Gelet op de wet van 12 juli 2016 houdende de eerste aanpassing van de algemene uitgavenbegroting voor het begrotingsjaar 2016, inzonderheid op de justitiebegroting programma 59/3;

Gelet op het koninklijk besluit van 26 april 1968 tot inrichting en coördinatie van de controles op de toekenning en op de aanwending van de toelagen;

Gelet op het koninklijk besluit van 20 november 2008 houdende regeling inzake de subsidiëring van de vereniging zonder winstoogmerk "Boeddhistische Unie van België" – "Union Bouddhique Belge", artikel 12;

Gelet op het ministerieel besluit van 20 november 2008 tot uitvoering van het koninklijk besluit houdende regeling inzake de subsidiëring van de vereniging zonder winstoogmerk "Boeddhistische Unie van België" – "Union Bouddhique Belge".

Gelet op het ministerieel besluit van 22 februari 2016 betreffende de toelage aan de Boeddhistische Unie van België voor het dienstjaar 2016;

Gelet op de begroting van de Boeddhistische Unie van Belgïe voor het dienstjaar 2016;

Gelet op de begrotingswijziging van de Boeddhistische Unie van Belgïe voor het dienstjaar 2016;

Gelet op het advies van de Inspecteur van Financiën van 8 november 2016,

Besluit :

Artikel 1. Artikel 2 van het ministerieel besluit van 22 februari 2016 betreffende de toelage toegekend aan de Boeddhistische Unie van België voor het dienstjaar 2016 wordt vervangen door de volgende bepaling :

« Art. 2. Deze som zal volgens de volgende modaliteiten toegewezen worden :

- Werkingskosten en huren en huurlasten	41.202,37 EUR;
- Personeel	22.847,63 EUR;
- Bankkosten	750,00 EUR;
- Investeringen	200,00 EUR ».

Art. 2. Artikel 3 van hetzelfde besluit wordt vervangen door de volgende bepaling :

"Art. 3. De schijf van 10 % van het subsidiebedrag wordt uitbetaald nadat de rekeningen van het jaar 2016 alsook het verslag van een door het Instituut van de Bedrijfsrevisoren erkende bedrijfsrevisor zijn overgezonden. De FOD Justitie voert voor de definitieve uitbetaling een controle uit op deze documenten.

Alle stukken dienen te zijn ondertekend door alle statutair daartoe toegelaten personen.

Indien de sociale bijdragen en de belastingen niet zouden worden betaald dan zullen deze sommen onmiddellijk terugvorderbaar zijn.

De Boeddhistische Unie van Belgïe wordt hoofdzakelijk gesubsidieerd door de FOD Justitie, het is ertoe verplicht de wetgeving inzake overheidsopdrachten na te leven.

Elke niet-verantwoorde subsidie moet worden terugbetaald.

Art. 3. Dit besluit heeft uitwerking met ingang van 1 januari 2016.

Brussel, 6 december 2016.

K. GEENS

Vu la loi du 12 juillet 2016 contenant le premier ajustement du budget général des dépenses pour l'année budgétaire 2016 notamment le budget Justice programme 59/3;

Vu l'arrêté royal du 26 avril 1968 réglant l'organisation et la coordination des contrôles de l'octroi et de l'emploi des subventions;

Vu l'arrêté royal du 20 novembre 2008 portant réglementation relative à l'octroi de subsides à l'association sans but lucratif « Union Bouddhique Belge » - « Boeddhistische Unie van België », article 12;

Vu l'arrêté ministériel du 20 novembre 2008 portant exécution de l'arrêté royal portant réglementation relative à l'octroi de subsides à l'association sans but lucratif « Union Bouddhique Belge » - « Boeddhistische Unie van België » .

Vu l'arrêté ministériel du 22 février 2016 relatif au subside à l'Union Bouddhique Belge pour l'exercice 2016;

Vu le budget de l'Union Bouddhique belge pour l'année 2016;

Vu la modification budgétaire de l'Union Bouddhique belge pour l'exercice 2016;

Vu l'avis de l'Inspecteur des Finances du 8 novembre 2016,

Arrête :

Article 1er. L'article 2 de l'arrêté ministériel du 22 février 2016 relatif au subside octroyé à l'Union Bouddhique Belge pour l'exercice 2016 est remplacé par la disposition suivante :

"Art. 2. Cette somme est attribuée selon les modalités suivantes :

- Frais de fonctionnement et loyers et charges	41.202,37 euros;
- Personnel	22.847,63 euros;
- Frais bancaires	750,00 euros;
- Investissements	200,00 euros ».

Art. 2. L'article 3 du même arrêté est remplacé par la disposition suivante :

« Art. 3. La tranche de 10 % du subside est mise en paiement après communication des comptes de l'année 2016 et du rapport d'un réviseur d'entreprise agréé par l'Institut national des Réviseurs d'entreprises. Un contrôle est effectué sur ces documents par le SPF Justice avant la mise en paiement définitive.

Toutes les pièces doivent être soussignées par toutes les personnes statutairement autorisées.

Au cas où les charges sociales et les impôts ne seraient pas payés, ces sommes deviennent remboursables sans délai.

L'Union Bouddhique Belge, est principalement subventionné par le SPF Justice, il a l'obligation de respecter la législation sur les marchés publics.

Toute subvention non justifiée fera l'objet d'un remboursement.

Art. 3. Le présent arrêté produit ses effets le 1er janvier 2016.

Bruxelles, le 6 décembre 2016.

K. GEENS

RIJKSINSTITUUT VOOR ZIEKTE- EN INVALIDITEITSVERZEKERING

[C − 2016/22478]

5 DECEMBER 2016. — Verordening betreffende het elektronisch voorschrift binnen het ziekenhuis

Het Comité van de verzekering voor geneeskundige verzorging van het Rijksinstituut voor Ziekte- en Invaliditeitsverzekering,

Gelet op de wet betreffende de verplichte verzekering voor geneeskundige verzorging en uitkeringen, gecoördineerd op 14 juli 1994, artikelen 9*bis* en 22, 11°;

Gelet op het advies van de Nationale Commissie tandartsen-ziekenfondsen van 23 november 2016;

Gelet op het advies van de Nationale Commissie artsen-ziekenfondsen van 28 november 2016;

INSTITUT NATIONAL D'ASSURANCE MALADIE-INVALIDITE

[C − 2016/22478]

5 DECEMBRE 2016. — Règlement relatif à la prescription électronique intra hospitalière

Le Comité de l'assurance soins de santé de l'Institut national d'assurance maladie-invalidité,

Vu la loi relative à l'assurance obligatoire soins de santé et indemnités, coordonnée le 14 juillet 1994, les article 9*bis* et 22, 11°;

Vu l'avis de la Commission Nationale dento-mutualiste du 23 novembre 2016;

Vu l'avis de la Commission Nationale médico-mutualiste du 28 novembre 2016;

Na erover te hebben beraadslaagd in zijn vergadering van 5 december 2016;

Besluit :

Artikel 1. De elektronische voorschriften opgesteld overeenkomstig het protocol in bijlage kunnen hun papieren equivalent vervangen.

Art. 2. De huidige verordening treedt in werking de dag waarop het in het *Belgisch Staatsblad* wordt bekend gemaakt.

Brussel, 5 december 2016.

De Leidend Ambtenaar, De Voorzitter,

H. De Ridder. J. Verstraeten.

Bijlage bij de verordening van 5 december 2016 betreffende het elektronisch voorschrift binnen het ziekenhuis

Protocol gesloten tussen de verzekeringsinstellingen en de akkoorden- of overeenkomstencommissies betreffende het elektronisch ziekenhuisvoorschrift.

Gelet op de artikelen 9*bis* en 22, 11°, van de gecoördineerde wet van 14 juli 1994 betreffende de verplichte verzekering voor geneeskundige verzorging en uitkeringen;

Gelet op het artikel 36/1 van de wet van 21 augustus 2008 houdende oprichting en organisatie van het eHealth-platform en diverse bepalingen,

Artikel 1. Het huidig protocol is van toepassing op de ziekenhuisvoorschriften voorzien door of krachtens de gecoördineerde wet van 10 mei 2015 betreffende de uitoefening van de gezondheidszorgberoepen en/of door of krachtens de gecoördineerde wet van 14 juli 1994 betreffende de verplichte verzekering voor geneeskundige verzorging en uitkeringen.

Onder ziekenhuisvoorschrift wordt verstaan een voorschrift van een bevoegde zorgverlener verbonden aan het ziekenhuis met betrekking tot een patiënt van het ziekenhuis (ambulant of gehospitaliseerd) en uitgevoerd in een van de diensten van het ziekenhuis

Artikel 2. Elk elektronische ziekenhuisvoorschrift moet de voorwaarden betreffende de bewijswaarde vastgesteld door het artikel 36/1 van de wet van 21 augustus 2008 houdende oprichting en organisatie van het eHealth-platform en diverse bepalingen respecteren.

Het moet eveneens alle wettelijk of reglementaire vereiste vermeldingen voor het papieren voorschrift dat het vervangt, bevatten.

Artikel 3. Het ziekenhuis legt de nodige procedures vast om een correcte identificatie van de voorschrijver te garanderen. Hierbij wordt voorzien in één van de volgende procedures :

— Authenticatie door middel van gebruikersnaam en paswoord.

De gebruikersnaam en het paswoord zijn strikt persoonlijk en niet overdraagbaar. Het paswoord kan eenmalig of meermaals gebruikt worden. Indien het paswoord meermaals kan worden gebruikt, dient de voorschrijver het paswoord zo snel mogelijk na ontvangst en in elk geval bij het eerste gebruik ervan te wijzigen.

Indien het paswoord meermaals gebruikt kan worden, dient de voorschrijver nadien dit paswoord op regelmatige tijdstippen te wijzigen. De procedures van regelmatig wijzigen van paswoorden moeten verplicht en uitgevoerd worden door het ziekenhuis.

Een veilig paswoord is idealiter samengesteld uit 15 tekens en minstens uit 8 tekens. Een paswoord kan hetzij eenmalig worden gebruikt doordat het bij elk gebruik wordt berekend op basis van een "challenge" (dynamisch paswoord), hetzij meermaals gebruikt worden (statisch paswoord).

Een paswoord dat meermaals gebruikt kan worden, bevat alfanumerieke karakters en symbolen, geplaatst in een volgorde die niet makkelijk kan worden geraden. Elke voorschrijver dient ervoor te zorgen dat het gekozen paswoord voldoet aan deze eisen. Elke voorschrijver is zelf aansprakelijk in de gevallen waarin een paswoord wordt achterhaald en/of misbruikt.

Elke voorschrijver dient zorgvuldig om te gaan met zijn gebruikersnaam en paswoord en is tot geheimhouding ervan gehouden. Elke voorschrijver is aansprakelijk voor elk al dan niet geoorloofd gebruik ervan, met inbegrip van elk gebruik door derden.

Après en avoir délibéré au cours de sa séance du 5 décembre 2016,

Arrête :

Article 1er. Les prescriptions électroniques rédigées conformément au protocole en annexe peuvent remplacer leur équivalent papier.

Art. 2. Le présent règlement entre en vigueur le jour de sa publication au *Moniteur belge*

Bruxelles, le 5 décembre 2016.

Le Fonctionnaire dirigéant, Le Président,

H. De Ridder. J. Verstraeten.

Annexe au règlement du 5 décembre 2016 relatif à la prescription électronique intra hospitalière

Protocole conclu entre les organismes assureurs et les commissions d'accord ou de conventions relatif à la prescription hospitalière électronique

Vu les articles 9*bis* et 22, 11°, de la loi coordonnée le 14 juillet 1994 relative à l'assurance obligatoire soins de santé et indemnités;

Vu l'article 36/1 de la loi du 21 août 2008 relative à l'institution et à l'organisation de la plate-forme eHealth et portant diverses dispositions;

Article 1er. Le présent protocole s'applique aux prescriptions hospitalières prévues par ou en vertu de la loi coordonnée le 10 mai 2015 relative à l'exercice des professions de santé et/ou par ou en vertu de la loi coordonnée le 14 juillet 1994 relative à l'assurance obligatoire soins de santé et indemnités.

Par prescription hospitalière, on entend une prescription d'un dispensateur de soins compétent attaché à l'hôpital relative à un patient de l'hôpital (ambulant ou hospitalisé) et exécutée dans l'un des services de l'hôpital.

Article 2. Toute prescription électronique hospitalière doit respecter les conditions relatives à la force probante fixées par l'article 36/1 de la loi du 21 août 2008 relative à l'institution et à l'organisation de la plate-forme eHealth et portant diverses dispositions.

Elle doit également comporter toutes les mentions exigées légalement ou réglementairement pour la prescription papier qu'elle remplace.

Article 3. L'hôpital fixe les procédures utiles pour garantir l'identification et l'authentification correcte du prescripteur. À cet égard, une des procédures suivantes est mise en œuvre :

— Authentification au moyen d'un nom d'utilisateur et d'un mot de passe.

Le nom d'utilisateur et le mot de passe sont strictement personnels et non transmissibles. Le mot de passe peut être utilisé une seule fois ou plusieurs fois. Si le mot de passe peut être utilisé plusieurs fois, le prescripteur est tenu de modifier le mot de passe le plus rapidement possible ou du moins au moment de la première utilisation.

Si le mot de passe peut être utilisé plusieurs fois, le prescripteur doit ensuite régulièrement modifier ce mot de passe. Des procédures de modification régulière des mots de passe doivent être mises en œuvre et rendues obligatoires par l'hôpital.

Un mot de passe sécurisé est idéalement composé de 15 signes et comporte au moins 8 signes. Un mot de passe peut soit être utilisé une fois sur base d'un « challenge » (mot de passe dynamique) chiffré pour chaque utilisation, soit être utilisé plusieurs fois (mot de passe statique).

Un mot de passe qui peut être utilisé plusieurs fois contient des caractères et des symboles alphanumériques placés dans un ordre difficile à déceler. Chaque prescripteur doit veiller à ce que le mot de passe choisi réponde à ces conditions. La responsabilité de chaque prescripteur est engagée lorsqu'un mot de passe est décelé et/ou utilisé de manière illicite.

Il appartient à chaque prescripteur de faire un usage judicieux de son nom d'utilisateur et mot de passe et d'assurer le secret en ce domaine. Chaque prescripteur assume la responsabilité de tout usage approprié ou non de son nom d'utilisateur et mot de passe, en ce compris l'usage par des tiers.

Indien een gebruiker kennis heeft van het verlies van zijn gebruikersnaam en/of paswoord of van elk ongeoorloofd gebruik door derden van zijn gebruikersnaam en/of paswoord, of een dergelijk verlies of ongeoorloofd gebruik vermoedt, dient hij onmiddellijk alle nodige maatregelen te treffen en de informatieveiligheidsconsulent binnen het ziekenhuis op de hoogte te brengen.

Zo spoedig mogelijk na de ontvangst van de melding en binnen de grenzen van de redelijkheid, worden alle mogelijke inspanningen geleverd om verder misbruik te voorkomen.

Elke voorschrijver blijft aansprakelijk voor alle rechtmatig gebruik van zijn gebruikersnaam en/of paswoord en alle onrechtmatig gebruik ingevolge van nalatigheid van zijn gebruikersnaam en/of paswoord dat heeft plaatsgevonden voor het tijdstip waarop de gebruikersnaam en het paswoord geïnactiveerd werden.

— Authenticatie door middel van een sterkere authenticatieprocedure dan gebruikersnaam/paswoord, meer bepaald door middel van het authenticatiecertificaat op de elektronische identiteitskaart of een ander certificaat dat voldoet aan de bepalingen van de wet van 9 juli 2001 houdende vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische handtekeningen en certificatiediensten.

— Authenticatie met identificatiebadge (of een gelijkaardig middel) ter beschikking gesteld van de zorgverlener. Deze badge (of een gelijkaardig middel) is strikt persoonlijk en niet overdraagbaar.

Elke voorschrijver is aansprakelijk voor alle gepast of ongepast gebruik van zijn badge (of een gelijkaardig middel), met inbegrip van het gebruik door derden.

Indien een gebruiker kennis heeft van het verlies van zijn badge (of een gelijkaardig middel) of van elk ongeoorloofd gebruik hiervan door derden, of een dergelijk verlies of ongeoorloofd gebruik vermoedt, dient hij onmiddellijk alle nodige maatregelen te treffen en de informatieveiligheidsconsulent binnen het ziekenhuis op de hoogte te brengen.

Zo spoedig mogelijk na de ontvangst van de melding en binnen de grenzen van de redelijkheid, worden alle mogelijke inspanningen geleverd om verder misbruik te voorkomen.

Elke voorschrijver blijft aansprakelijk voor alle rechtmatig gebruik van zijn badge (of een gelijkaardig middel) en alle onrechtmatig gebruik van zijn badge (of een gelijkaardig middel) ingevolge van nalatigheid dat heeft plaatsgevonden voor het tijdstip waarop de gebruikersnaam en het paswoord geïnactiveerd werden.

Artikel 4. Het elektronisch voorschrift wordt binnen een ziekenhuis bewaard op een wijze dat het niet meer mogelijk is om deze te wijzigen of te wissen zonder sporen na te laten. Daartoe wordt de hierna beschreven procedure van hashing, tijdsregistratie, elektronische handtekening en opslag van het resultaat gevolgd.

Er wordt een hashing procedure toegepast op ieder elektronisch voorschrift. Het gebruikte hashalgoritme is minstens een SHA 256.

Het resultaat van de hashing (de hashcode) is berekend op basis van de specifieke inhoud van het gehashte bestand. Er kan met andere woorden op basis van een bepaalde hashing maar één hashcode overeenkomen met een welbepaalde inhoud. Indien de inhoud van een bestand wordt gewijzigd, dan is bij een nieuwe hashing met hetzelfde hashalgoritme de hashcode verschillend. Aan de hand van de originele hashcode kan dan ook worden vastgesteld of het bestand nadien werd gewijzigd.

Het ziekenhuis voorziet in een systeem van veiligheidsloggins waardoor iedere aanmaak, wijziging of vernietiging van het elektronisch voorschrift en de bijhorende hashcode, die onderworpen is aan de tijdsregistratie, wordt gelogd.

Voor tijdsregistratie van de elektronische voorschriften wordt er binnen ieder ziekenhuis een specifieke databank gecreëerd.

Nadat de hashcode aan de procedure van tijdsregistratie zoals beschreven in dit protocol is onderworpen, wordt elk elektronisch voorschrift met de bijhorende hashcode onderworpen aan de tijdsregistratie in deze databank als afzonderlijk bestand opgeslagen.

De elektronische voorschriften worden in de specifieke databank opgenomen in een KMEHR versie 1*bis* formaat van niveau 1 of 4. Hierbij wordt minstens de identificatiegegevens betreffende de voorschrijver en de patiënt op gestructureerde wijze beschreven.

Lorsqu'un utilisateur est au courant de la perte de son nom d'utilisateur et/ou mot de passe ou d'une quelconque utilisation inappropriée de son nom d'utilisateur et/ou mot de passe par des tiers ou lorsqu'il soupçonne une telle perte ou utilisation inappropriée il doit prendre immédiatement toutes les mesures nécessaires et en informer le conseiller en sécurité de l'information de l'hôpital.

Dans les plus brefs délais de la réception de cette communication et dans les limites du raisonnable, tout sera mis en œuvre pour éviter tout abus.

Chaque prescripteur continue à assumer la responsabilité de chaque usage légitime de son nom d'utilisateur et/ou de son mot de passe et de chaque usage illégitime suite à la négligence de son nom d'utilisateur et/ou de mot de passe avant l'inactivation du nom d'utilisateur ou du mot de passe.

— Authentification au moyen d'une procédure d'authentification plus forte que le nom d'utilisateur/mot de passe, plus précisément au moyen de certificat d'authentification sur la carte d'identité électronique ou d'un autre certificat répondant aux dispositions de la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification.

— Authentification par badge (ou moyen similaire) d'identification mis à disposition du prescripteur. Ce badge (ou moyen similaire) est strictement personnel et non transmissible.

Chaque prescripteur assume la responsabilité de tout usage approprié ou non de son badge (ou moyen similaire), en ce compris l'usage par des tiers.

Lorsqu'un utilisateur est au courant de la perte de son badge (ou moyen similaire) ou d'une quelconque utilisation inappropriée de celui-ci par des tiers ou lorsqu'il soupçonne une telle perte ou utilisation inappropriée il doit prendre immédiatement toutes les mesures nécessaires et en informer le conseiller en sécurité de l'information de l'hôpital.

Dans les plus brefs délais de la réception de cette communication et dans les limites du raisonnable, tout sera mis en œuvre pour éviter tout abus.

Chaque prescripteur continue à assumer la responsabilité de chaque usage légitime de son badge (ou moyen similaire) et de chaque usage illégitime de son badge (ou moyen similaire) suite à la négligence avant l'inactivation de celui-ci.

Article 4. La prescription électronique est conservée de manière à ce qu'il ne soit plus possible de la modifier ou de la supprimer de manière inaperçue. La procédure de hachage, horodatage, signature électronique et enregistrement du résultat, décrite ci-après est appliquée à cet effet.

Une procédure de hachage est appliquée . L'algorithme est au moins un SHA 256.

Le résultat du hachage (hash-code) est calculé sur base du contenu spécifique du fichier ayant fait l'objet du hachage. En d'autres termes, sur base d'un hachage déterminé il n'y a qu'un seul hash-code qui correspond à un contenu déterminé. Si le contenu d'un fichier est modifié, le hash-code sera différent lors d'un nouveau hachage avec le même algorithme de hachage. Le hash-code original permet également de déterminer si le fichier a été modifié par la suite.

L'hôpital prévoit un système de logging de sécurité permettant de réaliser un logging de toute création, modification ou destruction de la prescription électronique et du hash-code y afférents ayant fait l'objet d'un horodatage

Pour l'horodatage des prescriptions électroniques, une banque de données spécifique est créée au sein de l'hôpital.

Après avoir soumis le hash-code à une procédure d'horodatage décrite dans le présent protocole, chaque prescription électronique et le hash-code horodaté y afférent sont enregistrés dans cette banque de données sous forme de fichiers spécifiques.

Les prescriptions électroniques sont enregistrées dans une banque de données spécifique dans un format KMEHR version 1*bis* d'un niveau 1 ou 4. Au minimum, les données d'identification relatives au prescripteur et au patient sont décrites de manière structurée.

Artikel 5. De hashcodes berekend op basis van het elektronisch voorschrift worden onderworpen aan een tijdsregistratie door het eHealth-platform.

Teneinde een overbelasting van de tijdsregistratiedienst te voorkomen, wordt niet voorzien in een tijdsregistratie van iedere hashcode van elke individueel elektronisch voorschrift. In plaats hiervan worden een aantal hashcodes gegroepeerd (in een time stamp bag of TSBag) waarvoor vervolgens één tijdsregistratie wordt aangevraagd.

Iedere vijf minuten zal een bij het ziekenhuis geïnstalleerd programma de nieuw aangemaakte elektronische voorschriften uit de voorlopige bewaarplaats selecteren en groeperen in een TSBag. Het ziekenhuis maakt de TSBag over aan de tijdsregistratiedienst van het ehealth-platform en vraag een tijdsregistratie op het niveau van de TSBag.

Het platform kent vervolgens een tijdsregistratie en een elektronische handtekening aan de TSBag toe.

Het maakt dan aan het ziekenhuis de TSBag voorzien van een een tijdsregistratie en een elektronische handtekening over aan het ziekenhuis.

De software van het ziekenhuis slaat de betreffende hashcodes van de elektronische voorschriften, de TSBag, de tijdsregistratie en de handtekening in het archief van het ziekenhuis op.

Het ziekenhuis is gehouden de lezing van de elektronische voorschriften toe te laten tijdens de verplichte bewaringstermijn van toepassing op de papieren voorschriften die zij vervangen.

De tijdsregistratiedienst van het platform archiveert eveneens in een gegevensbank gecreëerd voor dit doel alle ontvangen TSBags en geleverde tijdsregistraties teneinde de betrokken partijen in geval te ondersteunen in geval van geschil.

Artikel 6. Controle en toezicht

De controle en het toezicht van toepassing op de bepalingen van het huidig protocol worden verricht :

1) Op het niveau van het ziekenhuis

Het toezicht in het ziekenhuis op de voorwaarden zoals bedoeld in artikel 3 moet verricht worden door de informatieveiligheidsconsulent.

De ziekenhuizen moeten de naam, voornaam, hoedanigheid, naam werkgever en plaats van tewerkstelling van de informatieveiligheidsconsulent meedelen aan het Sectoraal comité van de sociale zekerheid en van de gezondheid, afdeling gezondheid. Elke wijziging in deze gegevens moet door de ziekenhuizen binnen de 14 kalenderdagen worden medegedeeld.

2) Op het niveau van het RIZIV

Het toezicht op het respecteren van de bepalingen van dit artikel gebeurt door respectievelijk de Dienst voor Geneeskundige Evaluatie en Controle en de Dienst voor Administratieve Controle, elk op vlak van hun bevoegdheden. Daartoe dient de informatieveiligheidsconsulent van het ziekenhuis een dossier bij te houden waarin het geheel van de procedures, het materiaal en de gebruikte programma's in detail worden beschreven, in het bijzonder om de controle-instanties toe te laten om onmiddellijk toegang te hebben tot de elektronische voorschriften, de bijhorende TSBags en de tijdsregistratie. Dit dossier moet regelmatig worden geactualiseerd. Dit dossier moet ter beschikking gehouden worden voor de controlediensten van het RIZIV.

Onverminderd hun eigen specifieke bevoegdheden moeten de controlediensten eventuele tekortkomingen en onregelmatigheden meedelen aan de overeenkomstencommissie tussen de verpleeginrichtingen en verzekeringsinstellingen.

Artikel 7. Het protocol gesloten op 3 september 2009 en 1 december 2009 tussen de representatieve organisaties van de verplegingsinrichtingen en verzekeringsinstellingen, houdende de voorwaarden en de modaliteiten volgens welke een elektronisch document met precisie kan worden geassocieerd aan een referentiedatum en een referentietijdstip en het niet meer onmerkbaar kan worden gewijzigd, wordt vervangen door het huidig protocol.

Gezien om te worden gevoegd bij de verordening van 5 december 2016

De Leidend Ambtenaar, De Voorzitter,

H. De Ridder. J. Verstraeten.

Article 5. Les hash-codes calculés à partir de la prescription électronique sont horodatés par la plate-forme eHealth.

Pour éviter une surcharge du service d'horodatage, un horodatage de chaque hash-code de chaque prescription électronique individuelle n'est pas prévu. Cependant, plusieurs hash-codes sont regroupés (dans un Time Stamp Bag ou TSBag) et ensuite une seule demande d'horodatage est introduite.

Toutes les cinq minutes, un programme installé au sein de l'hôpital sélectionnera et regroupera dans un TSBag les nouvelles prescriptions électroniques du dépôt provisoire.

L'hôpital transmet le TSBag au service d'horodatage de la plate-forme eHealth et demande un horodatage au niveau du TSBag.

La plate-forme attribue ensuite une estampille temporelle et une signature électronique au TSBag.

Elle transmet alors à l'hôpital le TSBag pourvu d'une estampille temporelle et d'une signature électronique. Le logiciel de l'hôpital enregistre les hash-codes concernés des prescriptions électroniques, le TSBag, l'estampille temporelle et la signature dans les archives de l'hôpital.

L'hôpital est tenu de permettre la lecture des prescriptions électroniques pendant la durée obligatoire de conservation applicable aux prescriptions papier qu'elles remplacent.

Le service d'horodatage de la plate-forme archive également dans une banque de données créée à cet effet tous les TSBag reçus et les estampilles temporelles délivrées afin de soutenir les parties concernées en cas de litige.

Article 6. Contrôle et surveillance

Le contrôle et la surveillance de l'application des dispositions du présent protocole s'effectuent :

1) au niveau de l'hôpital

La surveillance au niveau de l'hôpital des conditions visées à l'article 3 doit être assurée par le conseiller en sécurité de l'information.

Les hôpitaux doivent communiquer à la section santé du Comité sectoriel de la sécurité sociale et de la santé le nom, le prénom, la qualité, le nom de l'employeur et le lieu d'occupation de leur conseiller en sécurité de l'information. Toute modification intervenant dans ces données doit également être communiquée dans les 14 jours civils.

2) au niveau de l'INAMI

La surveillance du respect des dispositions du présent article est assurée respectivement par le Service d'évaluation et de contrôle médicaux et le Service du contrôle administratif, chacun au niveau de ses compétences. A cet effet, le conseiller en sécurité de l'information de l'hôpital tient à jour un dossier dans lequel sont détaillés l'ensemble des procédures, le matériel et les programmes utilisés, en particulier afin de permettre aux instances de contrôle d'avoir immédiatement accès aux prescriptions électroniques et aux TSBags et estampilles temporelles y associés. Ce dossier doit être régulièrement actualisé. Il doit être tenu à la disposition des services de contrôle de l'INAMI.

Sans préjudice de leurs propres compétences spécifiques, les services de contrôle doivent communiquer les éventuelles lacunes ou irrégularités à la Commission de conventions entre les établissements hospitaliers et les organismes assureurs.

Article 7. Le protocole conclu le 3 septembre 2009 et le 1er décembre 2009 entre les organisations représentatives des établissements hospitaliers et les organismes assureurs, portant les conditions et les modalités selon lesquelles un document électronique peut être associé, de manière précise, à une date de référence et une heure de référence et ne peut plus être modifié de manière imperceptible est remplacé par le présent protocole .

Vu pour être annexé au règlement du 5 décembre 2016.

Le Fonctionnaire dirigéant, Le Président,

H. De Ridder. J. Verstraeten.