United States Government Accountability Office

Report to Congressional Committees

May 2018

MEDICAL RECORDS

Fees and Challenges Associated with Patients' Access

Accessible Version

GAO-18-386

GAO Highlights

Highlights of GAO-18-386, a report to congressional committees

May 2018

MEDICAL RECORDS

Fees and Challenges Associated with Patients' Access

Why GAO Did This Study

HIPAA and its implementing regulations, as amended by the Health Information Technology for Economic and Clinical Health Act, require health care providers to give patients, upon request, access to their medical records, which contain protected health information (i.e., diagnoses, billing information, medications, and test results). This right of access allows patients to obtain their records or have them forwarded to a person or entity of their choice—such as another provider—in a timely manner while being charged a reasonable, cost-based fee. Third parties, such as a lawyer or someone processing disability claims, may also request copies of a patient's medical records with permission from the patient.

The 21st Century Cures Act included a provision for GAO to study patient access to medical records. Among other things, this report describes (1) what is known about the fees for accessing patients' medical records and (2) challenges identified by patients and providers when patients request access to their medical records. GAO reviewed selected HIPAA requirements and implementing regulations and guidance, and relevant laws in four states selected in part because they established a range of fees associated with obtaining copies of medical records. GAO also interviewed four provider associations, seven vendors that work for providers, six patient advocates, state officials, and Department of Health and Human Services' (HHS) officials. The information GAO obtained and its analysis of laws in the selected states are not generalizable. HHS provided technical comments on this report.

View GAO-18-386. For more information, contact Carolyn L. Yocom at (202) 512-7114 or yocomc@gao.gov.

What GAO Found

Available information suggests that the fees charged for accessing medical records can vary depending on the type of request and the state in which the request is made. Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations, providers are authorized to charge a reasonable, cost-based fee when patients request copies of their medical records or request that their records be forwarded to another provider or entity. In the case of third-party requests, when a patient gives permission for another entity—for example, an attorney—to request copies of the patient's medical records, the fees are not subject to the reasonable cost-based standard and are generally governed by state law. According to stakeholders GAO interviewed, the fees for third-party requests are generally higher than the fees charged to patients and can vary significantly across states.

The four states GAO reviewed have state laws that vary in terms of the fees allowed for patient and third-party requests for medical records. For example, three of the states have per-page fee amounts for patient and third-party records requests. The amounts charged are based on the number of pages requested and vary across the three states.

- One of the three states has established a different per-page fee amount for third-party requests. The other two do not authorize a different fee for patient and third-party requests.
- One of the three states also specifies a maximum allowable fee if the provider uses an electronic health records system. The other two do not differentiate costs for electronic or paper records.

In the fourth state, state law entitles individuals to one free copy of their medical record. The statute allows a charge of up to $1 per page for additional copies. Patient advocates, provider associations, and other stakeholders GAO interviewed identified challenges that patients and providers face when patients request access to their medical records.

- Patients' challenges include incurring what they believe to be high fees when requesting medical records—for example, when facing severe medical issues that have generated a high number of medical records. Additionally, not all patients are aware that they have a right to challenge providers who deny them access to their medical records.
- Providers' challenges include the costs of responding to patient requests for records due to the allocation of staff time and other resources. In addition, according to provider associations and others GAO interviewed, fulfilling requests for medical records has become more complex and challenging for providers, in part because providers may store this information in multiple electronic record systems or in a mix of paper and electronic records.

Contents

Letter 1

Background 4
Available Information Suggests That Fees for Accessing Patient Medical Records Vary by Type of Request and State 8
Stakeholders Identified Fees and Other Challenges for Patients Accessing Medical Records and Challenges for Providers in Allocating Resources to Respond to Requests 13
OCR Investigates Complaints, Audits Providers, and Educates Patients and Providers about Patient Access 19
Agency Comments 25

Appendix I: GAO Contact and Staff Acknowledgments 27

GAO Contact 27
Staff Acknowledgments 27

Appendix II: Accessible Data 28

Data Table 28

Tables

Table 1: Health Insurance Portability and Accountability Act Access Guidance Options for Calculating Reasonable, Cost-Based Fees for Patient and Patient-Directed Requests 9
Table 2: Allowable Fees for Requests for Medical Records in Selected States 11

Figures

Figure 1: Provider and Vendor Process for Fulfilling Medical Record Requests 7
Figure 2: HHS Office for Civil Rights Time to Close Complaints Received between February 2016 and June 2017 21
Accessible Data for Figure 2: HHS Office for Civil Rights Time to Close Complaints Received between February 2016 and June 2017 28

Abbreviations

EHR	electronic health record
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act of 1996
HITECH Act	Health Information Technology for Economic and Clinical Health Act
OCR	Office for Civil Rights
OIG	Office of Inspector General
ONC	Office of the National Coordinator for Health Information Technology
ROI	release-of-information

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

May 14, 2018

The Honorable Lamar Alexander
Chairman
The Honorable Patty Murray
Ranking Member
Committee on Health, Education, Labor, and Pensions
United States Senate

The Honorable Greg Walden
Chairman
The Honorable Frank Pallone Jr.
Ranking Member
Committee on Energy and Commerce
House of Representatives

In the course of seeking or obtaining health care, patients may request and obtain their medical records. They may, for example, want to take their medical records to another health care provider, or use the records to apply for disability coverage or resolve a dispute over insurance coverage.[1] Patients may obtain their records directly in an electronic or paper form or direct one provider to send these records to another provider or entity, such as an insurer or lawyer. In other cases, a third party, such as a lawyer or someone processing disability claims, may directly contact a provider to request access to a patient's medical records with permission from the patient.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended, and its implementing regulations, require HIPAA-covered entities (e.g., providers and insurers) to provide individuals, upon request, with access to their medical records, which contain protected health information (e.g., information on diagnoses, billing, medications, and test results).[2] This right of access allows patients to obtain their medical

[1]For the purposes of this report, we use the term "provider" to refer to physicians, hospitals, and other health care practitioners.

[2]The Health Information Technology for Economic and Clinical Health (HITECH) Act amended HIPAA and its implementing regulations. As relevant here, the HITECH Act specified requirements in the application of the patient access regulation. Pub. L. No. 111-5, § 13405(e), 123 Stat. 115, 268 (2009).

records in a timely manner while being charged a reasonable, cost-based fee. Federal law also states that an individual can direct a provider to send the records to a person of the individual's choice.[3] In 2016, the Department of Health and Human Services' (HHS) Office for Civil Rights (OCR), which is responsible for enforcing the rights established under HIPAA, issued guidance about the right of access. Among other things, the guidance states that when a patient requests that his or her medical records be forwarded to a person or entity, a reasonable, cost-based fee can be charged.

The 21st Century Cures Act included a provision for us to study patient access to medical records and issue a report by June 13, 2018.[4] In this report we describe

1. what is known about the fees charged for accessing patients' medical records,
2. challenges identified by patients and providers when patients request access to their medical records, and
3. efforts by OCR to ensure patients' access to their medical records.

To describe what is known about the fees charged for accessing patients' medical records, we reviewed selected HIPAA requirements and implementing regulations and guidance. We conducted interviews with relevant stakeholders, including representatives from seven release-of-information (ROI) vendors and nine individuals or entities with expertise in HIPAA, including HIPAA lawyers in both private practice and who work in health policy.[5] We selected these stakeholders based on our initial background research, prior work, and input from other stakeholders. During our interviews, we asked about examples of state laws that govern the fees for obtaining copies of medical records. Using this information, we judgmentally selected four states for closer review—Kentucky, Ohio,

[3]Given that this report is about patient access to medical records, in some instances we use the term "patient" to refer to an individual with regard to his or her HIPAA access rights and "provider" to refer to providers who are the relevant HIPAA-covered entities. The Privacy Rule defines "covered entity" as a health plan, a health care clearinghouse, and a health care provider who transmits any health information in electronic form in connection with a transaction covered by the regulations. 45 C.F.R. § 160.103 (2017).

[4]Pub. L. No. 114-255, § 4008, 130 Stat. 1033, 1184-1185 (2016).

[5]ROI vendors gather and release medical records on behalf of providers.

Rhode Island, and Wisconsin. We selected these states based on input from stakeholders, a review of state laws, and because these states have a range of different types of fees. In Ohio, Rhode Island, and Wisconsin, we interviewed officials in the state agencies responsible for oversight of patients' access to medical records. Officials from Kentucky declined an interview but provided written responses to our questions. The information we obtained from stakeholders and our analysis of laws in the selected states are not generalizable.

To describe challenges identified by patients and providers when patients request access to their medical records, we interviewed relevant stakeholders. Specifically, we interviewed individuals or entities with expertise in the topic of patients' access to health information (referred to hereafter as experts), six patient advocates, representatives from four organizations that represent providers (provider representatives), and representatives from seven ROI vendor companies. We judgmentally selected these stakeholders based on our previous studies, presentations at conferences, relevant testimony at Congressional hearings, and recommendations by other interviewees. We also interviewed officials from HHS's OCR, Office of the National Coordinator for Health Information Technology (ONC), and Office of Inspector General (OIG). We obtained specific examples of situations when patients have faced challenges accessing their medical records; these examples were provided to us by OCR and an organization that collects anecdotes from patients about their experiences. The information we obtained from stakeholders is not generalizable.

To describe efforts by OCR to ensure patients' access to their medical records, we reviewed data from OCR on all patient access complaints received between February 2016 and June 2017. We assessed the reliability of these data by (1) performing electronic testing of required data elements, (2) reviewing existing information about the data and the system that produced them, and (3) consulting agency officials who are knowledgeable about the data. We determined that these data were sufficiently reliable for the purposes of our reporting objectives. We also reviewed relevant OCR documentation, including policies and procedures, audit guidelines, and reports on HIPAA violations, as well as 10 examples of patient access complaints provided to us by OCR. Finally, we interviewed officials from OCR and ONC.

We conducted this performance audit from March 2017 to May 2018 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain

sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Medical Record Requests

Patients may request copies of their medical records, or request that copies of their records be sent to a designated person or entity of their choice.

- In a ***patient request***, a patient or former patient requests access to or copies of some or all of her medical records, in either paper or electronic format. For example, a patient might want to keep copies for her own personal use or to bring with her when moving or changing providers.
- In a ***patient-directed request***, a patient or former patient requests that a provider or other covered entity send a copy of the patient's medical records directly to another person or entity, such as another provider. For example, a patient might request that her medical records be forwarded to another provider because the patient is moving or wants to seek a second opinion.
- In a ***third-party request***, a third party, such as an attorney, obtains permission from a patient (via a HIPAA authorization form that is signed by the patient) to access the patient's medical records. For example, with permission from the patient, a lawyer might request copies of a patient's medical records to pursue a malpractice case.[6]

HIPAA

HIPAA's Privacy Rule—the regulations that implement HIPAA's privacy protections—requires that upon request, HIPAA-covered entities, such as

[6]A patient's records may be released by means of a patient-directed request or a third-party request. A key difference between patient, patient-directed, and third-party requests is that in the case of the two types of patient requests, a provider is required to disclose the record, except when an exception applies. In contrast, in a third-party request with a valid HIPAA authorization, the provider is permitted (but not required) to disclose the record.

health care providers and health plans, provide individuals with access to their medical records.[7] Under HIPAA's implementing regulations, providers and other covered entities must respond to a patient or patient-directed request for medical records within 30 days. The Privacy Rule also establishes an individual's right to inspect or obtain a copy of his or her medical records which, as amended in 2013, includes the right to direct a covered entity to transmit a copy of the medical records to a designated person or entity of the individual's choice.[8] Individuals have the right to access their medical records for as long as the information is maintained by a covered entity or by a business associate on behalf of a covered entity, regardless of when the information was created; whether the information is maintained in paper or electronic systems onsite, remotely, or is archived; or where the information originated. Finally, the HIPAA Privacy Rule also describes the circumstances under which protected health information in medical records may be released to patients and third parties.[9]

In February 2016, OCR issued guidance to explain its 2013 regulations.[10] Among other things, this guidance states that as part of a patient's right of access, patients have the right to obtain copies of their medical records

[7]See 45 C.F.R. pt. 164 (2017). Medical records contain protected health information that is kept in designated record sets maintained by the covered entity. The designated record set is defined at 45 CFR §164.501 as a group of records maintained by or for a covered entity that comprises the medical records and billing records about individuals maintained by or for a covered health care provider; enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or other records that are used, in whole or in part, by or for the covered entity to make decisions about individuals.

[8]45 C.F.R. §§ 164.502(a)(1), 164.524(c)(3)(ii) (2017). In 2013, HHS issued a final rule to implement statutory amendments to HIPAA made under the HITECH Act. See 78 Fed. Reg. 5566 (Jan. 25, 2013).

[9]In addition to HIPAA's Privacy Rule, there are several other HIPAA rules related to protected health information and patient medical records. For example, the HIPAA Security Rule establishes national standards to protect electronic health information and requires certain safeguards to ensure the confidentiality, integrity, and availability of such information (see 45 CFR Part 160 and Subparts A and C of Part 164). The HIPAA Breach Notification Rule requires covered entities to notify affected individuals and HHS following a breach of unsecured protected health information (see 45 CFR Part 160 and Subparts A and D of Part 164).

[10]OCR's guidance on individuals' rights under HIPAA to access their health information can be found online. See Department of Health and Human Services, *Individuals' Right under HIPAA to Access Their Health Information 45 CFR § 164.524,* accessed December 21, 2017, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html.

and the right to have their records forwarded to a person or entity of their choice; in these circumstances, patients are only to be charged a "reasonable, cost-based fee."[11] The guidance further notes that state laws that provide individuals with greater rights of access to their medical records are not preempted by HIPAA and still apply. With respect to fees, patients may not be charged more than allowed under the Privacy Rule, even if state law provides for higher or different fees.[12]

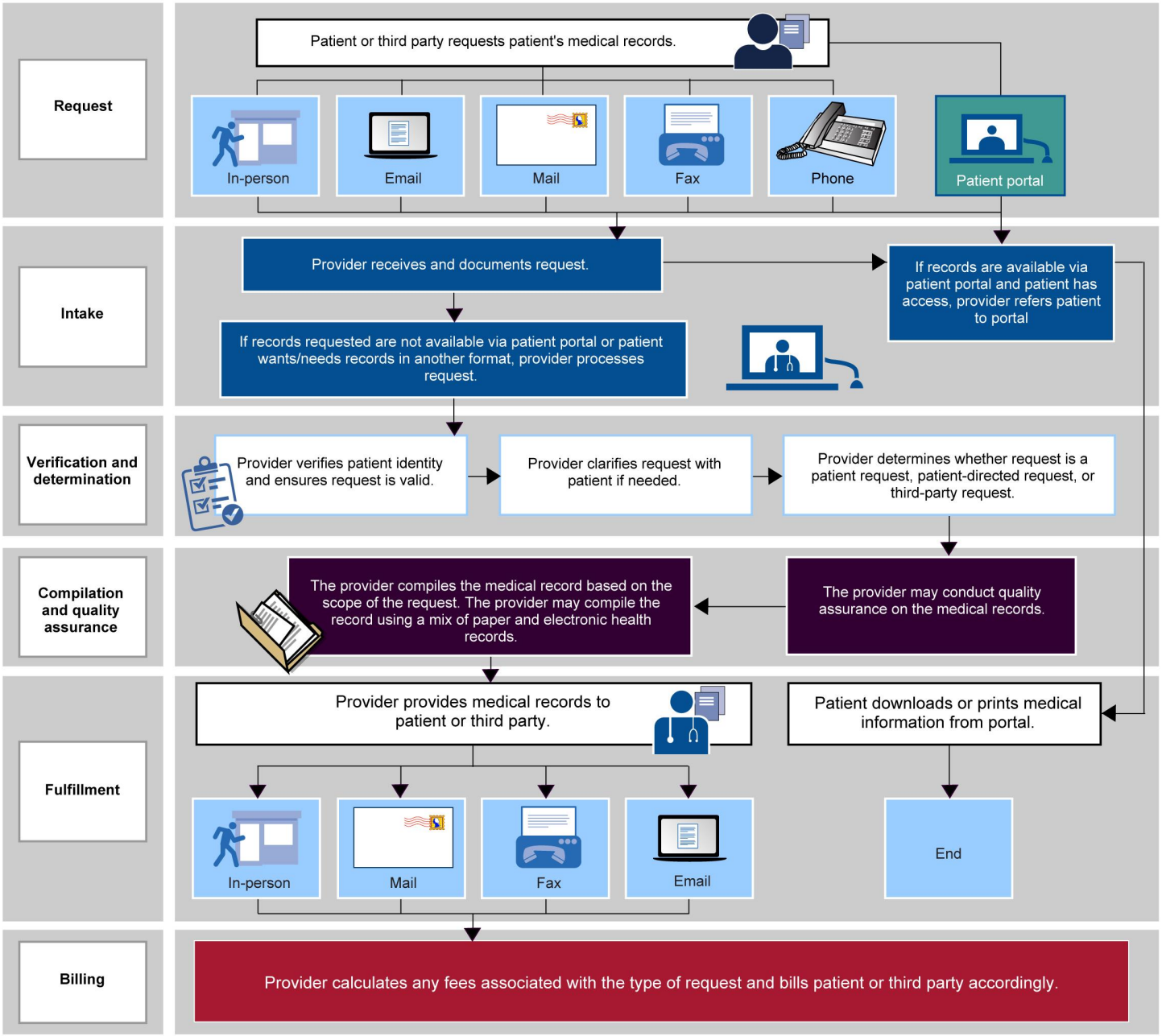
Fulfilling Medical Record Requests

To respond to medical record requests, providers either use staff within their organization or may contract with ROI vendors to conduct this work. In general, both providers' staff and ROI vendors follow the same process when fulfilling requests for medical records for both individual patients and third parties. (See fig. 1.)

[11]45 C.F.R. § 164.524(c)(4) (2017).

[12]In general, state laws that are contrary to the HIPAA Privacy Rule are preempted by HIPAA unless a specific exception applies. One exception is if the state law provides greater privacy rights (including patient access rights) with respect to such information.

Figure 1: Provider and Vendor Process for Fulfilling Medical Record Requests



Source: GAO analysis. | GAO-18-386

Available Information Suggests That Fees for Accessing Patient Medical Records Vary by Type of Request and State

Available information suggests that the allowable fees for accessing medical records vary by type of request—that is, whether a patient or third party is making the request—and by state. Federal laws establish limits on the fees that may be charged for two of the three types of requests for medical records: (1) patient requests, when patients request access to their medical records, and (2) patient-directed requests, when patients request that their records be sent to another person or entity, such as another provider. HIPAA does not establish limits on fees for third-party requests.

For patient and patient-directed requests, providers may charge a "reasonable, cost-based fee" under HIPAA's implementing regulations. OCR's 2016 guidance gives examples of options providers (or a ROI vendor responding to requests for medical records on behalf of a provider) may use in determining a "reasonable cost-based fee."[13] (See table 1.)

[13]On January 8, 2018, Ciox Health, LLC, a ROI vendor, filed suit against HHS regarding the "reasonable, cost-based fee" applicable to patient-directed requests. *Ciox Health, LLC v. Azar*, No. 1:18-cv-0040 (D.D.C. filed Jan. 8, 2018). As of April 2018, no decision had been rendered in this case.

Table 1: Health Insurance Portability and Accountability Act Access Guidance Options for Calculating Reasonable, Cost-Based Fees for Patient and Patient-Directed Requests

Category	Option 1 Actual costs	Option 2 Average costs	Option 3 Flat fee
Method for calculating portion of fee for labor costs	Provider calculates actual labor costs to fulfill the request.	Provider develops a schedule of costs for labor based on average labor costs to fulfill standard types of requests.	A provider may charge individuals a flat fee for all requests for electronic copies of protected health information that is maintained electronically, provided the fee does not exceed $6.50.
Types of labor/materials for which fee applies	Labor for copying (and creating a summary or explanation if the individual requests or agrees), applicable supplies (CD or USB drive), and postage.	Providers may add to the average labor cost amount any applicable supply (e.g., paper, or CD or USB drive) or postage costs.	Charge may not exceed $6.50 and is inclusive of all labor, supplies, and postage.
Types of labor/materials that must be provided free of charge	Review of access request; searching for, retrieving, and otherwise preparing the responsive information for copying; ensuring information relates to the correct individual; segregating, collecting, compiling, and otherwise preparing the response information for copying. Per page fees are not permitted for paper or electronic copies of protected health information maintained electronically.	Review of access request; searching for, retrieving, and otherwise preparing the responsive information for copying; ensuring information relates to the correct individual; segregating, collecting, compiling, and otherwise preparing the response information for copying. Per page fees are not permitted for paper or electronic copies of protected health information maintained electronically.	Review of access request; searching for, retrieving, and otherwise preparing the responsive information for copying; ensuring information relates to the correct individual; segregating, collecting, compiling, and otherwise preparing the response information for copying. Per page fees are not permitted for paper or electronic copies of protected health information maintained electronically.

Source: Department of Health and Human Services' Office for Civil Rights 2016 guidance. | GAO-18-386

In addition to the HIPAA requirements, some states have established their own fee schedules, formulas, or limits on the allowable fees for patient and patient-directed requests. State laws that allow for higher fees than permitted under HIPAA are preempted by the federal law, but those providing for lower fees are not preempted.[14] Representatives from ROI vendors, provider representatives, and other stakeholders we interviewed told us that not all states have established their own requirements governing the fees for medical record requests and, among the states that have, the laws can vary. For example, states can vary as to whether they set a maximum fee that may be charged or whether they establish a fee schedule that is applicable to paper records, electronic records, or

[14]OCR's 2016 access guidance does not establish a fee schedule and does not specify a dollar amount that is to be charged for every request for records. Instead, it describes three permissible methods of calculating the reasonable, cost-based fee permitted by the regulation.

both. While states may establish per-page amounts that can be charged for a copy of a patient's medical records, these per-page amounts can vary.

In contrast with patient and patient-directed requests, the fees for third-party requests are not limited by HIPAA's reasonable, cost-based standard for access requests and are instead governed by state laws, regulations, or other requirements. For third-party requests, providers and vendors working on their behalf may charge whatever is allowed under these state requirements. According to ROI vendors and other stakeholders we interviewed, such fees are typically higher than the reasonable, cost-based fees permitted under HIPAA for patient and patient-directed requests and may be established by formulas that vary by state. For example, states can vary as to whether they establish per-page copy fees, allow providers to charge a flat fee, or charge different fees based on the type of media requested (e.g., electronic copies, X-rays, microfilm, paper, etc.). Additionally, state laws of general applicability (for example, the commercial code) may govern the permissible fees applicable to ROI release of records. Representatives of ROI vendors we interviewed stated that there is significant variation in the state laws that govern the fees for third-party requests, and companies employ staff to track the different frameworks.

Across the four selected states, we found examples of the kinds of variation stakeholders have described in the allowable fees for patient and third-party requests for medical records. (See table 2.)

- Three of the states— Ohio, Rhode Island, and Wisconsin—have established per-page fee amounts. The amounts charged are based on the number of pages requested and vary across the three states. These three states have also established specific fee rates for requesting media such as X-ray or magnetic resonance imaging scan images.
- One state—Ohio—has established a different per-page fee amount for third-party requests. The other three states have not established different fees for different types of requests (i.e., between patient and third-party requests).
- One state—Rhode Island—specifies a maximum allowable fee if the provider uses an electronic health records (EHR) system for patient and patient-directed requests.

- One state—Kentucky—entitles individuals to one free copy of their medical record under state law. The statute allows a charge of up to $1 per page for additional copies of a patient's medical records.

Table 2: Allowable Fees for Requests for Medical Records in Selected States

State and statute	Methods of charging fees for patient and patient-directed requests[a]	Methods of charging fees for third- parties	Does the statute distinguish between paper and electronic records?	Special fees for other types of media	Other allowed fees
Kentucky KY. REV. STAT. § 422.317	Copy of medical record provided without charge.	Copying fee not to exceed $1 per page for second copy upon request by patient, patient's attorney or authorized representative.	Statute does not distinguish between paper and electronic records.	Fees for other media not specified.	Other allowed fees are not explicitly mentioned.
Ohio OHIO REV. CODE § 3701.741	For paper or electronic data, per page fees of $2.74 for pages 1-10, $0.57 for pages 11-50, $0.23 for pages 51 and higher.	Initial fee of $16.84, $1.11 per page for pages 1-10, $0.57 per page for pages 11-50, and $0.23 per page for pages 51 and higher.	Statute refers explicitly to paper or electronic data but does not specify different rates.	$1.87 per page for CAT, MRI, or X-ray images on paper or film (all requests).	Actual cost of postage.
Rhode Island[b] R.I.Gen. Laws § 23-1-48	For electronic records, fee of $0.50 for pages 1-100, $0.25 for pages 101 and higher, with $100 cap. For paper records, $0.50 for pages 1-100 and $0.25 for pages 101 and higher, with no cap.	Same as for patient requests.	Yes, cap of $100 for electronically stored medical records.	Copies of X-rays or films not producible by photocopy shall be provided at actual costs for materials and supplies.	Up to $25 for clerical services (including research handling and data retrieval) for both paper and electronic.[c]
Wisconsin WIS. STAT. §146.83	For paper copies: $1 per page for pages 1-25; $0.75 cents per page for pages 26-50; $0.50 cents per page for pages 51-100; and $0.30 cents per page for pages 101 and higher.	Statute does not explicitly refer to third parties.	Statute does not explicitly refer to the charges for electronic records.	For microfiche or microfilm copies, $1.50 per page. For a print of an X-ray, $10 per image.	Actual shipping costs and applicable taxes.

Source: GAO analysis of state laws. | GAO-18-386

[a]The state statutes do not explicitly refer to patient-directed requests.

[b]Rhode Island enacted a new statutory fee schedule in July 2017 and does not specify a different rate for patient and third-party requests. Prior to enactment of the new statute, the state's fee schedule specified a maximum allowable fee of $127.49 for patient requests but did not establish a maximum

allowable fee for third-party requests. Under the new statute, Rhode Island also allows providers or ROI vendors to charge a $25 clerical and retrieval fee for patient requests (including patient-directed requests) for medical records. However, the Department of Health and Human Services' Office for Civil Rights' 2013 Final Rule and 2016 guidance states that retrieval costs are not permitted under the Privacy Rule and may not be charged to individuals even if authorized by state law.

[c]Other allowable fees in Rhode Island are a special handling fee of $10 if records must be delivered within 48 hours.

In some cases, questions have been raised about the fee structure that should be applied to certain types of requests. Representatives from ROI vendors we interviewed told us that they have seen an increase in third parties (primarily law firms) submitting requests for medical records and indicating that the requests are patient-directed and therefore subject to HIPAA's reasonable, cost-based fee standard.[15] According to these representatives, it is sometimes difficult for them to determine whether it is an attorney making a third-party request or an attorney submitting a patient-directed request because, for example, patient-directed requests are submitted by a patient's attorney and appear similar to traditional third-party requests (e.g., they appear on legal letterhead).[16] As a result, the representatives said that they are often unsure about which fee structure to apply to the request: a reasonable, cost-based fee or a fee for a third-party request, which ROI vendors told us is typically higher.[17]

When asked about the reported distinction between fees for patient-directed and third-party requests, OCR officials told us that they are in the process of considering whether any clarification is needed to their 2016 guidance. This guidance describes the requirements of HIPAA and the Health Information Technology for Economic and Clinical Health (HITECH) Act, as well as their implementing regulations. HIPAA provides patients with a legally enforceable right of access to their medical records.

[15]As noted earlier, in 2013, HHS amended its regulations to state that the patient right of access includes patient-directed requests. In 2016, OCR issued guidance stating that the fee limitations applicable to individual patient requests are also applicable to patient-directed requests.

[16]OCR's guidance states that a covered entity (i.e., a health care provider) may not require an individual to provide a reason for requesting access and that the individual's rationale for requesting access, if voluntarily offered or known by the provider, cannot be used to deny access to the medical records.

[17]Third-party requests must contain a valid HIPAA authorization, the requirements for which are set forth in regulation. 45 C.F.R. § 164.508(c) (2017). Patient directed requests that direct that records to be sent to a third party have fewer requirements than are required in a HIPAA authorization. To direct a copy to a third party, the patient's request must be in writing, signed, and must clearly identify the designated person or entity and the location to which the protected health information should be sent. 45 C.F.R. § 164.524(c)(3)(ii) (2017).

OCR officials explained that the HITECH Act amended HIPAA and specifies that a patient's right of access includes the right to direct a provider to transmit the records directly to an entity or individual designated by the individual.[18] According to OCR officials, the same requirements for providing a medical record to an individual, such as the limits on allowable fees and the format and timeliness requirements, apply to patient-directed requests. OCR officials told us that they are considering whether—and if so, how—they could clarify the 2016 guidance within the constraints of HIPAA and the HITECH Act.

Stakeholders Identified Fees and Other Challenges for Patients Accessing Medical Records and Challenges for Providers in Allocating Resources to Respond to Requests

Patient advocates and others we interviewed described challenges patients face accessing medical records, such as high fees. Provider representatives described challenges providers face, including allocating staff time and other resources to respond to requests for medical records.

[18]Pub. L. No. 111-5, § 13405(e)(1), 123 Stat. 115, 264 (Feb. 7, 2009). The HITECH Act also states that any fee a covered entity may impose shall not be greater than the entity's labor costs.

Patient Advocates and Other Stakeholders Described High Fees for Obtaining Medical Records, While Providers and Patients May Be Unaware of Patients' Access Rights

Multiple stakeholders we interviewed—patient advocates, a provider representative, experts, and a representative from an ROI vendor—told us that some patients have incurred high fees when requesting access to their medical records. Stakeholders noted that in some cases the fees reported by patients appear to exceed the reasonable, cost-based standard established under HIPAA.[19] One patient advocacy organization, which collects information on patients' access to their medical records, described the following examples reported to them by patients:

- Two patients described being charged fees exceeding $500 for a single medical record request.
- One patient was charged $148 for a PDF version of her medical record.
- Two patients were directed to pay an annual subscription fee in order to access their medical records.
- One patient was charged a retrieval fee by a hospital's ROI vendor for a copy of her medical records. Retrieval fees are prohibited under HIPAA.[20]

In addition, according to patient advocates we interviewed, high fees can adversely affect patients' access to their medical records. For example, one patient advocate told us that some patients simply cancel their requests after learning about the potential costs associated with their request. Another patient advocate told us that patients are often unable to

[19]According to an April 2017 article, fees that appear to exceed HIPAA's reasonable, cost-based standard may be driven in part by the existence of state laws that are inconsistent with—and are preempted by—HIPAA's fee limitations. See A.W. Jaspers, J.L. Cox, H.A. Krumholz, "Copy Fees and Limitation of Patients' Access to Their Own Medical Records," *JAMA Internal Medicine*, vol. 177, no. 4 (2017). State laws that provide individuals with greater rights of access to their protected health information than the Privacy Rule, such as those states that require records to be provided free of charge once per year or that are not contrary to the Privacy Rule, are not preempted by HIPAA and thus still apply.

[20]According to one patient advocate with whom we spoke, some ROI vendors do not itemize the fees they charge for access to medical records, which makes it difficult to determine whether the fees are "reasonable."

afford the fees charged for accessing their medical records, even in cases when the fees are allowed under HIPAA or applicable state law. This advocate explained that per-page fees, even if legally authorized, can pose challenges for patients; in particular, patients who have been seriously ill can accumulate medical records that number in the thousands of pages and can, as a result, face fees in excess of $1,000 for a single copy of their records.

Stakeholders we interviewed told us that in many cases, providers may also be unaware of patients' right to access their medical records and the laws governing the fees for doing so.

- Two patient advocates and an expert said that patients are sometimes denied access to their medical records.[21]
- Patient advocates and experts told us that some providers are not aware of the 2016 OCR guidance, which describes patients' rights to access their medical records, as well as the permitted fees for such access.
- One patient advocate and a provider representative also noted that providers may be confused about caregivers' and family members' access to medical records. For example, providers sometimes incorrectly deny family members' access to a patient's health information, which HIPAA allows under certain circumstances.[22]
- Provider representatives, patient advocates, and an expert agreed that providers could benefit from more training on medical record access issues, including training on the options patients have for accessing their medical records.

Stakeholders we interviewed also noted that patients themselves are not always aware of their right to access their medical records, do not always know that they can submit a formal complaint to HHS's OCR when denied access, and could benefit from specific educational efforts that raise awareness of these issues. For example, patient advocates said that the "notice of privacy practices" form that patients receive and are asked to

[21]One stakeholder noted that one reason for denying patients access to their medical records was fear that patients will use the information to sue the provider.

[22]For example, when a family member is involved in the patient's care, the Privacy Rule does not require written consent for a provider to share health information with family members as long as the patient does not object (and other conditions are met). 45 C.F.R. § 164.510 (2017).

sign when they first seek care from a provider could be improved to raise awareness of the rights associated with accessing medical records. This form is used to explain a provider's privacy policies and obligations, and what patients have to do to obtain access to their medical records. However, a provider association and an expert told us that these forms are not always easy for patients to understand, and patients might not always read them. OCR has developed a standard privacy notice that providers may adopt if they choose. However, a patient advocate told us that most providers are still using their own versions of the notice.

Provider Representatives and Other Stakeholders Described Challenges of Allocating Staff Time and Other Resources, While Technology Has Improved Patients' Ability to Access Records

Multiple stakeholders we interviewed told us that responding to patient requests for medical records can be challenging because it requires the allocation of staff and other resources and as a result, responding to such requests can be costly. Furthermore, a provider representative, three representatives from ROI vendors, and a patient advocate confirmed that providers and their staff may lack the expertise needed for responding to requests for medical records in a manner that complies with HIPAA and applicable state laws. Providers can receive training on HIPAA related issues; however, a patient advocate told us that this training, which may be provided by private companies, often focuses on security issues (i.e., maintaining secure medical record systems) and not on the rights of patients.

In addition, stakeholders we interviewed commonly stated that the increased use of electronically stored health information in EHRs has resulted in a more complex and challenging environment when responding to requests for patients' medical records. For example, these stakeholders noted the following:

- Extracting medical records from EHRs is not a simple "push of a button" and often requires providers or their ROI vendors to go through multiple systems to compile the requested information. Stakeholders noted that printing a complete record from an EHR system can result in a document that is hundreds of pages long due to the amount of data stored in EHR systems.

- Representatives from three ROI vendors told us that as providers have transitioned from using paper records to using EHR systems, information has been scanned into electronic medical records. This has, in some cases, resulted in records being incorrectly merged (e.g., the records of two patients merged into a single record). As a result, when responding to a medical record request, providers or their vendors must carefully go through each page of the record to ensure only the correct patient's medical records are being released.
- A provider representative, representatives from four ROI vendors, and two experts noted that providers often have multiple active EHR systems, or have legacy EHR systems in which some medical records are stored. This requires providers and their vendors to go through multiple EHR systems to extract information in response to a medical record request.
- Some providers still have a mix of paper and electronic records, which ROI vendors and provider representatives told us makes responding to medical record requests more difficult and time consuming.
- A provider representative and other stakeholders said that while patients can request copies of their records in an electronic format, providers may have security concerns about sending information via unsecured email or providing electronic information via a patient's USB stick, which increases the risk of a provider's system becoming infected with malware.

While health information technology has created some challenges for providers, numerous stakeholders we interviewed told us that the technologies have made accessing medical records and other information easier and less costly for patients. For example, multiple stakeholders we interviewed told us that an increase in the use of patient portals has reduced the number of patient requests for access to their medical records because patients are able to directly access some health information through the portals.[23] As we have previously reported, patient portals have facilitated patient access to medical records and patients have noted the benefits from having such electronic access, even though

[23]A patient portal is a secure online website that gives patients 24-hour access to their personal health information and medical records anywhere with an Internet connection. Portals are purchased by providers and generally only include health information generated and made available by that individual provider. We have reported on the information providers generally make available via patient portals. See GAO, *Health Information Technology: HHS Should Assess the Effectiveness of Its Efforts to Enhance Patient Access to and Use of Electronic Health Information,* GAO-17-305 (Washington, D.C.: Mar. 15, 2017).

portals do not always contain all the information patients need.[24] The use of patient portals has not eliminated patient requests for access to their medical records; a provider representative we interviewed said that many patients still prefer to obtain paper copies of their records.

[24] *See* GAO-17-305.

OCR Investigates Complaints, Audits Providers, and Educates Patients and Providers about Patient Access

To enforce patients' right of access under HIPAA's Privacy Rule, the HHS OCR undertakes four types of efforts. OCR (1) investigates complaints it receives from patients and others regarding access to patient medical records, (2) audits a sample of providers to determine the extent to which their policies and procedures are compliant with HIPAA, (3) reports to Congress on compliance with HIPAA, and (4) educates patients and providers about patients' rights to access their medical records.

Investigation of Patient Complaints

OCR has established a process for investigating patients' complaints over access to their medical records. Via an online portal on its website, OCR receives complaints submitted by patients.[25] Staff in OCR's headquarters office conduct an initial review of the information provided by the complainant.[26] According to OCR officials, complaints that cannot be immediately resolved are generally assigned to a regional office investigator, who is responsible for reviewing the complaint and obtaining additional information from the complainant and provider, if needed.[27] After the investigator completes the investigation, OCR issues a letter to both the provider and patient explaining what OCR has found. Depending on the nature of the findings, OCR may, for example, issue technical assistance to the provider; close the complaint without identifying a violation; require the provider to implement a corrective action plan; conduct a more detailed investigation; and, if warranted, levy a civil

[25]OCR's online portal is available online. See Department of Health and Human Services Office for Civil Rights, *Complaint Portal,* accessed April 2, 2018, https://ocrportal.hhs.gov/ocr/cp/wizard_cp.jsf

[26]OCR officials noted that if a complainant refuses to sign a release form allowing OCR to speak with the provider in question and obtain the patient's information, OCR does not conduct any investigation. OCR staff stated that patients sometimes refuse to sign such a release form.

[27]OCR comprises nine regional offices.

monetary penalty.[28] According to OCR officials, the use of civil monetary penalties is rare and reserved for situations where providers' behavior is particularly egregious.

Examples of patient access complaints provided to us by OCR included complaints about the following:

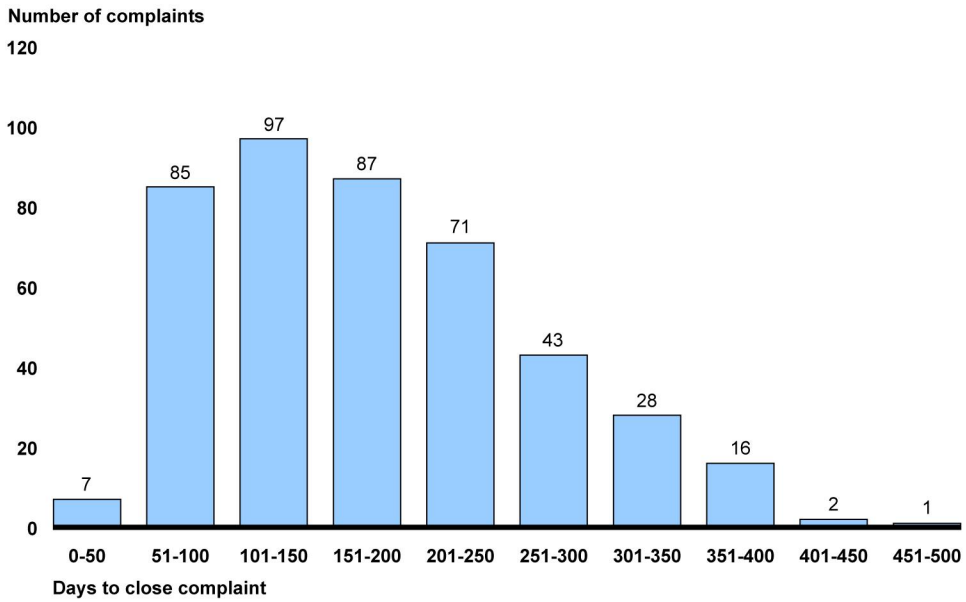
- providers not responding even after the patient made multiple requests, or providers taking longer than 30 days to respond to a request for medical records or other information ;[29]
- providers charging excessive fees for copies of patients' medical records;
- providers not responding to requests from personal representatives or caregivers; and
- providers denying medical records requests from a parent or parents of children.

Our analysis of OCR data also shows that the amount of time OCR takes to investigate and close a patient access complaint varies. OCR received a total of 583 patient access complaints between February 2016 and June 2017, closing 437 of these complaints during that same time period. These 437 complaints took anywhere from 11 to 497 days to close. (See fig. 2.) The majority of these 437 complaints (63 percent) were closed in 200 or fewer days. OCR officials stated that while there is no required time frame for closing a complaint involving patients' access to their medical records, they aim to close cases in fewer than 365 days.

[28]Under HIPAA, OCR has the authority to take enforcement action and impose civil monetary penalties on providers and other covered entities that violate HIPAA. 42 U.S.C. § 1320d-5. As of October 2017, OCR officials confirmed that the agency has levied a civil monetary penalty on one provider for violating the patient right of access under HIPAA.

[29]Under HIPAA's implementing regulations, providers and other covered entities must respond to a patient or patient-directed request for medical records within 30 days. 45 C.F.R. § 164.524(b) (2017).

Figure 2: HHS Office for Civil Rights Time to Close Complaints Received between February 2016 and June 2017



Source: GAO analysis of the Department of Health and Human Services (HHS) Office for Civil Rights data. | GAO-18-386

According to OCR officials, while there is no required time frame for closing a patient access case, investigators aim to get patients access to their medical records as soon as possible, which typically occurs before the case is formally closed (i.e., a formal letter is issued to provider and patient). OCR officials noted a number of reasons why complaints can take a significant amount of time to close. In some cases, the patient receives her records early in the investigation, but the complaint is kept open by OCR to ensure that agreed-upon or recommended corrective actions are taken by the provider—for example, training staff on patient access rights or demonstrating that the provider's policies pertaining to patient access have been changed. In other complaints, time is needed for OCR to obtain consent from the patient who filed the complaint. OCR officials noted that in some instances, patients ultimately decide they do not want to give OCR consent to investigate their complaint, due to concerns that the provider will learn their identity. OCR officials also noted that complaints that are moving towards more serious enforcement actions, such as civil monetary penalties, may also take a long time to close. Finally, OCR officials noted that their own staffing limitations in regional offices can sometimes result in complaints taking additional time to close.

OCR Audits

The HITECH Act requires OCR to conduct periodic audits of selected covered entities in order to review the policies and procedures the covered entities have established to meet HIPAA requirements and standards.[30] The right of patients to access their medical records is included in these requirements. As part of its most recent audit, OCR officials stated that they reviewed 103 covered entities regarding their policies related to patient access to health information, including the entities' notice of privacy practices.[31] In addition, OCR reviewed any access requests the covered entities received from patients, including both requests that were granted and requests that were denied. OCR examined these access requests to determine whether access was provided in a manner that was consistent with the covered entities' policies and procedures and whether the entities fulfilled the requests they received within the 30-day time frame established under the Privacy Rule. OCR also examined any fees that were charged for access and whether those fees met HIPAA's reasonable, cost-based standard. OCR officials said that after completing each audit, OCR submitted a draft report for the audited entity for review. The entity had 10 days to review and submit any feedback to OCR, which OCR reviewed and incorporated into the entity's final audit report. According to OCR officials, OCR has completed this phase of the audit program and will release a final report in 2018.

[30]42 U.S.C. § 17940.

The HITECH Act requires OCR to conduct periodic audits of covered entity and business associate compliance with the HIPAA Privacy, Security, and Breach Notification Rules. In 2011 and 2012, OCR implemented a pilot audit program to assess the controls and processes implemented by 115 covered entities to comply with HIPAA's requirements. Additionally, in 2013, OCR conducted an evaluation of the effectiveness of the pilot program. OCR completed the second phase of the audit program in which it audited covered entities and business associates for compliance with HIPAA rules.

[31]Every covered entity and business associate in the country was eligible to be selected for an audit; however, business associates were not audited on the patient access standard since they are not subject to this provision. To select its 103 covered entities, OCR identified pools of covered entities that represented a range of health care providers and other organizations that are considered covered entities under HIPAA. Sampling criteria for selecting entities to audit included size of entity, type of entity, geographic location, and current enforcement activity with OCR. OCR did not select entities for audit that had an open complaint investigation with OCR or were currently undergoing a compliance review by OCR.

Annual Report to Congress

The HITECH Act directs HHS to submit an annual report to Congress on compliance with HIPAA that includes details about complaints of alleged violations of the Privacy Rule and the resolution of these complaints.[32] The patient right of access is part of the HIPAA and Privacy Rule requirements. The report, which is issued by OCR, includes information on the patient access complaints OCR has received, the number of investigations it has conducted, and the fines OCR has levied. OCR issued its most recent report in 2016. The report summarized complaints and enforcement actions for the 2013 through 2014 calendar years. OCR officials stated that they are in the process of reviewing a draft report that will be released in mid-2018 and contain information and data from calendar years 2015 and 2016.

Provider and Patient Education Efforts

As part of its responsibilities to enforce HIPAA's Privacy Rule, OCR also provides a variety of educational materials that aim to educate both patients and providers about patients' right to access their medical records. These materials include the following:

- In September 2017, OCR published a pamphlet that aims to educate consumers, particularly caregivers, about patients' rights to access their medical records, including how to file a complaint if denied access.[33]

[32]Section 13424(a) of the HITECH Act requires the Secretary of the Department of Health and Human Services to prepare and submit an annual report to Congress regarding compliance with the Privacy and Security Rules promulgated under HIPAA. In addition, Section 13424(a)(2) of the HITECH Act requires that each report be made available to the public on the web site of the Department. OCR submits the reports to Congress every 2 years and posts the reports, as well as submission letters to the applicable Congressional committee. See Department of Health and Human Services, *Report to Congress on Privacy Rule and Security Rule Compliance*, accessed April 4, 2018, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/reports-congress/index.html; and *Reports to Congress on Breach Notification Program*, accessed April 4, 2018, https://www.hhs.gov/hipaa/for-professionals/breach-notification/reports-congress/index.html

[33]This pamphlet and other consumer information can be found online. See Department of Health and Human Services, *Get It. Check It. Use It.*, accessed April 4 2018, https://www.hhs.gov/hipaa/for-individuals/right-to-access/index.html.

- OCR has worked with ONC to produce three videos ("Your Health Information, Your Rights!") and an infographic aimed at educating patients and others about patients' rights to access their medical records.[34]
- OCR has developed provider education videos that aim to educate providers on the rights of patients to access their medical records and how such access can enable patients to be more involved in their own care. Providers can receive continuing education credits for watching these videos.

To assist providers, OCR has worked with ONC to develop a model notice of privacy practices to help providers adequately communicate access rights to patients in a standardized, easy-to-understand way.[35]

Agency Comments

We provided a draft of this report to HHS for review. HHS provided us with technical comments, which we incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees, the Secretary of Health and Human Services, and other interested parties. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you or your staffs have any questions about this report, please contact me at (202) 512-7114 or at yocomc@gao.gov. Contact points for our Office of Congressional Relations and Office of Public Affairs can be found on the last page of this report. Other major contributors to this report are listed in appendix I.

[34]These resources are available online. See Department of Health and Human Services, *Your Rights under HIPAA*, accessed April 4, 2018, https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html.

[35]The model notice can be found online. See Department of Health and Human Services, *Model Notices of Privacy Practices*, accessed January 12, 2018, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/model-notices-privacy-practices/index.html.

Carolyn L. Yocom
Director, Health Care

Appendix I: GAO Contact and Staff Acknowledgments

GAO Contact

Carolyn L. Yocom, (202) 512-7114 or yocomc@gao.gov

Staff Acknowledgments

In addition to the contact named above, Tom Conahan, Assistant Director; Andrea E. Richardson, Analyst-in-Charge; Krister Friday; and Monica Perez-Nelson made key contributions to this report.

Appendix II: Accessible Data

Data Table

Accessible Data for Figure 2: HHS Office for Civil Rights Time to Close Complaints Received between February 2016 and June 2017

Days to close complaints	Number of complaints
0-50	7
51-100	85
101-150	97
151-200	87
201-250	71
251-300	43
301-350	28
351-400	16
401-450	2
451-500	1

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (https://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to https://www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: https://www.gao.gov/fraudnet/fraudnet.htm

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548