2020

OCTOBER 1, 2020

ONC and CMS Final Rules Summary:

Interoperability and Information Blocking

SHB.COM

SHOOK

SHOOK
HARDY & BACON

TABLE OF CONTENTS

Introduction

Aimed at enabling greater patient access and mandating interoperability, recent Final Rules from the Office of the National Coordinator for Health IT ("ONC") and the Centers for Medicare and Medicaid Services ("CMS") have put forth new requirements—which apply to covered entities and certain business associates alike—to reduce information blocking and standardize implementation of multiple Application Programming Interfaces. With the deadlines to implement these requirements quickly approaching, covered entities and applicable business associates need to consider the necessary overhaul of health information technology infrastructure and other protocols to comply with the Rules. This summary provides the purposes behind the Rules, noteworthy insight culled from public comments and responses published in the Federal Register, key requirements of each Rule, and action items for organizations that are responsible for carrying out the new requirements. The detailed action items, coupled with comprehensive coverage requirements of each Rule, provide a framework for covered entities and business associates to begin evaluating their current protocols and determine the fastest path to compliance with the recent ONC and CMS Rules.

Background

- Congress passed the 21st Century Cures Act to govern the access, exchange and use of health information. In addition to providing patients with more access and autonomy over their health information, the Cures Act strives to drive innovation in the health IT space through interoperability standards.
- The Office of the National Coordinator for Health IT put forth the Cures Act Final Rule, which implements provisions from the Cures Act regarding interoperability and information blocking.
- The Centers for Medicare and Medicaid Services also put forth a final rule entitled "CMS Interoperability and Patient Access Final Rule" that aligns with the ONC Rule with respect to interoperability to provide guidance to CMS-regulated payers.

Purpose of ONC Final Rule

- Implement provisions of the 21st Century Cures Act designed to advance interoperability; support the access, exchange and use of EHI; and address occurrences of information blocking
- Re-inject competition into health care markets by lowering barriers to entry and preventing abuses of market power
- Improve access to and quality of information that Americans need to make informed health care decisions
- Identify reasonable and necessary activities that do not constitute information blocking

Purpose of CMS Final Rule

- Advance interoperability and patient access to health information by liberating patient data using CMS authority to regulate Medicare Advantage, Medicaid, CHIP and Qualified Health Plan issuers on Federally-facilitated Exchanges

Requirements – ONC Final Rule[1]

Application Programming Interfaces ("APIs")

KEY TERMS[2]

- **Certified API Developer:** Health IT Developer that creates certified API technology.
- **API Information Source:** Health care organization that deploys certified API Technology.
- **API Users:** Persons or entities that create or use software applications that interact with certified API technology.

ADOPTED STANDARDS

- Adopted **HL7 Fast Healthcare Interoperability Resources (FHIR)** standard and corresponding specifications along with **OpenID Connect Core** standard[3]
- Adopted this standard to advance industry efforts to use the HL7 FHIR 4 standard and provide **patients** more control and **access** to their own health data **"without special effort"**[4]
- Use standardized API to enable access and exchange of information through the use of common technologies, such as smart phones, computers and tablets, and different applications, such as personal health records

KEY CERTIFIED API REQUIREMENTS[5]

- Support two types of API-enabled (i.e., "read" services) services: (1) services for which a **single patient's data** is the focus, and (2) services for which **multiple patients' data are the focus**, that can ultimately be securely used by third-party developers to access EHI
- Support **USDCI**
    - ONC Final Rule replaces Common Clinical Data Set (CCDS) with US Core Data for Interoperability, which defines a standardized set of health data classes and data elements for interoperable health info exchange

---

[1] There are detailed and helpful charts regarding the regulatory dates and compliance and enforcement timelines for the ONC Final Rule. *See* "ONC's Cures Act Final Rule Highlighted Regulatory Dates," https://www.healthit.gov/curesrule/overview/oncs-cures-act-final-rule-highlighted-regulatory-dates (last accessed Sept. 12, 2020); "Cures Act Final Rule Enforcement Discretion Dates and Timeframes," https://www.healthit.gov/cures/sites/default/files/cures/2020-04/Enforcement_Discretion.pdf (last accessed Sept. 12, 2020).

[2] 45 C.F.R. § 170.404(c).

[3] 45 C.F.R. § 170.215.

[4] 45 C.F.R. § 170.404(a)(1).

[5] 45 C.F.R. §§ 170.404(ii), 170.315(g)(10)(iv)-(vi).

- Establish a **secure and trusted connection** with an application requesting patient data according to implementation specifications
- Perform **authentication and authorization** for **API users**
- Issue a **refresh token valid for three months** during the initial connection to access data for a single patient, and through testing, show that the application is able to access single patient and multiple patient data in subsequent connections of applications without the need to re-authorize and re-authenticate when a valid refresh token is supplied
- **Revoke an authorized party's access** to a patient's information at a patient's direction
- **Provide a publicly accessible hyperlink without any additional access requirements** that has a **complete documentation of technical requirements and configurations** for API that allow another application to interact with API, process its responses and include T&C

FEES[6]

- Permitted **to charge API Information Sources** for **development**, **deployment** and **upgrade** of certified API tech and toward **recovering API usage costs**
- Permitted to charge for **value-added services** re: certified API tech, as long as they are not necessary to efficiently and effectively develop and deploy the software that interacts with certified API tech
- **Prohibited** from charging for intangible assets, opportunity costs or costs that led to IP if the actor charged a royalty for IP and that royalty include costs for creating the IP

Information Blocking Rule

ACTORS[7]

- **Healthcare Providers**: The definition of "healthcare provider" in Section 3000 of the Public Health Service Act (instead of the definition of the healthcare provider in the Health Insurance Portability and Accountability Act, or HIPAA). In response to public comments, the ONC stated that the use of this decision provided the Secretary with "discretion to expand the definition to any other category determined to be appropriate by the Secretary."[8]
- **Developers of Certified Health IT**: An individual or entity that develops or offers Certified Health IT. Certified Health includes electronic health record (EHR) systems that meet certain standards adopted by ONC.
- **Health Information Networks and Exchanges (HIN and HIE)**: An individual or entity that determines, controls or has the discretion to administer any requirement, policy or

[6] 45 C.F.R. § 170.404(a)(3).
[7] 45 C.F.R. § 171.102.
[8] *See* 85 Fed. Reg. 25795, https://www.federalregister.gov/d/2020-07419/p-1713.

agreement that permits, enables or requires the use of any technology or services for access, exchange or use of electronic health information (EHI) (1) among more than two unaffiliated individuals or entities, (2) for treatment, payment and healthcare operations purposes as defined by HIPAA.

INFORMATION BLOCKING GENERALLY

- **Information blocking:**[9] a practice (unless required by law or falling under one of the below exceptions) that is likely to **interfere with access**, **exchange or use of electronic health information**; and
    - If conducted by a health information technology **developer**, health information **network** or health information **exchange**, such developer, network or exchange knows, or should know, that such practice is **likely to interfere with**, **prevent or materially discourage access, exchange** or **use** of electronic health information; or
    - If conducted by a **health care provider**, such provider knows that such **practice is unreasonable** and is likely **to interfere with, prevent or materially discourage access, exchange or use** of electronic health information.
- An actor will **not be subject to enforcement actions** under the information blocking provision for civil monetary penalties (CMP) or appropriate disincentives **if the actor's practice** satisfies at least one **exception**. If the practice **does not fall under an exception**, the practice would instead be **evaluated on a case-by-case basis** to assess the specific facts and circumstances to determine whether information blocking has occurred.[10]

INFORMATION BLOCKING EXCEPTIONS[11]

- **Exceptions that involve not fulfilling requests to access, exchange or use EHI**[12]
    - **Preventing Harm Exception**: It will not be information blocking if an actor engages in practices that are **reasonable and necessary to prevent harm to a patient or another person**, provided certain conditions are met:
        - The actor must hold a **reasonable belief** that the practice will **substantially reduce a risk of harm**;
        - The actor's practice must be **no broader** than necessary;

---

[9] 45 C.F.R. § 171.103.

[10] *See* 85 Fed. Reg. 25649, https://www.federalregister.gov/d/2020-07419/p-260.

[11] The description of these exceptions are heavily compiled from the ONC's Fact Sheet regarding Information Blocking Exceptions. *See* "Cures Act Final Rule Information Blocking Exceptions," (https://www.healthit.gov/cures/sites/default/files/cures/2020-03/InformationBlockingExceptions.pdf) (last accessed Sept. 12, 2020).

[12] 45 C.F.R. §§ 171.201-205.

- The actor's practice must satisfy **at least one condition** from each of the following categories: type of risk, type of harm, and implementation basis; and
- The practice must satisfy the condition concerning **a patient's right to request review of an individualized determination of risk of harm.**

- **Privacy Exception**: It will not be information blocking if an actor does not fulfill a request to access, exchange or use EHI in order to **protect an individual's privacy**, provided certain conditions are met:
  - **Precondition not satisfied** (e.g., patient consent or authorization)
  - Health IT developer of certified health IT **not covered by HIPAA**
  - **Denial of an individual's request** for their EHI consistent with 45 CFR 164.524(a) (1) and (2)
  - Respecting an **individual's request not to share** information
- **Security Exception**: It will not be information blocking for an actor to interfere with the access, exchange or use of EHI in order to **protect the security of EHI**, provided certain conditions are met:
  - The practice must either implement a **qualifying organizational security policy** or implement a qualifying security **determination**.
  - The practice must be:
    - Directly related to **safeguarding the confidentiality, integrity and availability** of EHI;
    - Tailored to **specific security risks**; and
    - Implemented in a **consistent and non-discriminatory manner**.

- **Infeasibility Exception**: It will not be information blocking if an actor does not fulfill a request to access, exchange or use EHI due to the **infeasibility of the request**, provided certain conditions are met:
  - The practice must meet one of the following conditions:
    - **Uncontrollable events**: The actor cannot fulfill the request for access, exchange or use of electronic health information due to a natural or human-made disaster, public health emergency, public safety incident, war, terrorist attack, civil insurrection, strike or other labor unrest, telecommunication or internet service interruption, or act of military, civil or regulatory authority.
    - **Segmentation:** The actor cannot fulfill the request for access, exchange or use of EHI because the actor **cannot unambiguously segment** the requested EHI.
    - **Infeasibility under the circumstances**: The actor demonstrates through a **contemporaneous written record or other documentation** its consistent and non-discriminatory consideration of **certain factors** that led to its determination that complying with the request would be infeasible under the circumstances.

- The actor must provide a **written response** to the requestor within **10 business days of receipt of the request** with the reason(s) why the request is infeasible.

- **Health IT Performance Exception:** It will not be information blocking for an actor to take **reasonable and necessary measures to make health IT temporarily unavailable or to degrade the health IT's performance for the benefit of the overall performance of the health IT**, provided certain conditions are met:
  - The practice must:
    - Be implemented for a period of time **no longer than necessary** to achieve the maintenance or improvements for which the **health IT was made unavailable or the health IT's performance degraded**;
    - Be implemented in a **consistent and non-discriminatory manner**; and
    - Meet certain requirements if the unavailability or degradation is initiated by a health IT developer of certified health IT, HIE or HIN.
      - An actor may take action against a **third-party app that is negatively impacting the health IT's performance**, provided that the practice is:
        - For a period of time no longer than necessary to resolve any negative impacts;
        - Implemented in a consistent and non-discriminatory manner; and
        - Consistent with existing **service level agreements**, where applicable.
      - If the unavailability is in response to a risk of harm or security risk, the actor must only comply with the Preventing Harm or Security Exception, as applicable.

- **Exceptions that involve procedures for fulfilling requests to access, exchange or use EHI**[13]
  - **Content and Manner Exception**: It will not be information blocking for an actor to **limit the content of its response** to a request to access, exchange or use EHI or **the manner in which it fulfills a request** to access, exchange or use EHI, provided certain conditions are met.
    - *Content Condition*: Establishes the content an actor must provide in response to a request to access, exchange or use EHI in order to satisfy the exception.
      - Up to **24 months** after the publication date of the Cures Act final rule, an **actor must respond to a request** to access, exchange or use EHI with, at a minimum, the **EHI identified** by the data elements represented in the United States Core Data for Interoperability (**USCDI**) standard.

[13] 45 C.F.R. §§ 171.301-303.

- On and after **24 months** after the publication date of the Cures Act final rule, an actor must respond to a request to access, exchange or use EHI with EHI as defined in § 171.102.

- *Manner Condition*: Establishes the **manner in which an actor must fulfill a request** to access, exchange or use EHI in order to satisfy this exception.
  - An actor may need to fulfill a request in an alternative manner when the actor is:
    - Technically **unable to fulfill the request in any manner requested**; or
    - **Cannot reach agreeable terms** with the requestor to fulfill the request.
  - If an actor fulfills a request in an alternative manner, such **fulfillment must comply with the order of priority** described in the manner condition and must satisfy the Fees Exception and Licensing Exception, as applicable.

- **Fees Exception**: It will not be information blocking for an actor to charge fees, including **fees that result in a reasonable profit margin, for accessing, exchanging or using EHI**, provided certain conditions are met:
  - Meet the basis for fees condition. For instance, the fees an actor charges must:
    - Be based on **objective and verifiable criteria that are uniformly applied** for all similarly situated classes of persons or entities and requests.
    - Be **reasonably related to the actor's costs of providing the type of access, exchange or use of EHI**.
    - **Not be based** on whether the requestor or other person is a **competitor, potential competitor or will be using the EHI in a way that facilitates competition with the actor**.
    - Not be specifically excluded. For instance, the exception does not apply to:
      - **A fee based in any part on the electronic access by an individual**, their personal representative, or another person or entity designated by the individual to access the individual's EHI.
      - **A fee to perform an export of electronic health information** via the capability of health IT certified to § 170.315(b)(10).
  - Comply with Conditions of Certification in § 170.402(a)(4) (Assurances – certification to "EHI Export" criterion) or § 170.404 (API).

- **Licensing Exception**: It will not be information blocking for an actor to **license interoperability elements** for EHI to be accessed, exchanged or used, provided certain conditions are met:

- License negotiation conditions:
  - An actor must begin **license negotiations with the requestor within 10 business days from receipt of the request** and **negotiate a license within 30 business days from receipt of the request**.
  - The licensing conditions:
    - Scope of rights
    - Reasonable royalty
    - Non-discriminatory terms
    - Collateral terms
    - Non-disclosure agreement
  - Additional conditions relating to the provision of interoperability elements.

BUSINESS ASSOCIATE AGREEMENTS[14]

- The information blocking provision is meant to harmonize and work within the current HIPAA Privacy framework.
- Indeed, under the information blocking provision, if an **actor is *permitted* to provide access, exchange or use** of EHI under the HIPAA Privacy Rule, then the **actor must provide that access, exchange or use of EHI** so long as the actor is not prohibited by law from doing so.
- While the information blocking provision **does not require actors to violate BAA agreements**, a **BAA must not be used in a discriminatory manner** by an actor to forbid or limit disclosures that otherwise would be permitted by the Privacy Rule. In other words, the BAA itself cannot be used as a tool to block access or use of EHI.

[14] *See* 85 Fed. Reg. 25812-13, https://www.federalregister.gov/d/2020-07419/p-1900.

Requirements – CMS Final Rule

Application Programming Interfaces

WHO THIS SECTION APPLIES TO[15]

- **CMS-regulated payers**, specifically Medicare Advantage organizations, Medicaid Fee-for-Service (FFS) programs, Medicaid managed care plans, CHIP FFS programs, CHIP managed care entities, and QHP issuers on the FFEs, excluding issuers offering only Stand-alone dental plans (SADPs) and QHP issuers offering coverage in the Federally-facilitated Small Business Health Options Program (FF-SHOP)

CMS REGULATIONS

- CMS-regulated payers need to have two types of APIs: (1) a patient access API, and (2) a provider directory API.
- CMS Final Rule adopts the same API standard as the ONC Final Rule.[16] The response to public comments assured stakeholders that the intent is to remain consistent with the API standards set by ONC.[17]

PATIENT ACCESS API[18]

- Provide similar access to the API "without special effort from the enrollee"[19]
- Implement and maintain a **secure, standards-based (HL7 FHIR Released 4.0.1) API** that allows **patients to easily access their claims and encounter information**, including cost, as well as a defined subset of their clinical information through third-party applications of their choice[20]
- Provide documentation regarding the API functionality and operation[21]
- Make **data regarding adjudicated claims**, including claims data for payment decisions, provider remittances and enrollee cost-sharing, **available no later than one business day** after a claim is processed[22]

---

[15] "Interoperability and Patient Access Fact Sheet," https://www.healthit.gov/cures/sites/default/files/cures/2020-03/InformationBlockingExceptions.pdf (last accessed Sept. 12, 2020).
[16] 42 C.F.R. § 422.119(c).
[17] *See* 85 Fed. Reg. 25520, https://www.federalregister.gov/d/2020-05050/p-169.
[18] 42 C.F.R. §§ 422.119, 431.60, 438.242(b)(5), 457.730, 457.1233(d); 45 C.F.R. § 156.221.
[19] 42 C.F.R. § 422.119(a).
[20] 42 C.F.R. § 422.119(c).
[21] 42 C.F.R. § 422.119(d).
[22] 42 C.F.R. § 422.119(d)(1)(i).

- Make **encounter data and clinical data available no later than one business day** after the data is received by the payer[23]
- **Any data** with a **date of service on or after January 1, 2016**[24]
- Required to **implement** Patient Access API beginning **January 1, 2021**
- Using this API will make claims and encounter information easily accessible for the vast majority of patients enrolled with payers regulated by CMS

PROVIDER DIRECTORY API[25]

- Required to make **provider directory information publicly available** via a standards-based API
- Data must be **updated within 30 business days** of changes to directory info
- Applies to MA organizations, Medicaid and CHIP FFS programs, Medicaid managed care plans and CHIP managed care entities
- Required to implement the Provider Directory API by **January 1, 2021**
- Making this information broadly available in this way will encourage innovation by allowing third-party application developers to access information so they can create services that help patients find providers for care and treatment, as well as help clinicians find other providers for care coordination, in the most user-friendly and intuitive ways possible

Payer-to-Payer Data Exchange[26]

- **Exchange certain patient clinical data (USCDI)** at the **patient's request**, allowing the patient to take their information with them as they move from payer to payer over time to help create a cumulative health record with their current payer
- Applies to CMS-regulated payers noted above with respect to API standards
- Required to implement a process for this data exchange beginning **January 1, 2022**

---

[23] 42 C.F.R. §§ 422.119(d)(1)(ii)-(iii).
[24] 42 C.F.R. § 422.119(h)(i).
[25] 42 C.F.R. § 422.120 for MA organizations, 42 C.F.R. § 431.70 for Medicaid FFS programs, 42 C.F.R. § 438.242(b)(6) for Medicaid managed care plans, 42 C.F.R. § 457.760 for CHIP FFS programs, and 42 C.F.R. § 457.1233(d)(3).
[26] *See* 85 Fed. Reg. 25566, https://www.federalregister.gov/d/2020-05050/p-609; 42 C.F.R. §§ 422.119(f)(1), 438.62(b)(1)(vi), and 156.221(f)(1).

IMPROVING THE DUALLY ELIGIBLE EXPERIENCE BY INCREASING THE FREQUENCY OF FEDERAL-STATE DATA EXCHANGES[27]

- Update requirements for **states to exchange certain enrollee data** for individuals dually eligible for Medicare and Medicaid, including state buy-in files and "MMA files" **from monthly to daily exchange** to improve the dual eligible beneficiary experience
- **Applies to states**
- Required to implement this daily exchange starting **April 1, 2022**

PUBLIC REPORTING AND INFORMATION BLOCKING[28]

- CMS will **publicly report eligible clinicians, hospitals, and critical access hospitals (CAHs)** that may be **information blocking** based on how they **attested to certain Promoting Interoperability Program requirements.**
- Applicable **late 2020**

DIGITAL CONTACT INFORMATION[29]

- CMS will begin **publicly reporting** in late 2020 those **providers** who do **not list or update their digital contact information in the National Plan and Provider Enumeration System (NPPES)**. This includes providing digital contact information such as secure digital endpoints like a Direct Address and/or a FHIR API endpoint.[30]
- Applicable **late 2020**

ADMISSION, DISCHARGE AND TRANSFER EVENT NOTIFICATIONS[31]

- Modify Conditions of Participation (CoPs) to require **hospitals**, including psychiatric hospitals and CAHs, to send **electronic patient event notifications of a patient's admission, discharge and/or transfer** to **another healthcare facility or to another community provider or practitioner**
- Make reasonable efforts to send notifications **immediately prior to or at the time of** events to certain required recipients for treatment, care coordination or quality improvement purposes
- Must meet 5 main requirements:
    - The system's notification capacity is **fully operational** and the hospital uses it **in accordance** with all **applicable** state and federal **statutes and regulations**

---

[27] 42 C.F.R. §§ 406.26, 407.40, and 423.910.
[28] *See* 85 Fed. Reg. 25578, https://www.federalregister.gov/d/2020-05050/p-734.
[29] *See* 85 Fed. Reg. 25581, https://www.federalregister.gov/d/2020-05050/p-767.
[30] *See* 85 Fed. Reg. 25584, https://www.federalregister.gov/d/2020-05050/p-809.
[31] 42 C.F.R. § 482.24(d); 42 C.F.R. § 485.638(d); *see also* 85 Fed. Reg. 25586, https://www.federalregister.gov/d/2020-05050/p-828.

- The system **sends notifications** that include at least **patient name**, treating **practitioner name** and **sending institution name**.
- In accordance with laws and not against the patient's privacy preferences**, the system sends notifications directly, or through an intermediary** that facilitates exchange of health information, **at the time of**:
  - The **patient's registration** in the hospital's emergency department
  - The **patient's admission** to the hospital's inpatient services
- In accordance with laws and not against the patient's privacy preferences, the system **sends notifications directly**, or through an **intermediary** that facilitates exchange of health information, either **immediately prior to, or at the time of**:
  - The patient's **discharge or transfer** from the hospital's **emergency department**
  - The patient's **discharge or transfer** from the hospital's **inpatient** services
- The hospital has made a **reasonable effort** to ensure that the **system sends the notifications** to all applicable **post-acute care services providers and suppliers**, as well as to any of the following **practitioners and entities**, which must receive notification of the patient's status for treatment, care coordination or quality improvement purposes:
  - The patient's established **primary care practitioner**;
  - The patient's established primary care practice group; or
  - Other **practitioner primarily responsible for his or her care**.

- **Applicable** spring 2021

Next Steps

ONC Final Rule – Action Items

- Start directly working with current health IT infrastructure provider to develop a workable API that meets the requirements of the ONC Final Rule.
    - Consider programming the infrastructure to provide a notification to the patient if their information is about to be shared with an outside entity (i.e., the patient is about to use a third-party application) and state that the entity may not be obligated under HIPAA.
    - Ensure or contract for adherence to the HL7 FHIR 4 API standard.
- Take a look at policies regarding EHI exchange to avoid information blocking issues, such as:
    - How requests from healthcare providers are handled (including how decisions to deny access are documented),
    - How current BAAs could be construed as discriminatory within the confines of information blocking,
    - How current agreements regarding sharing of EHI are structured,
    - What and when fees are charged for access to EHI, and
    - How to handle future commercial transactions to avoid information blocking issues.

CMS Final Rule – Action Items

- Payers and Health Plans:
    - Work with current health IT infrastructure provider to implement data exchange requirements by the timelines set by the Rule.
        - Ensure or contract for adherence to the HL7 FHIR 4 API standard.
    - Third-party applications are likely not to be subject to information-blocking rules and are not subject to the CMS Final Rule. Although CMS is advocating for the use of third-party applications to implement and innovate using the required APIs, CMS stated that it does not have the authority to regulate third-party applications and said enforcement lies within the FTC's jurisdiction.[32]
        - Thoroughly vet the third-party applications that may have access to the API,
        - Review and revise agreements with third-party applications,
        - Review and revise privacy policies to disclaim acts by third-party applications.

[32] *See* 85 Fed. Reg. 25517, https://www.federalregister.gov/d/2020-05050/p-135

- Health plans need to educate (through materials or notices) their enrollees about the risks of sending PHI to third-party applications that are not regulated by HIPAA.
- Consider what the hyperlink to privacy and security resources on a public website that includes discussion of third-party apps may look like.

- Hospitals:
  - Review internal ability to provide e-notifications for certain patient events to determine:
    - How, when and what is provided in the notification
    - Which patient events should trigger a notification
  - If using an intermediary to deliver ADT notifications, review agreements regarding EHI exchange
  - Develop a plan for working with providers, such as primary care doctors, to obtain a list of patients associated with the providers in order to disseminate ADT notifications to providers
- Providers:
  - Ensure providers are updated in the NPPES and consider whether information blocking may be applicable (for attestation purposes)
  - Generate patient lists to use for receiving ADT notifications

2020

SHOOK
HARDY & BACON

SHB.COM

HEALTH / SCIENCE / TECHNOLOGY / SHB.COM /

Critical in a crisis, creative in court.®

ATLANTA
BOSTON
CHICAGO
DENVER
HOUSTON
KANSAS CITY
LONDON
LOS ANGELES
MIAMI
ORANGE COUNTY
PHILADELPHIA
SAN FRANCISCO
SEATTLE
TAMPA
WASHINGTON, D.C.

SHOOK