

2017年(平成29年)12月14日

藤沢市長 鈴木 恒夫 様

藤沢市個人情報保護制度
運営審議会会長 畠山 関之

診療費等窓口納付金の請求に係るコンピュータ処理について(答申)

2017年(平成29年)11月27日付けで諮問(第900号)された診療費等窓口納付金の請求に係るコンピュータ処理について次のとおり答申します。

1 審議会の結論

藤沢市個人情報の保護に関する条例(平成15年藤沢市条例第7号。以下「条例」という。)第18条の規定によるコンピュータ処理を行うことは適当であると認められる。

2 実施機関の説明要旨

実施機関の説明を総合すると、本事務の実施に当たりコンピュータ処理を行う必要性は、次のとおりである。

(1) 諮問に至った経過

支払不履行・分納不履行となる債務者の発生を未然に防止し、未収金債権の納付率の向上を図るためには、債務者にとって納付しやすい環境を整備し、絶え間ない督促業務を行う必要がある。市民病院では、口座振替の案内や、クレジットカードによる納付、未納通知書兼領収書を用いたゆうちょ銀行・郵便局での収納を可能とし、債務者の利便性の向上に努め、定期的に電話・文書・訪問による督促業務を行っていた。

しかし、長期間にわたり支払不履行・分納不履行の状態が続く債務者は、年々増加傾向にある。このような債務者の特徴として、自身を取り巻く状況が複雑・多様化している方が多く見受けられる。一例ではあるが、多額の診療費を滞納していた患者が亡くなり、患者家族が診療費の負担について争う状態が長期間続き、支払不履行の状態となる事例があった。

こうした状況の中でも納付率を更に高めるため、同規模の病院で行われている対策を参考にし、2017年(平成29年)4月1日、診療費等(患者負担分)に係る未収金債権の回収業務について、一番町綜合法律事務所(以下「法律事務所」という。)と業務委託契約を締結した。(資料1~3)

本業務委託の実施にあたっては、市民病院が法律事務所へ、債権情報について必要最小限度提供し、法律事務所と債務者との間で行われた交渉状況や入金

状況を確認する業務が必要となる。

債権情報を提供する業務にあたっては、回収業務に必要な情報を保存した記録媒体を法律事務所へ貸与することで、コンピュータ処理によらない方法にて対応している。

しかし、記録媒体の貸与により情報提供をしているため、未収金額が貸与時から変動したか確認する作業を電話連絡で行っており、事務処理の効率が非常に悪い状況である。

また、債務者との交渉状況や入金状況を確認する業務では、法律事務所から定期的に送付される報告書等で状況を確認していますが、交渉状況については、情報が随時更新されるため、市民病院と法律事務所との間で把握している情報に齟齬が生じる。現状、債務者から市民病院へ問い合わせがあった場合には、法律事務所に交渉状況を確認してから回答しており、迅速に業務を処理することが困難な状況である。

このことから、迅速かつ確実に効率的な業務を行うため、コンピュータを使用し、法律事務所が回収業務に使用しているクラウドシステム上で、データ伝送・データ共有を行うことに対し、条例第18条の規定に基づき、藤沢市個人情報保護制度運営審議会に諮問するものである。

(2) 提供する債権情報について

患者の診察券番号・氏名・生年月日・性別・住所・住民票の登録地・携帯電話番号・勤務先の名称・勤務先の電話番号、未収金債権整理業務に係る経過記録、受診日、入院日、退院日、診療日別の診療費と調定番号、診療科、最終入金日、委託日までの未収金額

入院費を滞納している患者の場合には、連帯保証人の氏名・年齢・住所・住民票の登録地・連絡先・勤務先の名称・勤務先の電話番号、患者と連帯保証人の関係を、患者が亡くなっている場合には、法定相続人の氏名・生年月日・住所・連絡先を併せて提供する。

(3) 業務委託の必要性について

ア 市民病院における未収金債権の増加は、深刻な状況となっている。平成28年度末時点で、過々年度未収金として41,970,480円を次年度に繰り越しており、7,857,647円を不納欠損として処理するなど、これらは年々増加する傾向にある。

多額の診療費を滞納している債務者に対しては支払交渉を重ね、交渉に応じない債務者に対しては必要に応じて法的措置を行うため、未収担当職員が督促業務に係る法令知識に精通している必要があるが、実際に処理を進める際のノウハウを担当内で集積することが困難な状況である。

このような状況の中、法律事務や交渉業務に秀でている法律事務所へ業務委託することは、納付率の向上に対し、非常に重要な効果を発揮すると考えられる。

イ 市民病院へ連絡する機会がないことを理由とする債務者に対して、積極的な納付交渉を展開することが可能となり、公平負担の理念をさらに推進することができる。

ウ 納付率の向上が見込まれることにより、督促状・催告書の発送件数の減少、滞納整理にかかる事務経費（印刷費・郵便料金等）の削減が想定される。

(4) コンピュータ処理の必要性について

主に次の理由から、債権情報を提供する業務及び交渉状況や入金状況を確認する業務をコンピュータ端末により処理する。

ア 法律事務所へ、回収業務が開始するまでの情報について、最新の状態でデータを伝送・共有することが可能になり、電話連絡等で未収金額の変動を確認するといった事務処理が軽減され、事務効率や業務の確実性が向上するため。

イ 債務者からの支払状況等に関する問い合わせや、滞納整理や督促状の発送などの業務に対応しなければならないことから、迅速かつ効率的に正確な情報を共有する必要があるため。

(5) クラウドシステム導入後の処理の流れについて

クラウドシステム導入後に処理内容が変更となる部分は、資料4のとおりである。

(6) コンピュータ処理の内容について

コンピュータ端末及びクラウドシステム上で行われるコンピュータ処理の内容は、次のとおりである。

ア 債権情報の提供

未収担当職員が、医事課内に設置されているコンピュータ端末を使用し、クラウドシステムに「債権情報入力データフォーマット」(資料5)、入院保証書・支払誓約書をスキャンしたPDFファイル、その他必要資料のデータを伝送する。

イ 委託債権の交渉状況・入金状況の確認

未収担当職員が、クラウドシステム上に保存された、法律事務所と債務者との間で行われた交渉状況や入金状況に係る記録を確認する。

(7) 収納事務の流れについて

回収された未収金債権は、法律事務所が開設した市民病院専用の普通預金口座に入金される。入金時には、法律事務所から市民病院へ、翌営業日中に「入金情報連絡票」(資料6)を添付した電子メールが送付される。回収された未収金債権は、毎月月末に集計され、入金実績報告書(資料7)にて報告があり、翌月の15日以降に市民病院の仮口座に振り込まれる。仮口座への振込みを確認後に、収納管理システム上で入金登録業務を行う。

(8) クラウドシステムの構成について

クラウドシステムは、株式会社セールスフォース・ドットコム(以下「システム運営会社」という。)のシステムを法律事務所独自の仕様に改修したもの(「新未収金奨励システム」という。)を使用する。本システムの構成内容は資料8のとおりである。

(9) 安全対策について

ア 未収担当職員での安全対策

(ア) 物理的対策

データ伝送・確認に使用するコンピュータ端末を、施錠可能な医事課内に設置し、セキュリティーワイヤー等の盗難防止対策を施し、外部へ持ち出しできないようにする。

(イ) 技術的対策

コンピュータ端末にはウイルス対策ソフトを導入し、ソフトウェア及びパターンファイルを最新の状態に保つ。

(ウ) 人的対策

- a クラウドシステムの利用に必要となるユーザーID、パスワードは、未収担当職員2名のみが取り扱うこととし、利用者の制限を設ける。
- b パスワードを定期的に更新する。
- c 個人情報の取扱いについては、「藤沢市コンピュータシステム管理運営規程」及び「藤沢市民病院情報セキュリティポリシー」を遵守し、個人情報の保護及び安全の確保に努めます。

イ 法律事務所での安全対策

(ア) 物理的対策

a データの管理

紙媒体の資料は、鍵のかかるキャビネットで保管している。債権情報は全てクラウドシステムに保存し、執務室内に設置されている各コンピュータ端末から回収業務に係るデータをコピーした記録、印刷した記録をすべてログ管理している。

b データの廃棄

業務委託契約が終了した際には、クラウドシステムに保存された全てのデータを、バックアップデータも含め確実に廃棄し、廃棄したことの証明を提出する。

(イ) 技術的対策

- a コンピュータ端末の使用はID、パスワードで管理しており、定期的に更新している。また、これらの更新記録はログ管理をしている。
- b 各コンピュータ端末のセキュリティは、ウイルス対策ソフトを利用し、最新のウイルスパターンを適用させ、ウイルス対策を施している。
- c 各コンピュータ端末における、メールの送受信の内容はすべて監視している。

(ウ) 人的対策

- a 回収業務を行う執務室への入室は、限られた職員にのみ許可し、入退室はすべてログ管理している。
- b 個人情報の適正な取扱いを確保するため、関係職員に対して必要な研修及び指導を行うとともに、個人情報の適正管理についての点検を行う。

ウ システム運営会社での安全対策

(ア) 技術的対策

a 徹底した情報管理

クラウドシステムに保存されている情報は、データ、データの定義情報、アプリケーションコードの3つのメタデータに分けてデータベース

に保管しており、データベースを閲覧しただけでは情報を確認できない。クラウドシステムに保存されたデータは利用者自身に所有権があるため、システムにログインできる利用者のみが情報を確認することができる。

b アクセス権限の管理

データベースへのアクセス権限は、米国本社の社員のごく一部にのみ許可している。事前に承認を得たデータベースへの処理以外は、実行が禁止され、不正な操作はリアルタイムに検知される仕組みである。また、全ての操作を定期的に記録している。

c 不正ソフトウェア対策

ITに関するサービスを提供している企業やCERTといった外部調査機関からの情報収集、セキュリティパッチの迅速な適用を行い、最新の不正ソフトウェア対策を実施している。

d 脆弱性診断

第三者機関によるアプリケーションに関する診断を年に3回、ネットワークに関する診断を年に4回実施している。指摘を受けた部分については、その都度解決している。

e 利用者認証機能

クラウドシステムを利用するには、ユーザーID、利用者が設定可能なパスワードを設定するだけでなく、使用するコンピュータ端末のIPアドレスをシステム運営会社に登録する必要があり、不正アクセスを防止できる仕組みである。また、不正利用を防ぐため、一定時間操作がない場合にはセッションを切るといった管理機能や、シングルサインオン機能がクラウドシステムに備わっている。

f ログイン履歴管理

過去6ヶ月間のログイン履歴を保管しており、必要に応じて、ログインの成功・失敗の記録、失敗した理由、アクセス元のIPアドレス、ブラウザ等の情報をCSVファイルで利用者が取得することが可能である。

g 暗号化通信

利用者がクラウドシステムにアクセスする際に使用する通信方法は、TLS/SSLによる暗号化通信に対応している。暗号化通信を利用することで、第三者によるデータの盗用や改ざんを防止することができる。また、データセンターからバックアップデータセンターへデータを送信する際には、システム運営会社専用の回線による通信を行う。

h その他

システム運営会社は、ISO27001、ISO27018を取得しており、Pマーク制度の認定も受けている。また、内部統制の有効性について証明するSSAE16SOC-1、2、3レポートを取得している。

(1) 人的対策

a オペレーションセンターによる監視・遠隔操作

4箇所に設けられたオペレーションサービスセンターから、24時間365日にわたり、データセンターの監視、システム管理の遠隔操作を行

う。

b 防犯対策

データセンター外観には看板や標識を設置しておらず、匿名性を確保している。また、24時間365日にわたり有人監視、防犯カメラによる監視を行い、全ての出入り口に無音アラームと警察への自動通知機能を設置している。

c 不正侵入対策

生体認証によるなりすまし防止設備、共連れやなだれ込み防止設備など、複数段階の認証を行い、データセンターの安全性を維持する。

(ウ) 物理的対策

a 震災対策

データセンターは免震設計となっており、年1回以上の頻度で防災訓練を行っています。また、火災に対する対応として、火災予兆検知システム、消火システムを設置している。

b 停電対策

無停電電源装置（UPS）及びガスタービン方式による非常用発電機にて電力供給を行うことが可能である。構成も冗長構成（N+1）をとり、最低48時間稼働分の燃料をデータセンター敷地内に備蓄している。

(10) 実施予定時期

2018年（平成30年）4月から実施予定である。

(11) 添付資料

資料1 藤沢市民病院医業未収金回収業務委託仕様書

資料2 業務委託契約書

資料3 現行の処理の流れ

資料4 クラウドシステム導入後の処理の流れ

資料5 債権情報入力データフォーマット

資料6 入金情報連絡票

資料7 入金実績報告書

資料8 クラウドシステム構成図

資料9 個人情報取扱事務届出書

3 審議会の判断理由

当審議会は、コンピュータ処理を行うことについて、次に述べる理由により、審議会の結論のとおり判断をするものである。

(1) コンピュータ処理を行う必要性について

実施機関では、コンピュータ処理を行う必要性について、次のように述べている。

債権情報を提供する業務及び交渉状況や入金状況を確認する業務について、次の理由によりコンピュータ端末により処理する必要がある。

(ア) 法律事務所へ、回収業務が開始するまでの情報について、最新の状態でデータを伝送・共有することが可能になり、電話連絡等で未収金額の変動

を確認するといった事務処理が軽減され、事務効率や業務の確実性が向上するため。

- (1) 債務者からの支払状況等に関する問い合わせや、滞納整理や督促状の発送などの業務に対応しなければならないことから、迅速かつ効率的に正確な情報を共有する必要があるため。

以上のことから判断すると、コンピュータ処理を行う必要性があると認められる。

(2) 安全対策について

実施機関が2 説明要旨(9)ア(ア)から(ウ)まで、イ(ア)から(ウ)まで及びウ(ア)から(ウ)までにおいて示す安全対策は、次のとおりである。

ア 実施機関における安全対策

(ア) コンピュータウイルスによるデータの破壊を防止するための措置するための措置 ア(イ)

(イ) 必要最小限の担当者以外の者がデータにアクセスできないようにするための措置 ア(ウ) a 及び b

(ウ) 日常的な安全対策 ア(ア) 及び(ウ) c

イ 法律事務所における安全対策

(ア) コンピュータウイルスによるデータの破壊を防止するための措置するための措置 イ(イ) b

(イ) 必要最小限の担当者以外の者がデータにアクセスできないようにするための措置 イ(イ) a 及び(ウ) a

(ウ) 日常的な安全対策 イ(ア) a 及び(ウ) b

(エ) ネットワークからの情報流出を防止するための措置 イ(イ) c

(オ) 利用後にデータを確実に消去するための措置 イ(ア) b

ウ システム運営会社における安全対策

(ア) コンピュータウイルスによるデータの破壊を防止するための措置するための措置 ウ(ア) c 及び d

(イ) 必要最小限の担当者以外の者がデータにアクセスできないようにするための措置 ウ(ア) a , b 及び f

(ウ) 日常的な安全対策 ウ(ア) h , (イ) a , b 及び c 並びに(ウ) a 及び b

(エ) ネットワークからの情報流出を防止するための措置 ウ(ア) g

(オ) 利用後にデータを確実に消去するための措置

(カ) ネットワークへの不正アクセスを防止するための措置 ウ(ア) e

以上のことから判断すると、安全対策上の措置が施されていると認められる。

以上に述べたところにより、コンピュータ処理を行うことは適当であると認められる。

以 上