Pharmacy Health Information Technology Collaborative

Via Electronic Submission to: http://www.regulations.gov

April 11, 2016

The Substance Abuse and Mental Health
Service Administration
Department of Health and Human Services
Attention: SAMHSA-4162-200
5600 Fishers Lane, Room13No2B
Rockville, MD 20857

Re: SAMHSA-4162-20 – Confidentiality of Substance Use Disorder Patient Records

Dear Sir/Madam:

On behalf of the membership of the Pharmacy Health Information Technology Collaborative (Collaborative), we are pleased to submit comments on *SAMHSA-4162-20 – Confidentiality of Substance Use Disorder Patient Records.*

Pharmacists provide patient-centered care and services, maintain secure patient care records, and as part of the integrated health care team, they are directly involved with other health care providers and patients in various practice settings, which may include Part 2 programs for substance use disorder.

The Collaborative supports the objective of maintaining confidentiality of substance use disorder patient records. In reviewing the proposed rule, however, we note that requiring the use of secure, certified health IT, networks, and devices, especially for the transmission of patient records, does not appear to be included in the proposed provisions. We believe this should be a requirement for safeguarding patient records. Cybercrime and threats are a fast-growing challenge. Also requiring the use of secure health IT for the transport of patient records would bring the proposed rule into alignment with the Office of the National Coordinator's *Federal Health IT Strategic Plan 2015-2020* and *Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap*, as well as the certified health IT requirements for the Meaningful Use Electronic Health Record Incentive Program.

The Collaborative has been involved with the federal agencies developing the national health IT framework since 2010. The Collaborative is supportive of recommendations to improve the safety of health IT through coordinated governance

and safely designed and implemented systems, while maintaining and protecting patient privacy.

The following are our comments for *SAMHSA-4162-20 – Confidentiality of Substance Use Disorder Patient Records.*

§2.11 Definitions
Patient identifying information

The Collaborative recommends including phone numbers and email addresses as part of patient identifying information. Although this definition lists some specifics and includes "or similar information by which the identity of a patient…can be determined with reasonable accuracy…by reference or other publicly available information," we believe additional examples, particularly regarding those publicly accessible by electronic means, should be provided. Through electronic telephone directories and other online databases available and accessible on the Internet, reverse phone lookup and reverse phone number lookup can be used to not only identify an individual's name but can also be used to find the individual's address and email address. Reverse email address searches online can also be conducted for obtaining individual identifying information.

§2.13 Confidentiality restrictions and safeguards

The Collaborative recommends defining the terms "in writing" and "written requests" and adding them to §2.11 Definitions. It is not clear under this section if the intent of these terms means solely the use of paper or if they include using electronic documents. With changing technology, understanding these terms is critical for implementing confidentiality restrictions and safeguards, as writing does include the use of electronic documents, email, etc. Many health care practices and health care facilities are also now using electronic tablets with patients and other aspects of electronic media for obtaining written requests and consent. This section should be consistent with other sections of this proposed rule in which paper and electronic documents are stated as permitted.

Also, security for the transmission of consented disclosures is not addressed if being done electronically and appears to be missing throughout the proposed rule. We recommend that the use of secure, certified health IT be added as a requirement for not only this section but for implementing the proposed rule to protect any transmission of information contained in patient records. Requiring this would also bring the proposed rule more into alignment with the Office of the National Coordinator's *Federal Health IT Strategic Plan 2015-2020* and *Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap*, as well as the health IT requirements for the Meaningful Use Electronic Health Record Incentive Program.

§2.16 Security for records

The Collaborative supports requiring that those holding patient identifying information have formal policies and procedures in place for paper and electronic records to protect against unauthorized uses and disclosures and anticipated threats or hazards to patient identifying information. What appears to be missing from the proposed requirement, however, are security standards that should be met and incorporated into policies and procedures. There is no mention of security standards in this section.

The HIPAA Privacy, Security, and Breach Notification Rules cover paper and electronic health records and apply to most health care providers. These rules set out national privacy and security standards that must be followed. We recommend that compliance with the HIPAA security standards, at a minimum, be written into this section as a requirement for establishing formal policies and procedures.

As noted in our comments for §2.13, security for the transmission of electronic health records or patient records is not addressed in this section and appears to be missing throughout the proposed rule. We recommend that the use of secure, certified health IT also be added as a requirement to protect any transmission of information contained in patient records.

§2.19 Disposition of records by discontinued programs

The Collaborative supports the proposed requirements for removing or destroying patient identifying information from paper and electronic records if a Part 2 program discontinues operation. We also request the agency to clarify one aspect. In this section, the requirements for removing or destroying such information also apply if a Part 2 program is taken over or acquired by another program. Does this mean that the acquiring program would need to start from scratch and create new patient records for existing patients that it may acquire from the Part 2 program?

§2.31 Consent requirements

The Collaborative supports the use of paper and electronic format for the required elements of written consent, though, a security requirement should be added. As noted in our comments for §2.13, security for obtaining consent and the transmission of electronic health records or patient records is not addressed. We recommend that the use of secure, certified health IT be added as a requirement to protect any transmission of information contained in patient records.

§2.34 Disclosures to prevent multiple enrollments

The Collaborative supports allowing a Part 2 program to disclose patient records to a withdrawal management or maintenance treatment program not more than 200 miles away for the purpose of preventing the multiple enrollment of a patient as specified under the proposed provisions. We request a clarification and have a recommendation.

The proposal would also allow a Part 2 program to disclose patient records to a central registry. This is the only section in the proposal in which disclosure to a central registry is mentioned. We request clarification as to what type of central registry is being considered. Our reason for requesting this clarification is that it is not clear if such a central registry would include Prescription Drug Monitoring Programs (PDMPs).

Part 2 protections include a prohibition on the redisclosure of information received directly from a Part 2 program. A pharmacy receiving electronic prescription information directly from a Part 2 program must obtain patient consent to send that information to a PDMP. Patient consent is also required for the PDMP to redisclose that information to those with access to the PDMP. Because pharmacy systems are not able to identify which providers are subject to Part 2, this could make it difficult to prevent Part 2 data from reaching the PDMP. This was on the list of topics discussed at a SAMHSA public listening session on June 11, 2014 regarding the *Confidentiality of Alcohol and Drug Abuse Patient Regulations*. It is not clear if a resolution to this concern was developed.

As noted in our comments for §2.13, security for the transmission of electronic health records or patient records, including those to a central registry or other withdrawal programs, is not addressed and appears to be missing throughout the proposed rule. We recommend that the use of secure, certified health IT be added as a requirement to protect any transmission of information contained in patient records.

Subpart D – Disclosures Without Medical Emergencies

§2.51 Medical emergencies
(b) Special rule

The Collaborative supports the special rule allowing the disclosure of patient identifying information to medical personnel at the Food and Drug Administration (FDA) who provide a reason to believe that the health of any individual may be threatened by an error in manufacture, labeling, or sale of a product under the FDA's jurisdiction and that the information is to be used solely for the exclusive purpose of notifying patients or their physicians of potential dangers. We do, however, have a concern.

As noted in our comments for §2.13, security for the transmission of electronic health records or patient records is not addressed and appears to be missing throughout the proposed rule. We recommend that the use of secure, certified health IT be added as a requirement to protect any transmission of information contained in patient records.

§2.53 Audits and evaluation
(b) Copying, removing, downloading, or forwarding patient records

The Collaborative is supportive of the provisions for audits and evaluation. We do, however, have a concern.

As noted in our comments for §2.13, security for the transmission of electronic health records or patient records is not addressed and appears to be missing throughout the proposed rule. We recommend that the use of secure, certified health IT be a written requirement for not only Part 2 program providers but also for those organizations, firms, etc., that will conduct such audits and evaluations to protect any transmission of information contained in patient records.

*****

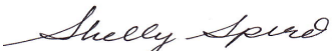
The Pharmacy HIT Collaborative's vision and mission are to assure the nation's health care system is supported by meaningful use of HIT, the integration of pharmacists for the provision of quality patient care, and to advocate and educate key stakeholders regarding the meaningful use of HIT and the inclusion of pharmacists within a technology-enabled integrated health care system. The Collaborative was formed in the fall of 2010 by nine pharmacy professional associations, representing 250,000 members, and also includes associate members from other pharmacy-related organizations. The Pharmacy HIT Collaborative's founding organizations represent pharmacists in all patient care settings and other facets of pharmacy, including pharmacy education and pharmacy education accreditation. The Collaborative's Associate Members represent e-prescribing and health information networks, a standards development organization, transaction processing networks, pharmacy companies, system vendors and other organizations that support pharmacists' services. For additional information, visit www.pharmacyhit.org.

*****

On behalf of the Pharmacy HIT Collaborative, thank you again for the opportunity to comment on *SAMHSA-4162-20 – Confidentiality of Substance Use Disorder Patient Records.*

For more information, contact Shelly Spiro, Executive Director, Pharmacy HIT Collaborative, at shelly@pharmacyhit.org.

Respectfully submitted,



Shelly Spiro
Executive Director, Pharmacy HIT Collaborative

Shelly Spiro, RPh, FASCP
Executive Director
Pharmacy HIT Collaborative
shelly@pharmacyhit.org

Mary Jo Carden, RPh, JD
Vice President, Govt. & Pharmacy Affairs
Academy of Managed Care Pharmacy
mcarden@amcp.org

Peter H. Vlasses, PharmD, DSc (Hon), BCPS, FCCP
Executive Director
Accreditation Council for Pharmacy Education (ACPE)
pvlasses@acpe-accredit.org

Rylan Hanks, PharmD
Regulatory Intelligence
Global Regulatory and R&D Policy – Biosimilars
Amgen, Inc.
rhanks@amgen.com

William Lang, MPH
Senior Policy Advisor
American Association of Colleges of Pharmacy
wlang@aacp.org

C. Edwin Webb, Pharm.D., MPH
Associate Executive Director
American College of Clinical Pharmacy
ewebb@accp.com

Arnold E. Clayman, PD, FASCP
Vice President of Pharmacy Practice & Government Affairs
American Society of Consultant Pharmacists
Aclayman@ascp.com

Tony Matessa
Cardinal Health - Commercial Technologies
Director, Product Marketing Lead
www.cardinalhealth.com/fuse

Steve Long
Director, Technical Operations, Retail Services
Greenway Health
steve.long@greenwayhealth.com

Rebecca Snead
Executive Vice President and CEO
National Alliance of State Pharmacy Associations
rsnead@naspa.us

Stephen Mullenix. RPh
Senior Vice President, Communications & Industry Relations
National Council for Prescription Drug Programs (NCPDP)
smullenix@ncpdp.org

Cynthia Kesteloot
Vice President of Operations
OutcomesMTM
ckesteloot@outcomesmtm.com

Cathy DuRei
Director, Trade Channel Management
Pfizer US Trade Group
Cathy.DuRei@Pfizer.com

Adrian Durbin
Director, Public Policy
McKesson Corporate Public Affairs
Adrian.Durbin@McKesson.com