for determining whether the person who will apply and document the analysis has the requisite knowledge and experience, and a procedure for assessing and maintaining the required documentation; iii. if using the process in 3.212(a)(2), has a procedure for removing and confirming removal of all provider and reporter (individual and institutional, including affiliated organizations, corporate parents, subsidiaries, practice partners, employers, members of the workforce, or household members), identifiers specified in 3.212(a)(2)(i) and for making the determination required in 3.212(a)(2)(ii) iv. has a procedure for removing and confirming removal of all patient identifiers as specified in 3.212(b); and v. if 3.212(a)(3) is applicable, has a procedure for ensuring compliance. ▪ Address the entire spectrum of data activities from receipt, processing, use, storage, return to providers (if requested), and/or destruction? ▪ Specify how the PSO will undertake "recovery" from emergencies, system failures, or security breaches? ▪ Require documenting security breaches and evaluating their causes in an attempt to prevent reoccurrence?

Row	Security Requirements	Sample Self-Assessment Questions
3		If the PSO (or its parent organization) uses an IT vendor, are there contractual provisions that: (1) ensure that disclosure determinations can only be authorized by the PSO; (2) require prompt notification of the PSO if data system emergencies, failures, or security breaches occur; (3) specify how "recovery" will take place, and (4) provide for evaluation of the causes of data system emergencies, failures, or security breaches? If the PSO is a component of another entity with which it shares an IT system, has the component PSO ensured that there can be no unauthorized access by individuals or units of the parent organization(s) (section 3.102(c)(2)(i) of the Patient Safety Rule)?

Row	Security Requirements	Sample Self-Assessment Questions
4	Section 3.106(b)(1)(ii) Training of the PSO workforce and PSO contractors who receive, access, or handle patient safety work product regarding the requirements of the Patient Safety Act, this Part, and the PSO's policies and procedures regarding the confidentiality and security of patient safety work product.	With respect to staff and contractor training: What procedures has the PSO adopted and implemented to fulfill this requirement? For example, what is the timing of the training in relation to contract execution or onboarding and initiating tasks involving access to PSWP? What is the curriculum content regarding the confidentiality and security protections for PSWP? How does the PSO assess the effectiveness of its training? Does the PSO provide refresher training and assessment? If so, how frequently? Is there a process for: (1) reminding departing workforce (including temporary workforce and contractors) of their continuing confidentiality obligations regarding PSWP to which they had access during the time they served as PSO workforce; (2) retrieving any PSWP in their possession; and (3) deactivating their access to PSWP? How does the training address compliance with security policies and procedures regarding electronic security (e.g., strong passwords/other authentication, virus/spyware/phishing awareness, security of electronic communications)? Does the PSO conduct background checks as part of its hiring processes? If the PSO is a component of one or more parent organization(s), how does the PSO ensure that its workforce and contractors understand that PSWP cannot be shared with individuals or units of its parent organization(s) except as authorized by the rule? Specifically: ▪ How does the PSO's training address the risk of impermissible disclosures of patient safety work product to the parent organization, including inadvertent or deliberate access/disclosure by electronic means, hard copy and via discussion? ▪ If any individual or unit of the parent organization has access to PSWP product held by the component PSO, does the PSO have a written agreement meeting the requirements of section 3.102(c)(3) to authorize this access? See Table 1, Row #19. ▪ How has the PSO documented that other members of its workforce (nonshared staff) and its contractor(s) are aware of the prohibition on making unauthorized disclosures of PSWP to individuals or units of the PSO's parent organization(s)?

Distinguishing Patient Safety Work Product A PSO must address:		
Row	**Security Requirements**	**Sample Self-Assessment Questions**
5	Section 3.106(b)(2)(i) Maintenance of the security of patient safety work product, whether in electronic or other media, through either physical separation from non-patient safety work product, or if co-located with non-patient safety work product, by making patient safety work product distinguishable so that the appropriate form and level of security can be applied and maintained.	Can the PSO document how it ensures PSWP – in all forms – is always maintained at the appropriate level of security? Has the PSO defined the physical and virtual (electronic) space that comprises its patient safety evaluation system? Has the PSO determined whether all PSWP is separated from non-patient safety work product? For any PSWP co-located with non-patient safety work product, has the PSO documented how it distinguishes patient safety work product and ensures appropriate security measures are applied? Does the PSO restrict access to PSWP to only those members of its workforce that require access? How does the PSO ensure that PSWP product is maintained within its patient safety evaluation system? How does the PSO ensure that others do not have access to its PSWP? How do the PSO's policies and procedures ensure that: • PSWP submitted by a provider is always distinguishable from non-PSWP? Note: If its listing is revoked, a PSO must be able to transfer, return, or otherwise handle the PSWP it collected or analyzed for each provider consistent with the disposition requirements at section 3.108(b)(3) of the Patient Safety Rule.

Row	Security Requirements	Sample Self-Assessment Questions
6	Section 3.106(b)(2)(ii) Protection of the media, whether in electronic, paper, or other media or format, that contain patient safety work product, limiting access to authorized users, and sanitizing and destroying such media before their disposal or release for reuse.	Do the PSO's policies and procedures: ▪ Permit PSWP to be used off-site by its workforce, contractors, or vendors? If so, how does the PSO provide for the encryption of PSWP in any electronic storage device for transfer or use offsite (e.g., laptops, portable hard drives)? If not, how does the PSO ensure the protection of PSWP? ▪ Prohibit the use of wireless access to PSWP that is not encrypted? ▪ Provide for the complete sanitation of equipment and media that contained PSWP when it is being taken out of service? If the PSO is not using hard drive erasure software, how will it ensure complete sanitation? ▪ Ensure an appropriate level of security/strength and related security measures for passwords and/or other authentication modalities for authorized users?

Row	Security Requirements	Sample Self-Assessment Questions
7	Section 3.106(b)(2)(iii) Physical and environmental protection, to control and limit physical and virtual access to places and equipment where patient safety work product is received, accessed, or handled.	Does the PSO have: ▪ A physical security plan to prevent unauthorized external access to the portion of the facility in which PSWP is handled (as defined in section 3.106(a))? For example, do the PSO's offices or facilities have guards, video surveillance, timed locks, etc.? ▪ Controls to prevent unauthorized physical access, tampering, and theft of PSWP within the facility? These could include locked doors, signs warning of restricted areas, surveillance cameras, alarms, and identification numbers and security cables on computers. ▪ An individual who is responsible for maintaining physical and/or electronic security (i.e., responsible for administering access keys or user logins/passwords)? ▪ Policies and procedures for how this security will be maintained (e.g., new hire review, periodic, recurring access level review, timeframe for removal of terminated employees)? ▪ Additional security measures in place to protect facility-based and virtual workstations with PSWP, such as using privacy screens, enabling password protected screen savers or an automatic logoff functionality for inactive workstations? ▪ Records of when maintenance workers who are not part of the PSO's workforce (e.g., plumber, electrician, painter, facility staff) have access to locations in which PSWP is maintained? Has the PSO adopted safeguards against the potential threat of electronic intrusion? For example, does the PSO have— ▪ Hardware firewalls to prevent intrusion from hackers or malicious software? If not, does the PSO take other steps to preclude external intrusion (e.g., maintaining PSWP on computers that are not connected to the internet)? ▪ Does the PSO have port restrictions for wired jacks that connect to a network to ensure users cannot plug home/unmanaged/inappropriate devices into a network that may contain PSWP?

Security Control and Monitoring A PSO must address:		
Row	**Security Requirements**	**Sample Self-Assessment Questions**
8	Section 3.106(b)(3)(i) Identification of those authorized to receive, access, or handle patient safety work product and an audit capacity to detect unlawful, unauthorized, or inappropriate receipt, access, or handling of patient safety work product.	Is the PSO able to: ▪ Authenticate authorized users (internally) and authorized recipients externally (e.g., contractor staff, providers, etc.) submitting PSWP to the PSO? ▪ Track access by authorized users? ▪ Determine if PSWP has been received, accessed, or handled by an unauthorized user?
9	Section 3.106(b)(3)(ii) Methods to prevent unauthorized receipt, access, or handling of patient safety work product.	In addition to the questions posed elsewhere in this table— ▪ Is it possible to access PSWP from outside the PSO's facility? If so, what types of security are required to obtain access? ▪ Are there policies and procedures in place for monitoring server logs to review unauthorized attempts at access to the information system(s) containing PSWP?

Security Assessment A PSO must address:		
Row	**Security Requirements**	**Sample Self-Assessment Questions**
10	Section 3.106(b)(4)(i) Periodic assessments of security risks and controls to establish if its controls are effective, to correct any deficiency identified, and to reduce or eliminate any vulnerabilities.	Does the PSO conduct periodic assessments of its security risks and controls for PSWP? Did all such risk assessment meet prevailing industry standards or practices? What did the PSO determine were its principal points of vulnerability for the protection of PSWP and how do its security standards address those major vulnerabilities? If the PSO did not conduct a risk assessment before developing its security plan for PSWP, how did the PSO determine that the standards it adopted were adequate and reasonable? Has the PSO established a schedule for periodic risk analyses? If so, on what basis did the PSO establish the frequency with which it will conduct risk analyses?
11	Section 3.106(b)(4)(ii) System and communications protection to monitor, control, and protect PSO receipt, access, or handling of patient safety work product with particular attention to the transmission of patient safety work product to and from providers, other PSOs, contractors or any other responsible persons.	How has the PSO addressed the vulnerabilities that exist when PSWP is transmitted? For example: ▪ How does the PSO ensure the secure transportation and/or transmission to the PSO of PSWP to and from its reporting providers? ▪ How does the PSO ensure secure communications with its reporting providers of PSWP? ▪ Do the PSO's policies address secure email, avoiding discussion of PSWP when using cell phones that may be easily compromised, avoiding the use of unsecure fax machines, etc.?