



WHAT HAS CHANGED?

Disposition of Records

When an SUD patient sends an incidental message to the personal device of an employee of a Part 2 program, the employee will be able to fulfill the Part 2 requirement for “sanitizing” the device by deleting that message.



WHAT HAS CHANGED?

Consent Requirements

An SUD patient may consent to disclosure of the patient's Part 2 treatment records to an entity (e.g., the Social Security Administration), without naming a specific person as the recipient for the disclosure.



WHAT HAS CHANGED?

Disclosures Permitted w/ Written Consent

Disclosures for the purpose of “payment and health care operations” are permitted with written consent, in connection with an illustrative list of **18 activities** that constitute payment and health care operations now specified under the regulatory provision.

NOTE: The 18 activities can be found within the “What are Payments and Health Care Operations” document provided



WHAT HAS CHANGED?

Disclosures to Central Registries and PDMPs

Non-OTP (opioid treatment program) and non-central registry treating providers are now eligible to query a central registry to determine whether their patients are already receiving opioid treatment through a member program.

OTPs are permitted to enroll in a state prescription drug monitoring program (PDMP), and permitted to report data into the PDMP when prescribing or dispensing medications on Schedules II to V, consistent with applicable state law.



WHAT HAS CHANGED?

Medical Emergencies

Declared emergencies resulting from natural disasters (e.g., hurricanes) that disrupt treatment facilities and services are considered a “bona fide medical emergency,” for the purpose of disclosing SUD records without patient consent under Part 2.



WHAT HAS CHANGED?

Audit and Evaluation

Clarifies specific situations that fall within the scope of permissible disclosures for audits and/or program evaluation purposes.



Here are some of the other changes that ARE implemented:

- Any provider who legally holds patient identifying information may now disclose that information to scientific researchers who meet specific regulatory requirements.
- Researchers may link data they hold with data held in other data repositories if both the researcher and repository meet specific regulatory requirements. This change was designed to encourage research on substance use disorders.
- Patients who have consented to sharing their data may request a list of who has looked at their medical records
- Option for programs to use an abbreviated notice of the re-disclosure prohibition when disclosing Part 2 information;



Here are some of the other changes that ARE implemented:

- The ability to disclose Part 2 information to contractors, subcontractors and legal representatives (“contractors”) for payment and health care operations activities without additional patient consent, if certain conditions are met; and
- The ability of lawful holders to disclose Part 2 information for Medicaid, Medicare or Children’s Health Insurance Program (“CHIP”) audit or evaluation activities if certain conditions are met.



Here are some of the other changes that ARE implemented:

- Patients may consent to allowing disclosure of their information to providers through health information exchanges, according to the regulations of their state and HIE. This change is intended to allow patients to share information with their providers and with integrated healthcare systems, yet retain control over who can see their data.
- Audit and evaluation procedures determine if an organization meets Centers for Medicare and Medicaid Services (CMS) requirements for a CMS-regulated accountable care organization (ACO) or similar CMS-regulated organizations. This helps ensure that CMS-regulated entities can perform necessary audit and evaluation activities, including financial and quality assurance functions.



How can one get access to patient's information under SAMHSA 42 CFR Part 2

- To access a patient's medical records under SAMHSA, you must be a participating member of a health information exchange.
- If you are a participating member, you can look at all your patient's medical records after they have signed a Part 2–compliant consent form.
- If patient has signed a consent form that covers only general medical records, you will not be able to look at any records about substance abuse treatment until they sign a second, specific release.
- You must obtain a signed consent form for your patients, even if they have signed consent forms for other providers.
- Patient may withdraw consent at any time.



HIPAA and Part 2

42 CFR Part 2 RULEMAKING

Issuance of the 2022 Notice of Proposed Rulemaking (NPRM)

The Coronavirus Aid, Relief, and Economic Security (CARES) Act (enacted March 27, 2020) requires HHS to align certain aspects of Part 2 with the HIPAA rules and also requires HHS to update the HIPAA Privacy Rule Notice of Privacy Practices requirements to address Part 2 protections and individual rights.



The NPRM proposes to:

- Permit Part 2 programs to use and disclose Part 2 records based on a single prior consent signed by the patient for all future uses and disclosures for treatment, payment, and health care operations.
- Permit the redisclosure of Part 2 records as permitted by the HIPAA Privacy Rule by recipients that are Part 2 programs, HIPAA covered entities, and business associates, with certain exceptions.
- Expand prohibitions on the use and disclosure of Part 2 records in civil, criminal, administrative, or legislative proceedings conducted by a federal, state, or local authority against a patient, absent a court order or the consent of the patient.



The NPRM proposes to:

- ✓ Create two patient rights under Part 2 that align with individual rights under the HIPAA Privacy Rule:
 - ✓ Right to an accounting of disclosures
 - ✓ Right to request restrictions on disclosures for treatment, payment, and health care operations.
- ✓ Require disclosures to the Secretary for enforcement.
- ✓ Apply HIPAA civil and criminal penalties to Part 2 violations.
- ✓ Require Part 2 programs to establish a process to receive complaints of Part 2 violations.
- ✓ Prohibit Part 2 programs from taking adverse action against patients who file complaints.



The NPRM proposes to:

- ✓ Prohibit Part 2 programs from requiring patients to waive the right to file a complaint as a condition of providing treatment, enrollment, payment, or eligibility for services.
- ✓ Apply the standards in the HIPAA Breach Notification Rule to breaches of Part 2 records by Part 2 programs.
- ✓ Modify the Part 2 confidentiality notice requirements ("Patient Notice") to align with the HIPAA.



The NPRM proposes to:

- ✓ Modify the HIPAA Notice of Privacy Practices requirements for covered entities who receive or maintain Part 2 records to include a provision limiting redisclosure of Part 2 records for legal proceedings according to the Part 2 standards.
- ✓ Permit investigative agencies to apply for a court order to use or disclose Part 2 records after they unknowingly receive Part 2 records in the course of investigating or prosecuting a Part 2 program, when certain preconditions are met.



NOTE

While HHS is undertaking this rulemaking, the current Part 2 regulations remain in effect.



MEDICAL RECORDS ARE NOT CREATED EQUAL





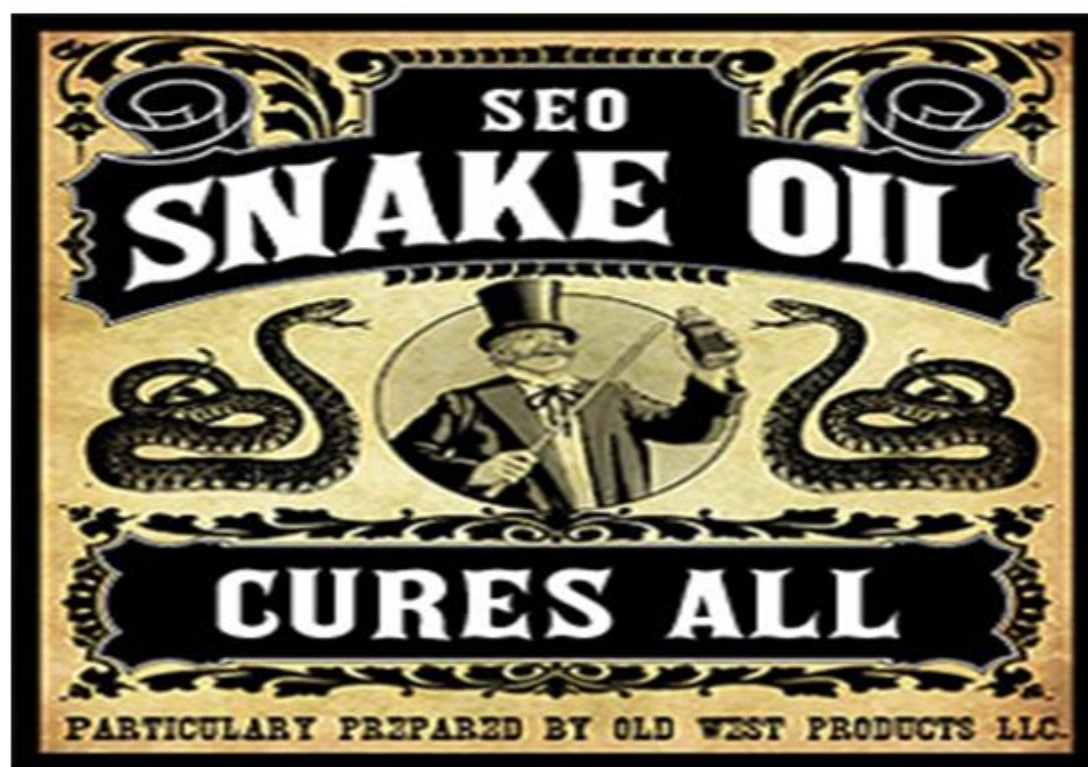
SEPARATING SUD RECORDS FROM NORMAL MEDICAL RECORDS

- Higher risks potential legal consequences for not properly securing SUD records
- In general, SUD records are only to be accessed by the provider of care (with limited exceptions as discussed later)
- Almost like attorney/client privilege
- If possible, within the EMR system, lock SUD portion of medical record to specific provider
- Ensure all EMR audit capabilities are enabled and audit trails are reviewed periodically

HIPAA RESOURCES



ALWAYS FACT CHECK WITH WWW.HHS.GOV
DON'T FALL FOR SNAKE OIL!!



<https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html>

The screenshot shows a web browser window with the URL <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html>. The page features a navigation bar with links for "HIPAA for Individuals", "Filing a Complaint", "HIPAA for Professionals", and "Newsroom". Below the navigation bar, a breadcrumb trail reads: "HHS > HIPAA Home > For Professionals > Compliance Enforcement > Audit > Audit Protocol".

On the left side, there is a sidebar menu with the following items: "HIPAA for Professionals", "Regulatory Initiatives", "Privacy", "Security", "Breach Notification", "Compliance & Enforcement" (which is expanded to show "Enforcement Rule", "Enforcement Process", "Enforcement Data", "Resolution Agreements", "Case Examples", "Audit", "Reports to Congress", and "State Attorneys General"), and "Audit".

The main content area is titled "Audit Protocol – Updated July 2018". It includes a text description of the Phase 2 HIPAA Audit Program, which reviews policies and procedures of covered entities and business associates. The text mentions that the audit protocol is updated to reflect the Omnibus Final Rule and is organized by Rule and regulatory provision. It also provides a link to submit feedback to OCR at OSOCRAudit@hhs.gov.

Below the text, there is a section titled "General Instructions" with a list of four numbered points:

1. Where the document says "entity," it means both covered entities and business associates unless identified as one or the other;
2. *Management* refers to the appropriate privacy, security, and breach notification official(s) or person(s) designated by the covered entity or business associate for the implementation of policies and procedures and other standards;
3. Entities must provide only the specified documents, not compendiums of all entity policies of procedures. The auditor will not search for relevant documentation that may be contained within such compilations;
4. Unless otherwise specified, all document requests are for versions in use as of the date of the audit notification and document request;

At the bottom right of the main content area, there is a blue button labeled "top". The Windows taskbar is visible at the bottom of the screen, showing the time as 9:44 AM on 2/4/2019.

<http://www.healthit.gov/providers-professionals/security-risk-assessment-tool>

UPDATED SRA TOOL Version 3.0

The screenshot shows the HealthIT.gov website with the Security Risk Assessment tool page. The page has a blue header with the HealthIT.gov logo and navigation links. A sidebar on the left lists various resources under 'Privacy, Security, and HIPAA'. The main content area features a 'Security Risk Assessment' section with a description of the tool's purpose and a 'New! Security Risk Assessment Tool Version 3.0' announcement. Below this, there are links to download the tool, user guides, and tutorial videos. A 'Need Help?' section on the right provides contact information for assistance.

Security Risk Assessment | HealthIT.gov

Official Website of the Office of the National Coordinator for Health Information Technology (ONC)

CONTACT | EMAIL UPDATES

Connect with us: LinkedIn Twitter Facebook

TOPICS | HOW DO IT | BLOG | NEWS | ABOUT ONC

Search

Home > Topics > Privacy, Security, and HIPAA > Security Risk Assessment

Privacy, Security, and HIPAA

- Educational Videos
- HIPAA Basics
- Privacy & Security Resources & Tools
- Security Risk Assessment**
 - Security Risk Assessment Tool
 - Security Risk Assessment Videos
 - Top 10 Myths of Security Risk Analysis
- Privacy & Security Training Games
- Model Privacy Notice (MPN)
- How APIs in Health Care can Support Access to Health Information: Learning Module
- Patient Consent and Interoperability

Security Risk Assessment

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule requires that covered entities and its business associates conduct a risk assessment of their healthcare organization. A risk assessment helps your organization ensure it is compliant with HIPAA's administrative, physical, and technical safeguards. A risk assessment also helps reveal areas where your organization's protected health information (PHI) could be at risk. To learn more about the assessment process and how it benefits your organization, [click here](#), visit the [Office for Civil Rights' official guidance](#).

New! Security Risk Assessment Tool Version 3.0

ONC, in collaboration with the HHS Office for Civil Rights (OCR), developed a new version of the downloadable Security Risk Assessment Tool (SRA Tool) to help guide you through the process.

[Download Version 3.0 of the SRA Tool \(.msi\) - 71.8 MB](#)

[Download the XML update file \(.XML\) - 323 KB](#)

For details on how to use the tool, download the SRA Tool User Guide (PDF - 3.2 MB)*.

Watch videos on contingency planning and what a risk assessment may involve

Read the HHS Press Release on release of SRA Tool 3.0 in October 2018.

Legacy Version: Security Risk Assessment Tool Version 2.0

Note that you can't directly transfer data from 2.0 to 3.0, but can upload certain portions (e.g., lists of assets and BAAs). Refer to the SRA Tool User Guide 3.0 for more information.

[Download Former SRA Tool 2.0](#)

[Download the SRA 2.0 event files from the April 29 Webinar \(ZIP - 4 MB\)](#)

[Download the SRA Tool 2.0 User Guide \(PDF - 4.5 MB\)](#)

From 2015: Watch videos on what a risk assessment may involve, and learn how to use the SRA Tool 2.0 by watching the SRA Tool Tutorial videos.

From 2015: learn how to use the SRA Tool 2.0 by watching the SRA Tool Tutorial videos.

[Download the SRA Tool 2.0 User Guide \(PDF - 4.5 MB\)](#)

Paper-based version of the SRA 2.0 tool is also available:

- Administrative Safeguards (DOCX - 397 KB)*
- Technical Safeguards (DOCX - 312 KB)*

Need Help?

Please leave any questions, comments, or feedback about the SRA Tool using our [Health IT Feedback Form](#). This includes any trouble in using the tool or problems/bugs with the application itself. Also, please feel free to leave any suggestions on how we could improve the tool in the future.

[Submit Questions Or Feedback](#)

Type here to search

9:04 AM 1/9/2019

SAMHSA RESOURCES




www.samhsa.gov

Secure <https://www.samhsa.gov/about-us/who-we-are>

Home Newsroom Site Map Contact Us

 Substance Abuse and Mental Health Services Administration

Search SAMHSA.gov

Connect with SAMHSA:    

Find Help & Treatment Topics Programs & Campaigns Grants Data **About Us** Publications

About Us » Who We Are   

About Us

Who We Are

Leadership
Regional Administrators
Offices and Centers
Laws and Regulations

Interagency Activities
Advisory Councils
Strategic Initiatives
Budget
Jobs and Internships
Social Media
Frequently Asked Questions
Contact Us
Newsroom

Who We Are

The Substance Abuse and Mental Health Services Administration (SAMHSA) is the agency within the U.S. Department of Health and Human Services that leads public health efforts to advance the behavioral health of the nation. SAMHSA's mission is to reduce the impact of substance abuse and mental illness on America's communities.

Congress established the Substance Abuse and Mental Health Services Administration (SAMHSA) in 1992 to make substance use and mental disorder information, services, and research more accessible. SAMHSA is a public agency within the U.S. Department of Health and Human Services (HHS).

Prevention, treatment, and recovery support services for behavioral health are important parts of the health service systems for the community. The services work to improve our health and minimize costs to individuals, families, businesses, and governments. However, people suffering from either substance use and mental disorders, or both, because of their illness are often excluded from the current health care system and instead have to rely on "public safety net" programs. Last year alone, close to 20 million people in need of substance abuse treatment did not receive it. Further, an estimated 11.8 million people reported an unmet need for mental health care. The gap in service to this population unnecessarily jeopardizes the health and wellness of people and causes a ripple effect in costs to American communities.

Vision

SAMHSA provides leadership and devotes its resources, including programs, policies, information and data, contracts and grants, to help the United States act on the knowledge that:

- Behavioral Health is essential to health
- Prevention works
- Treatment is effective
- People recover from mental and substance use disorders

Best Course of Action

BE PROACTIVE!!



THE END

Q&A

www.hipaa-consulting.com