御堂筋監査法人ニュースレター　September 2020

医療法人のシステム管理～アクセス管理編

公認会計士　森 康友
平成 25 年に税理士法人日本経営に入社し、医療・介護分野における会計・税務業務に従事、決算業務や申告業務、特定医療法人成りなど医療法人における様々な分野に精通。現在、御堂筋監査法人において、主に医療法人の監査業務を担当。

医療法人では、電子カルテをはじめ、多くのシステムを利用しており、また扱っている情報も患者情報等の機密性の高いものです。このため、適切な管理が必要となりますが、実施できている医療法人は少ないのが現状です。そこで、今回は我々が監査を行う中でよく発見される管理上の問題のうち、システムへのアクセスに関する項目を解説したいと思います。

問題1. パスワード管理について

医療情報システムの安全管理に関するガイドラインにおいて、ログイン時のパスワードの変更については、最長でも 2 ヶ月以内と規定されており、診療録管理体制加算は当該ガイドラインの準拠が要件とされています。

しかし、医療情報システムや人事給与システム等のパスワード管理について、定期的に変更を行っていないケースや定期的に変更しているものの、半年に 1 回や 3 ヶ月に 1 回等の規定を設けているケースが多く見られます。

長期間同じパスワードを使用している場合、当該パスワードが外部へ流出するリスクが高まり、結果、患者情報等の機密情報が漏洩するリスクが高まります。

情報漏洩の防止やガイドラインの準拠の観点からパスワード変更期間の見直しが望まれます。

そのうえで、パスワードを変更しなければ、変更期限以降はシステムへログインできなくする、あるいは変更を促す通知がログイン毎に届く等の設定を行い、運用上も実施されるような仕組みを構築することが望まれます。

法人の管理規定上はパスワードを定期的に変更するとされているものの、運用上は実施されていないケースも見られますので、管理規程が実際に運用される仕組みも必要です。

問題2. ID管理について

医療情報システムや人事給与システム等へのログインの際に用いられるＩＤについて、法人や部署で共有されているケースが多くみられます。

ＩＤを個人ごとに設定することは、情報の入力や修正、承認等を行うことができる権限を有する者を限定するとともに、ログイン履歴を確認することにより、システムへ誰がいつアクセスしたのかを把握することが出来ます。このため、システムへのアクセス管理が可能となります。

システム内には患者情報や人事給与情報といった機密情報が保管されているため、システムへのアクセスは厳格に管理することが望まれます。

また、ＩＤを個人ごとに設定しているものの、退職者等により使用されなくなったＩＤが削除されることなく残っているケースも散見されます。

ＩＤが削除されることなく残っている場合、既に部外者となった元職員によるシステムへのアクセスが可能となり、不正な情報の改竄や情報の漏洩といったリスクが高まります。

退職者のＩＤは一定期間内に削除するとともに、定期的に登録ＩＤの確認を行う等、ＩＤの適切な管理が望まれます。

問題3. 外部媒体のアクセスについて

医療情報システムや人事給与システム等への外部媒体（主にＵＳＢメモリ）によるアクセスが何ら制限されていないケースが見られます。

外部媒体によるアクセスが可能となっている場合、システムに保管されている情報を不正に外部へ持ち出される可能性が高まります。

情報漏洩の防止の観点から、個人のＵＳＢメモリの使用を禁止するとともに、法人内で利用されず放置されているＵＳＢメモリを回収する等の対策を行い、システムへアクセスできる媒体を限定することが望まれます。次いで、アクセスを可能とする媒体については、パスワードロック機能とウイルスチェック機能を搭載したものにする等セキュリティを強化することが望まれます。

アクセスできる媒体を限定しているにも関わらず、その媒体に対するセキュリティが不十部なケースも見みられます。当該媒体については、システムと同水準のセキュリティを設けることが必要です。