Patient Event Notifications

What Arizona Hospitals Need to Know
TABLE OF CONTENTS

EXECUTIVE SUMMARY 3
BREAKING IT DOWN: THE CMS ALERT REQUIREMENTS 4
   Hospitals subject to the alert requirement 4
   Hospital compliance under the new CoP 4
   The minimum alert content and technical requirements 5
   When alerts must be sent 5
TO WHOM ALERTS MUST BE SENT AND THE STANDARDS 6
HOSPITALS MUST MEET 6
   Who should receive these alerts? 6
   What does making “reasonable efforts” mean? 7
   Do recipients of alerts have any say in what the hospitals send to them? 9
   What about patient preferences? 10
USING INTERMEDIARIES TO MEET THE ALERT REQUIREMENTS 10
SENDING ALERTS - AT A GLANCE 11
PRIVACY OBLIGATIONS UNDER THE CoP 12
   HIPAA, Arizona State Confidentiality Laws and Alerts 12
   42 C.F.R. Part 2 and Alerts 13
   Arizona’s Health Information Organization (HIO) Law 13
WHAT HOSPITALS CAN EXPECT FROM SURVEYORS 14
REFERENCES & NOTES 16
ABOUT HEALTH CURRENT 17

A special thanks to Melissa Soliz, JD, Partner with Coppersmith Brockelman, PLC in Phoenix, AZ, for her contributions to this white paper.
EXECUTIVE SUMMARY

In May 2020, the Centers for Medicare & Medicaid Services (CMS) published the CMS Interoperability and Patient Access final rule that adds a new Condition of Participation (CoP) for hospitals. In an effort to support the care continuum, CMS will soon require hospitals to alert primary care providers (PCPs) and post-acute care providers (PACs) when patients are admitted, discharged, or transferred (ADT) from the emergency department (ED) or inpatient services. Whereas CMS refers to these alerts as Patient Event Notifications, they are commonly recognized as ADT alerts. The deadline for hospitals to comply with this new requirement is May 2, 2021.

The new requirement applies to hospitals (including psychiatric hospitals and critical access hospitals) that participate in Medicare or Medicaid and have an electronic system using HL7® version 2.5.1 or newer. This is typically the patient registration system, which can be a stand-alone administrative system or part of an electronic health record (EHR) system.

Hospitals with these technical capabilities must use reasonable efforts to send real-time alerts — directly or through an intermediary, such as a health information exchange (HIE) — to the patient’s PACs and PCPs who need to receive notification of the patient’s status for treatment, care coordination, or quality improvement purposes.

Non-compliance may threaten a hospital’s certification and ability to recoup payments from Medicare and Medicaid. Therefore, it is critical that hospitals understand the updated CoP and have a plan in place to meet the technical and administrative requirements.

This white paper breaks down the new CMS requirements for Patient Event Notification alerts and strategies for meeting these new compliance obligations. It is intended for educational purposes only and does not constitute legal advice. Please consult with legal counsel for guidance on how these federal laws apply to your organization.
BREAKING IT DOWN: THE CMS ALERT REQUIREMENT

Hospitals subject to the alert requirement
The new ADT alert requirements apply to hospitals participating in Medicare or Medicaid, including psychiatric hospitals and CAHs, with a system (e.g., patient registration or electronic health record (EHR) system) that uses HL7® version 2.5.1 or newer messaging standard. The hospital is not required to purchase a system if its current one does not support HL7® version 2.5.1. Thus, a hospital is exempt from the new CoP ADT Alert requirements if the hospital’s system utilizes a version of HL7 older than version 2.5.1.

Hospital compliance under the new CoP
CMS Certification is critical for hospitals because it determines whether they receive CMS payments. CMS payments make up a significant portion of the hospital’s payer mix. A hospital must meet all CoP requirements in order not to jeopardize its certification.

Under the new CoP, a hospital must demonstrate that:

• Its system is fully operational and operates in accordance with state and federal laws for health information
• Its system sends the minimum patient information, including patient name, treating practitioner name, and sending institution name
• Its system sends the ADT alerts either directly or through an intermediary at the time of ED registration or inpatient admission, and either immediately prior to or at the time of discharge/transfer to the providers specified in the CoP
• The hospital has made a reasonable effort to send the ADT alerts to all the providers specified in the CoP to the extent it is:
  o Permissible under applicable federal and state law and regulations
  o Not inconsistent with the patient’s expressed privacy preferences

This white paper breaks down and explores each of these requirements.
The minimum ADT alert content and technical requirements

The data elements required for the ADT notification are minimal:

- Patient name
- Treating practitioner (i.e., attending physician)
- Sending institution name (i.e., hospital)

Hospitals are not precluded from sending additional data elements. CMS encourages hospitals to consider other information that can be added to the ADT alerts to support care coordination or to meet a hospital’s other compliance obligations under the discharge planning CoP and Promoting Interoperability Program. Other data mentioned in the CMS Rule includes: diagnosis, chief complaint, discharge disposition, medication list, insurance policy coverage, other data that can be used for patient matching, hospital address and tax ID, contact information for other resources, etc. However, additional data elements should be included only if permitted by other state and federal laws applicable to the health information at issue (such as, HIPAA, 42 C.F.R. Part 2, and state confidentiality laws).

There is no particular format required for the alert. Similarly, there is no particular transport protocol (method of making this ADT alert available) mandated in the CoP. However, CMS does describe these notifications as being automated, electronic communications. Examples of acceptable transport protocols mentioned by CMS include (but are not limited to) Direct messaging and FHIR-based API. Hospitals and recipients have discretion in deciding what electronic delivery methods work best for them. Moreover, the CoP does not require exclusive use of a single method. A mix of methods may be used to meet the CoP requirements.

When ADT alerts must be sent

The following events trigger the ADT alert requirement:

- ED registration (including for observation)
- Hospital inpatient admission
- Discharge from the hospital’s ED
- Transfer from the hospital’s ED (i.e., to the hospital’s inpatient services)
- Discharge or transfer from the hospital’s inpatient services
ADT alerts are not required to be sent for:
- Other transfers within the hospital, such as from one inpatient service department to another inpatient service department
- Outpatient procedures (e.g., radiology, cardiac catheterization, outpatient surgery)

The required timing of the ADT alerts is essentially real time. That is:
- For admission or registration: at the time of such admission or registration
- For discharge or transfer: immediately prior to, or at the time of, such discharge or transfer

The ADT alert should not be sent:
- To a provider where not permissible under applicable federal and state law and regulations
- Where sending the ADT alert would be inconsistent with the patient’s expressed privacy preferences

The CoP does not limit ADT alerts to only Medicare and Medicaid patients. Hospitals should therefore plan to send ADT alerts for all patients who meet the criteria above.

TO WHOM ADT ALERTS MUST BE SENT AND THE STANDARDS HOSPITALS MUST MEET

Who should receive these ADT alerts?
Hospitals must make “reasonable efforts” to send the ADT alerts to the following providers which need to receive notification of the patient’s status for treatment, care coordination or quality improvement purposes:
- All “applicable” post-acute care services providers and suppliers (collectively, “PACs”)
- A patient’s “established” PCP practitioner or group, or other practitioner/group identified by the patient as primarily responsible for the patient’s care (collectively, “PCPs”)

Applicable PACs include:
- The PAC from which the patient was transferred to the hospital
- The PAC to which the patient is being transferred or referred from the hospital
Examples of common PACs are hospices, home health agencies and skilled nursing facilities. Established PCPs include:

- The PCP who has a care relationship that the patient recognizes as primary
- The PCP that is evidenced by documentation of the relationship in the patient’s medical record
- The PCP who referred the patient to the hospital

Examples of common PCPs include practitioners who specialize in general or family medicine, internal medicine, geriatrics or pediatrics.

There are no geographic limitations on the PACs and PCPs who should receive ADT alerts. For example, a vacationing patient from Ohio who is seen in an Arizona hospital ED, may trigger an ADT alert to the patient’s PCP in Ohio.

The CoP does not prevent hospitals from sending ADT alerts to others. However, these ADT alerts must not be sent to a patient’s PAC and PCP (or others) if doing so would not be permissible under applicable state and federal laws, or if inconsistent with a patient’s expressed privacy preference. We discuss these privacy related limitations on ADT alerts in greater detail below.

**What does making “reasonable efforts” mean?**

Hospitals are only required to use reasonable efforts to send ADT alerts to the patient’s PACs and PCP. They are not required to ensure receipt of the ADT alerts. The ordinary meaning of reasonable efforts is to use “one or more actions rationally calculated to achieve a stated objective, but not necessarily with the expectation that all possibilities are to be exhausted.” This is consistent with CMS’s decision to abandon its proposed requirement that hospitals have “reasonable certainty” that their ADT alerts are being received. Commenters on the proposed rule challenged the “reasonable certainty” standard as unworkable “given the limitations of the infrastructure that is currently available for sharing health information.” CMS agreed with commenters’ concerns, lowering the standard to
“reasonable efforts” in the final rule and explaining that it expects surveyors to “evaluate whether a hospital is making a reasonable effort to send patient event notifications while working within the constraints of its existing technology infrastructure.”

CMS leaves room for a hospital to demonstrate its system’s capability to meet this requirement in a variety of different ways, such as:

- Having processes and policies in place to identify patients' PCP and incorporate this information into the ADT system, or through recording information received from patients about their providers, such as by:
  - Asking the patient or caregiver during the intake process, or
  - Obtaining the provider information from the patient’s medical record
- Working with an intermediary that maintains information about a patient’s care relationship
- Through an analysis of care patterns or other attribution methods that seek to determine the provider most likely to be able to effectively coordinate care post-discharge for a specific patient
- Allowing a provider to specifically request notifications for a given patient for whom they are responsible for care coordination as confirmed through conversations with the patient

CMS does not require hospitals to use all of these methods. Rather, these are illustrative examples of the various different ways hospitals may employ processes to satisfy the reasonable efforts standard. CMS explains in the final rule that “through these provisions, we sought to allow for different ways that hospital might identify those practitioners.”

And hospitals are not expected to develop the technology to do this on their own. Hospitals may use an intermediary (or intermediaries) to meet this need. For instance, CMS specifically recognizes that many hospitals already use health information exchanges (HIEs) to send ADT alerts and may continue to do so in accordance with the new CoP. CMS writes in the preamble to the final rule:
We believe that the health information infrastructure that exists today will be sufficient to provide substantial support for the requirements we are finalizing in this rule. As other commenters noted, organizations such as health information exchanges are supporting the sharing of patient event notifications in many areas today. While we understand there is variation in availability of this infrastructure, we believe there are options increasingly available for hospitals to implement basic patient event notifications that will allow hospitals to demonstrate they have made a “reasonable effort” to ensure their system sends the required notifications, as per the policy finalized in this final rule.7

CMS does not expect hospitals to send notifications for a patient if:

• The hospital is not able to identify an appropriate recipient
• The recipient is not able to receive an electronic notification
• The recipient is not able to receive the notification in the manner that the hospital can send it

Do recipients of ADT alerts have any say in what the hospitals send to them?
An influx of ADT alerts may be overwhelming or not conducive to PAC and PCP clinical workflows. Hospitals may, but are not required to, honor requests from recipient providers to limit, modify and/or customize the ADT alerts recipients receive. For instance, a PAC or PCP could choose to only accept notifications of discharge and admission, but not transfer.

In the preamble to the final rule, CMS recognizes that these requests for modifications may come directly from the receiving providers or from a provider’s business associate, such as a HIE or accountable care organization (ACO). Because HIEs are business associates of both the hospitals and recipient providers in their networks, HIEs are in a unique position to meet the needs of both hospitals and the PACs/PCPs they are required to alert.

What about patient preferences?
CMS does not intend the CoP requirements to prevent a hospital or its business associates from documenting and honoring a patient’s request to not share their information with
another provider. CMS explains that:

> Based on commenters’ concerns regarding a patient’s ability to request that his or her medical information, in the form of a patient event notification, is not shared with other settings, we are revising and finalizing a requirement in this rule that a hospital (or CAH) must demonstrate that its notification system sends notifications, “to the extent permissible under applicable federal and state law and regulations and not inconsistent with the patient’s expressed privacy preferences.”

However, CMS is also clear that this requirement to honor a patient’s expressed privacy preferences does not impose an affirmative obligation on hospitals to obtain the patient’s express consent to send ADT alerts, unless consent is otherwise required by applicable state or federal privacy laws.

**USING INTERMEDIARIES TO MEET THE ADT ALERT REQUIREMENTS**

The new requirements expressly permit hospitals to send ADT alerts through an intermediary that facilitates the exchange of health information, such as a HIE. Specifically, a hospital may use an intermediary to:

- Send some or all of its ADT alerts
- Determine which receiving providers will receive ADT alerts, such as by partnering with a HIE that uses patient panels to match patient ADT alerts to their other treating providers
- Record patient privacy preferences and honor them

CMS also expressly permits hospitals to make exclusive use of an intermediary to satisfy the ADT alert requirements. However, exclusive use of an intermediary with a limited ability to deliver notifications to the specified set of recipients—for instance an intermediary which restricts its delivery to only those providers within a specific integrated healthcare system—would not satisfy the CoP. Alternatively, if a hospital demonstrates that an intermediary
HIE SUPPORT: SENDING PATIENT EVENT NOTIFICATION ALERTS

<table>
<thead>
<tr>
<th>Trigger</th>
<th>Timing</th>
<th>Target Audience</th>
<th>Data Delivered</th>
</tr>
</thead>
<tbody>
<tr>
<td>ED registration (including for observation)</td>
<td>At the time of</td>
<td>The following providers that need to receive notification of the patient’s status for treatment, care coordination, or quality improvement purposes: • All applicable PACs • Any of the following practitioners and entities: The patient’s established PCP practitioner or group OR Other practitioner/group identified by the patient as primarily responsible for the patient’s care</td>
<td>Minimum data elements: • Patient name • Sending institution (i.e., hospital) • Treating practitioner (i.e., attending physician) If permitted by applicable state and federal law, and not inconsistent with a patient’s expressed privacy preferences</td>
</tr>
<tr>
<td>Inpatient admission</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Discharge or transfer from the ED (including to inpatient)</td>
<td>Immediately prior to OR at the time of</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Discharge or transfer from inpatient services</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This white paper is intended for educational purposes only. It does not constitute legal advice. © 2020 Health Current
connects to a wide range of recipients and does not impose restrictions on which recipients are able to receive notifications through the intermediary, exclusive use of such an intermediary would satisfy the CoP.

**PRIVACY OBLIGATIONS UNDER THE CONDITIONS OF PARTICIPATION**

In addition to meeting the ADT alert requirements discussed above, hospitals must also demonstrate that its system is used in accordance with all state and federal statutes and regulations applicable to the hospital’s exchange of patient health information. Hospitals are not required to send ADT alerts if doing so is not permissible under other state and federal laws. And the CoP does not require hospitals to affirmatively obtain a patient’s authorization or consent to send ADT alerts where such laws would otherwise prohibit disclosure without authorization/consent. This white paper briefly discusses whether HIPAA, 42 C.F.R. Part 2 and Arizona state law permit hospitals to send ADT alerts.

**HIPAA, Arizona State Confidentiality Laws and ADT Alerts**

Hospitals must comply with the Health Information Portability and Accountability Act of 1996 and its implementing regulations, all as amended from time to time, collectively, “HIPAA”. HIPAA permits hospitals and their business associates to use and disclosure protected health information (PHI) without a patient’s authorization for the hospital’s own treatment, payment and healthcare operations purposes, as well as for the treatment purposes of other healthcare providers. Moreover, HIPAA permits disclosures that are required by law. The ADT alerts required by CMS are for treatment purposes and are also required by law. Thus, HIPAA doesn’t require hospitals to collect a patient’s HIPAA authorization in order to send ADT alerts to the patient’s PAC and PCP.

Additionally, the Arizona State Legislature in 2019 amended Arizona’s historically more protective confidentiality statutes for mental health information, communicable disease information and genetic testing information to align with HIPAA. Thus, these state laws will permit hospitals to send ADT alerts to the same extent as permitted by HIPAA.
42 C.F.R. Part 2 and ADT Alerts

Hospitals that operate substance use disorder (SUD) treatment programs within their EDs and/or inpatient services may also need to comply with the more stringent privacy protections required by 42 U.S.C. § 290dd-2 and at its implementing regulations at 42 C.F.R. Part 2, collectively, “Part 2”. Examples include hospitals that employ a dedicated Addiction Medicine Specialist or have a chemical dependency unit. Part 2 imposes more stringent privacy protections than HIPAA on patient identifying information from such programs that would identify a patient either directly or indirectly as having, or having had, a SUD. For such hospitals, the required ADT alerts—even if only the minimum alert content is sent—may trigger application of Part 2 if the “treating practitioner” is a known SUD provider.

Such hospitals may choose to:

- Not send ADT alerts subject to Part 2’s privacy protections
- Suppress the data elements that trigger application of Part 2, such as not sending the treating practitioner’s name
- Obtaining the patient’s Part 2 compliant consent for the disclosure and sending the ADT alert with the required prohibition on redisclosure notice

Hospitals interested in sending ADT alerts that contain Part 2 protected SUD information should carefully consider whether their technology infrastructure can support such alerts.

Arizona’s Health Information Organization (HIO) Law

Arizona is unique in that it is one of only a handful of states with a law that imposes obligations on organizations that provide data exchange services, such as ADT alerts, and healthcare providers, including hospitals, who share data through these organizations. Arizona’s HIO Law defines a HIO to mean “an organization that oversees and governs the exchange of individually identifiable health information among organizations according to nationally recognized standards,” with limited exceptions for healthcare providers, electronic medical records maintained for healthcare providers, health plans, and direct exchange of patient information without a separate organization involved in the exchange.
As a consequence, intermediary organizations that provide the technical and administrative structures for routing ADT alerts may trigger application of the HIO Law. If so, this will require hospitals to demonstrate that its use of the intermediary organization’s system is done in compliance with the HIO Law. The HIO Law uses a patient notice and opt out structure. For instance, the HIO Law provides that:

- The intermediary organization must maintain a Notice of Health Information Practices (“HIO Notice”), which includes, among other things, an explanation of how patients can opt out of participation in the HIO
- Participating healthcare providers must distribute and document distribution of the HIO Notice
- If a patient opts out, the intermediary organization is responsible for ensuring that none of the patient’s health information, including in the form of ADT alerts, is shared with third parties through the HIO within 30 days of the HIO’s receipt of the opt out request
- The intermediary organization must have certain policies, procedures and training in place to ensure compliance with the HIO Law requirements

WHAT HOSPITALS CAN EXPECT FROM SURVEYORS
State Survey Agencies and Accreditation Organizations look to the CoP during audits and/or unannounced “surveys” of hospitals. To determine compliance, surveyors follow the interpretive guidelines that CMS publishes in its State Operations Manual. CMS will be updating its State Operations Manual to add the ADT alert requirements. This should be carefully reviewed when it is released, to ensure that the hospital’s and/or its intermediary’s processes and policies are consistent with what the surveyor will be examining.

CMS’s commentary in the final rule does provide some insights into what surveyors will be examining. As with the survey of the hospital’s total medical records system, surveyors would utilize basic and effective survey procedures and methods such as:

- Review of the organizational structure and policy statements and an interview with the person responsible for the medical records service to first ascertain that the
hospital has a system that meets the initial requirements for patient event notifications in order to determine whether or not the hospital is exempt from the specific patient event notification requirements that follow (i.e., an ADT system that uses HL7® version 2.5.1 or newer messaging standard)

- Review of a sample of active and closed medical records for completeness and accuracy, including any patient event notifications, in accordance with federal and state laws and regulations and hospital policy
- Interview of medical records and other hospital staff, including physicians and other practitioners, to determine understanding of the patient events notification function of the system
- Conducting observations and interviews with medical records staff and leadership to determine if requirements for patient event notifications are being met

Thus, hospitals and any intermediaries that they choose to use should be ready to show documented policies, processes and audit logs that support the hospital’s compliance with the ADT alert requirements and the state and federal health information laws that apply to them.
REFERENCES

• CMS State Operations Manual, when updated to add the ADT alert CoP interpretive guidelines, will be posted on CMS.gov.
• Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule at 45 C.F.R. Parts 160 and 164, as amended.
• 42 C.F.R. Part 2 and new final rule amendments that will be effective on August 14, 2020: 85 Fed. Reg. 42986-43039
• Arizona Health Information Organization statutes, A.R.S. §§ 36-3801 through 3809
• Arizona’s health information confidentiality statutes, A.R.S. §§ 12-2291 through 2297 (medical records), A.R.S. § 12-2291 (genetic testing), A.R.S. § 36-509 (mental health), A.R.S. § 36-664 (communicable diseases)

NOTES

2. The specific regulations are being inserted as: 42 C.F.R. § 482.24(d) (hospitals); 42 C.F.R. § 482.61(f) (psychiatric hospitals); and 42 C.F.R. § 485.638(d) (CAHs).
5. 85 Fed. Reg. at 25600.
8. A.R.S. § 36-3801(5).
ABOUT HEALTH CURRENT
Health Current is a nonprofit organization that serves as Arizona’s statewide HIE. Health Current connects more than 750 organizations, such as hospitals and health systems, ACO/CINs, physician groups, behavioral health and community providers, long-term and post-acute care (PAC) organizations, rural health clinics, labs, emergency medical services, payers, and state and local health agencies. Among other data exchange services, Health Current offers an ADT alert service that is:

- Flexible and customizable
- Compliant with applicable state and federal laws, including Arizona’s HIO Law
- Leverages its established and wide range of connections with Arizona providers (either directly or through providers’ business associates, such as the ACO/CINs)
- Has the capability to send ADT alerts to a patient’s out-of-state providers through its regional and national participation in Patient Centered Data Home™ (PCDH)

Through leveraging existing technical infrastructure between hospitals and the HIE, and expanding capabilities to engage and connect with primary care and post-acute providers, Health Current can help your organization meet the new CMS requirement.

To learn more about our capabilities, contact Peter Steinken, Director of Community Engagement, at peter.steinken@healthcurrent.org or (602) 464-9641.

healthcurrent.org/CMS2021