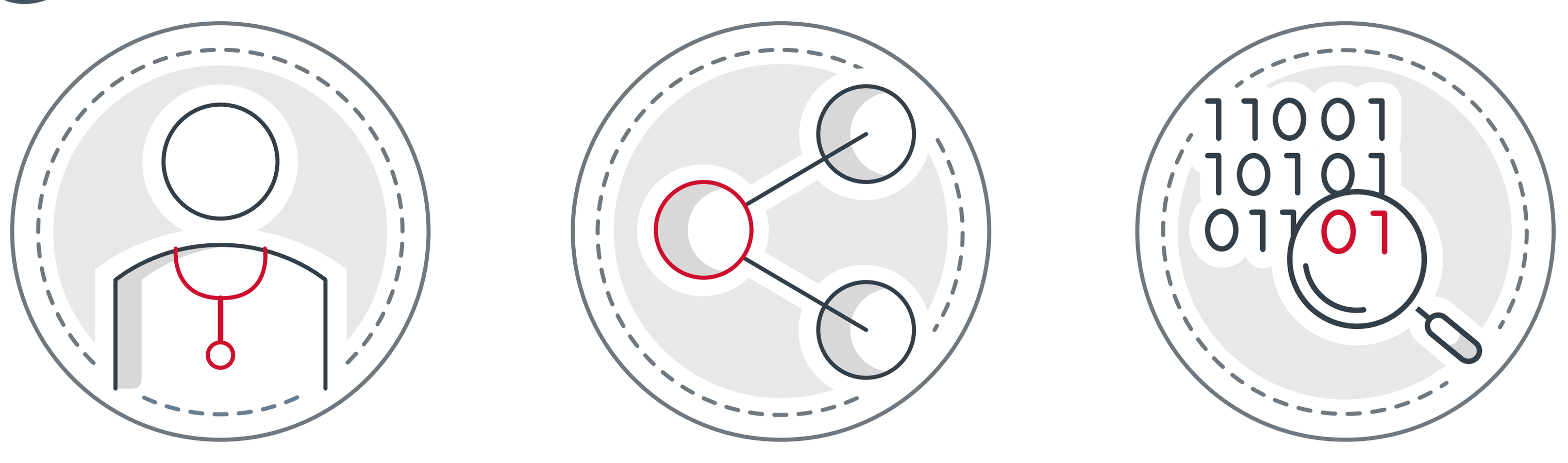
ARE YOU information blocking?

Policymakers have taken action to promote access to electronic health information and discourage information blocking. The Office of the National Coordinator for Health IT (ONC) established policies to hold accountable those who restrict the availability of electronic health information. Compliance with the information blocking prohibition takes effect on **April 5, 2021**.

WHO NEEDS TO PREPARE?

3 ACTORS subject to the information blocking prohibition



PROVIDER

HEALTH INFORMATION EXCHANGE OR NETWORK (HIE/HIN)

INFORMATION TECHNOLOGY DEVELOPER

EXCEPTIONS TO INFORMATION BLOCKING

8 EXCEPTIONS that don't constitute information blocking

ONC defined eight categories of activities that are considered reasonable exceptions to information blocking.

SECURITY
Allows actors to have reasonable practices in place to safeguard against security risks.

PREVENTING HARM
Focuses on physical harm, for example that could result due to incorrect information being exchanged and impacting patient care.

CONTENT AND MANNER
Clarifies certain conditions when there may be a limit to the type of data or the way the data is to provided.

HEALTH IT PERFORMANCE
Recognizes that technology may be unavailable under certain circumstances, for example due to required maintenance or upgrade.

PRIVACY
Protects patient health information when privacy laws and practices are applicable.

INFEASIBILITY
Acknowledges that some circumstances are beyond providers' control and pose a barrier to information access or exchange.

FEES
Permits actors to charge fees, including a reasonable profit margin, for access to data except where otherwise prohibited.

LICENSING
Promotes innovation, allows actors to charge reasonable royalties to license and recoup investments in development and maintenance.

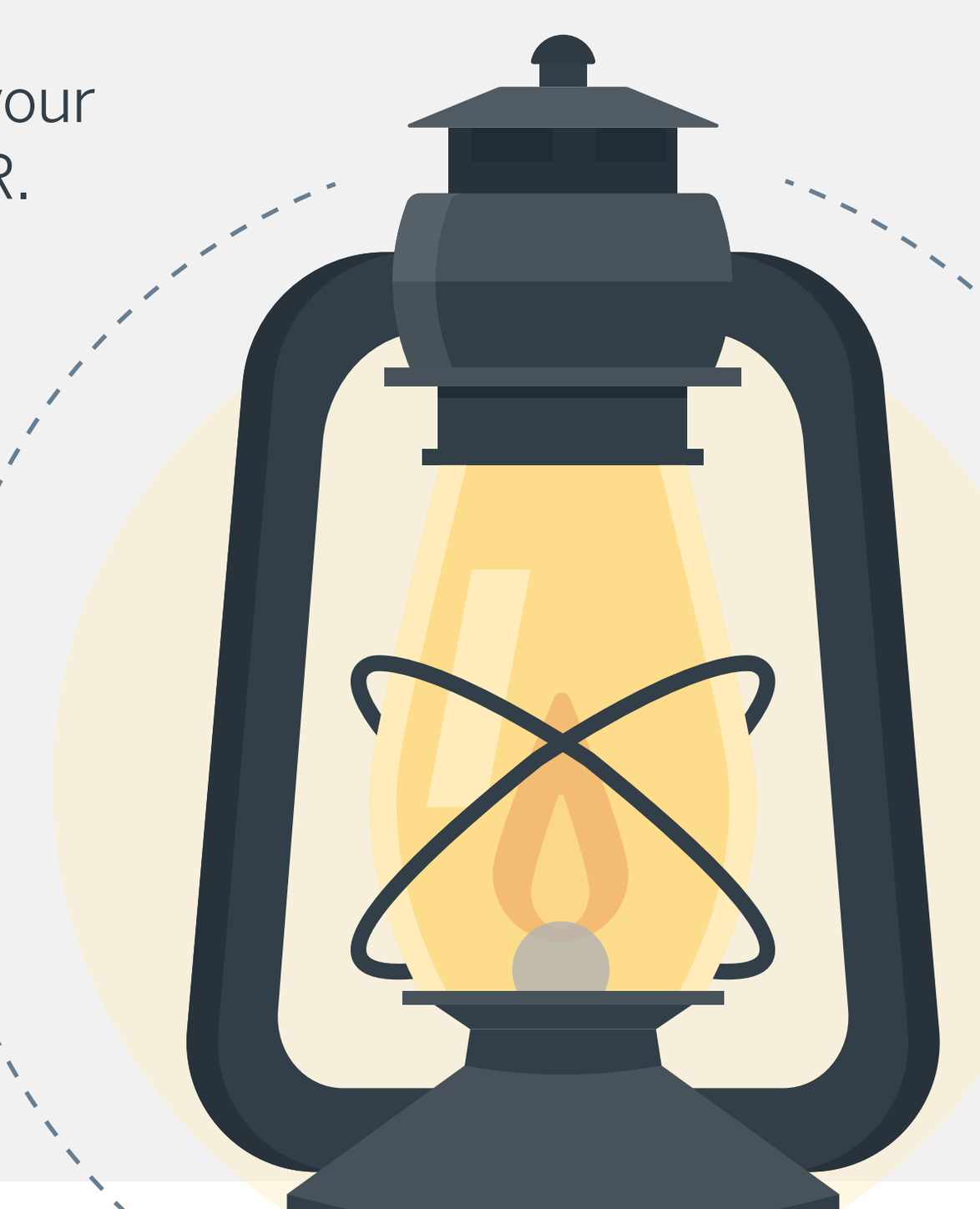
CRITICAL PREPARATIONS

1 ESTABLISH A MULTIDISCIPLINARY COMPLIANCE APPROACH

The information blocking provision impacts everyone in your organization who has a role in making electronic health information available.

Don't assign sole responsibility and accountability to your IT department based on their role in managing your EHR.

Do engage leaders from your compliance, legal, health information management, and patient experience departments. Also involve external partners in care delivery, such as a clinically integrated network or accountable care organization. Seek out various perspectives to support a comprehensive effort for assessing and addressing any potential gaps in information sharing.



2 BUILD AWARENESS AMONG CLINICIANS AND STAFF

Providing education across your organization supports your broader efforts to demonstrate that you are not engaging in information blocking.

Don't miss opportunities to incorporate information blocking education into existing compliance training efforts – for example, along with topics like HIPAA and Stark laws.

Do explain the ways that your organization shares data proactively, and provide instructions on what staff should do if they receive a request for access to electronic health information so that the requester receives a timely response.

3 FOSTER A CULTURE OF DATA ACCESS

Win buy-in from clinicians to support practices that promote data access -- making electronic health information readily available will empower patients to be more engaged with their health care, and minimize circumstances that could be implicated by the information blocking provision.

Don't impose unreasonable restrictions on the availability of electronic health information through your technology, policies, or processes.

Do take a strong stance on sharing electronic health information immediately whenever feasible, and provide timely responses to requests for data access. Check that you're covered under the ONC information blocking exceptions if there are cases where you withhold or delay access.

4 ASSESS POTENTIAL PENALTIES AND DISINCENTIVES

The repercussions for noncompliance with the information blocking provision are different for providers versus an IT developer or HIE/HIN.

Don't overlook that a provider could also be considered an IT developer and HIE/HIN actor.

Do assess whether you could be subject to Office of Inspector General (OIG) civil monetary penalties as an IT developer or HIE/HIN. Also watch for any additional provider disincentives beyond what's required under the CMS Promoting Interoperability (PI) programs.

5 RETAIN DOCUMENTATION TO SUPPORT YOUR APPROACH

You need to be prepared to defend against allegations of information blocking in case you are implicated in an investigation.

Don't underestimate what documentation you may already have available to support your compliance, or that can be repurposed and updated as evidence that you are not engaging in information blocking.

Do collect evidence proactively as you review and update your technology, policies, and processes to get ready for compliance. Revisit your documentation regularly, as your policies and processes evolve along with advances in health IT capabilities.

Advisory Board