IBM Watson Health Core

Οι Όροι Χρήσης (Terms of Use - "ToU") αποτελούνται από το παρόν έγγραφο "Όροι Χρήσης της IBM – Όροι για Συγκεκριμένες Προσφορές SaaS" ("Όροι για Συγκεκριμένες Προσφορές SaaS") και ένα έγγραφο με τίτλο "Όροι Χρήσης της IBM – Γενικοί Όροι" ("Γενικοί Όροι"), το οποίο είναι διαθέσιμο στην ιστοσελίδα: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

Σε περίπτωση που υπάρχει οποιαδήποτε αντίθεση, οι Όροι για Συγκεκριμένες Προσφορές SaaS κατισχύουν των Γενικών Όρων. Προβαίνοντας στην παραγγελία, πρόσβαση ή χρήση του IBM SaaS, ο Πελάτης αποδέχεται τους Όρους Χρήσης.

Οι Όροι Χρήσης διέπονται από τους όρους της Διεθνούς Σύμβασης Passport Advantage της IBM, της Διεθνούς Σύμβασης Passport Advantage Express της IBM ή της Διεθνούς Σύμβασης της IBM για Επιλεγμένες Προσφορές IBM SaaS, ανάλογα με την περίπτωση ("Σύμβαση"), οι οποίοι από κοινού με τους Όρους Χρήσης συνιστούν την πλήρη συμφωνία.

1. IBM SaaS

Οι ακόλουθες προσφορές IBM SaaS καλύπτονται από τους παρόντες Όρους για Συγκεκριμένες Προσφορές SaaS:

- IBM Watson Health Core
- IBM Watson Health Core Access
- IBM Watson Health Core Terminology Service

2. Μετρικά Συστήματα Χρέωσης

Το IBM SaaS πωλείται βάσει ενός από τα ακόλουθα μετρικά συστήματα χρέωσης, όπως καθορίζεται στο Έγγραφο Συναλλαγής:

α. **Προσβαση (Access)** – μια μονάδα μέτρησης βάσει της οποίας μπορεί να αποκτηθεί το IBM SaaS. Μια Πρόσβαση είναι το δικαίωμα χρήσης του IBM SaaS. Ο Πελάτης πρέπει να αποκτήσει ένα μόνο δικαίωμα Πρόσβασης για τη χρήση του IBM SaaS κατά τη διάρκεια της περιόδου μέτρησης που καθορίζεται στην Απόδειξη Δικαιώματος ή στο Έγγραφο Συναλλαγής του Πελάτη.

β. **Άτομο (Individual)** – μια μονάδα μέτρησης βάσεις της οποίας μπορεί να αποκτηθεί το IBM SaaS. Ένα Άτομο είναι ένα συγκεκριμένο αντικείμενο ή πρόσωπο. Πρέπει να αποκτηθούν επαρκή δικαιώματα για την κάλυψη κάθε Ατόμου του οποίου γίνεται επεξεργασία μέσω του IBM SaaS ή το οποίο βρίσκονται υπό τη διαχείριση του IBM SaaS κατά τη διάρκεια της περιόδου μέτρησης που καθορίζεται στην Απόδειξη Δικαιώματος ή στο Έγγραφο Συναλλαγής του Πελάτη.

   Για τους σκοπούς αυτού του IBM SaaS, ένα Άτομο είναι ένα πρόσωπο, μια συσκευή ή μια εφαρμογή για φορητές συσκευές τα δεδομένα της οποίας βρίσκονται υπό τη διαχείριση του IBM SaaS.

γ. **Περίπτωση Χρήσης (Instance)** – μια μονάδα μέτρησης βάσει της οποίας μπορεί να αποκτηθεί το IBM SaaS. Περίπτωση Χρήσης είναι η πρόσβαση σε μια συγκεκριμένη παραμετροποίηση του IBM SaaS. Πρέπει να αποκτηθούν επαρκή δικαιώματα για κάθε Περίπτωση Χρήσης του IBM SaaS που καθίσταται διαθέσιμη για πρόσβαση και χρήση κατά τη διάρκεια της περιόδου μέτρησης που καθορίζεται στην Απόδειξη Δικαιώματος ή στο Έγγραφο Συναλλαγής του Πελάτη.

3. Χρεώσεις και Τιμολόγηση

Το πληρωτέο ποσό για το IBM SaaS καθορίζεται σε ένα Έγγραφο Συναλλαγής.

3.1 Χρέωση για μη Πλήρη Μήνα

Στο Έγγραφο Συναλλαγής μπορεί να καθορίζεται μια χρέωση για μη πλήρη μήνα, η οποία θα υπολογίζεται κατ' αναλογία.

3.2 Χρεώσεις Υπέρβασης

Αν η πραγματική χρήση του IBM SaaS από τον Πελάτη κατά τη διάρκεια της περιόδου μέτρησης υπερβαίνει τα δικαιώματα χρήσης που ορίζονται στην Απόδειξη Δικαιώματος, τότε ο Πελάτης θα τιμολογηθεί για την υπέρβαση, όπως ορίζεται στο Έγγραφο Συναλλαγής.

4. Περίοδος Ισχύος και Επιλογές Ανανέωσης

Η περίοδος ισχύος του IBM SaaS αρχίζει κατά την ημερομηνία που η IBM ειδοποιεί τον Πελάτη ότι έχει πρόσβαση στο Πιλοτικό περιβάλλον λειτουργίας του IBM SaaS, όπως τεκμηριώνεται στο Έγγραφο Παραγγελίας. Η περίοδος συνδρομής για δικαιώματα επί Ατόμων αρχίζει κατά την ημερομηνία που η IBM ειδοποιεί τον Πελάτη ότι έχει πρόσβαση στο Παραγωγικό περιβάλλον λειτουργίας. Στο Έγγραφο Παραγγελίας θα καθορίζεται αν το IBM SaaS ανανεώνεται αυτόματα, εξακολουθεί να παρέχεται βάσει συνεχόμενης χρήσης ή διακόπτεται στο τέλος της περιόδου ισχύος.

Σε περίπτωση αυτόματης ανανέωσης, εκτός εάν ο Πελάτης παράσχει έγγραφη ειδοποίηση τουλάχιστον 90 ημέρες πριν την ημερομηνία λήξης της περιόδου ισχύος, το IBM SaaS θα ανανεώνεται αυτόματα για το χρονικό διάστημα που καθορίζεται στην Απόδειξη Δικαιώματος.

Σε περίπτωση συνεχόμενης χρήσης, το IBM SaaS θα εξακολουθεί να είναι διαθέσιμο σε μηνιαία βάση έως ότου ο Πελάτης προβεί σε έγγραφη δήλωση καταγγελίας 90 ημερών. Το IBM SaaS θα εξακολουθεί να είναι διαθέσιμο μέχρι το τέλος του ημερολογιακού μήνα μετά την εν λόγω περίοδο 90 ημερών.

5. Τεχνική Υποστήριξη

Η IBM θα καταστήσει διαθέσιμο το Εγχειρίδιο Υποστήριξης του IBM SaaS (IBM Software as a Service Support Handbook), στο οποίο παρέχονται πληροφορίες επικοινωνίας, πληροφορίες για τις χρονικές περιόδους συντήρησης και άλλες πληροφορίες και διαδικασίες τεχνικής υποστήριξης. Για πληροφορίες επικοινωνίας και άλλες λεπτομέρειες σχετικά με τις διαδικασίες υποστήριξης, ανατρέξτε στο Εγχειρίδιο Υποστήριξης του IBM SaaS: https://support.ibmcloud.com.

Παρέχεται τεχνική υποστήριξη και υποστήριξη για απλά αιτήματα παραμετροποίησης του IBM SaaS μέσω ηλεκτρονικής υποβολής. Η τεχνική υποστήριξη παρέχεται με το IBM SaaS και δεν διατίθεται ως χωριστή προσφορά.

Δεν πρέπει να περιλαμβάνονται Πληροφορίες Προσωπικού Χαρακτήρα (Personal Information - "Πληροφορίες PI"), συμπεριλαμβανομένων Προστατευμένων Πληροφοριών Υγείας (Protected Health Information - "Πληροφορίες PHI") και Ευαίσθητων Πληροφοριών Προσωπικού Χαρακτήρα (Sensitive Personal Information - "Πληροφορίες SPI") σε οποιαδήποτε τεκμηρίωση ή πληροφορίες που παρέχονται κατά την αναφορά ενός προβλήματος.

6. Ορισμοί

Εφαρμοστέοι Νόμοι (Applicable Laws) – οποιοιδήποτε νόμοι, νομοθετήματα ή νομοθετικές πράξεις, κανόνες, κανονισμοί, οδηγίες, διατάγματα ή άλλες απαιτήσεις που εκδόθηκαν από κυβερνητική αρχή ή οποιαδήποτε άλλα γενικώς αναγνωρισμένα πρότυπα του κλάδου που διέπουν την εκτέλεση των παρόντων Όρων Χρήσης.

API – μια Διεπαφή Προγραμμάτων Εφαρμογών (Application Program Interface), που είναι ένα σύνολο ρουτινών, πρωτοκόλλων και εργαλείων για τη δημιουργία εφαρμογών λογισμικού. Τα API καθορίζει τον τρόπο αλληλεπίδρασης των λειτουργικών τμημάτων λογισμικού και χρησιμοποιούνται κατά τον προγραμματισμό λειτουργικών τμημάτων του γραφικού περιβάλλοντος χρήστη (GUI).

Εξουσιοδοτημένος Διαχειριστής (Authorized Administrator) – οποιοσδήποτε υπάλληλος του Πελάτη, εγκεκριμένος από τον Πελάτη εργολάβος, άτομο ή ομάδα που είναι υπεύθυνος(-η) για τη διαχείριση της αδιάλειπτης και αξιόπιστης λειτουργίας της πλατφόρμας. Στις υποχρεώσεις του μπορεί να περιλαμβάνονται η παραμετροποίηση και η υποστήριξη της πλατφόρμας και η διαχείριση χρηστών και λογαριασμών. Ο διαχειριστής μπορεί επίσης να είναι κλινικός ερευνητής που είναι υπεύθυνος για την οργάνωση μιας μελέτης στο σύστημα του Watson Health.

Εξουσιοδοτημένο Άτομο (Authorized Individual) – οποιοδήποτε ταυτοποιημένο πρόσωπο, φορητή συσκευή ή εφαρμογή σε φορητή συσκευή στην οποία έχουν χορηγηθεί δικαιώματα πρόσβασης για την αποστολή δεδομένων στο Watson Health Core. Στα εξουσιοδοτημένα άτομα μπορεί να περιλαμβάνονται ο Πελάτης, οι συμμετέχοντες σε μια μελέτη, ή πελάτες ή ασθενείς του Πελάτη.

Νόμοι περί Προστασίας Δεδομένων που Ισχύουν για τον Πελάτη (Client Applicable Data Laws) – οι Νόμοι περί Προστασίας Δεδομένων που διέπουν την εκπλήρωση από τον Πελάτη των υποχρεώσεών του που απορρέουν από τη Σύμβαση, τα Σχετικά Έγγραφα και τις αντίστοιχες Περιγραφές Υπηρεσιών, Έγγραφα Παραγγελίας και Περιγραφές Έργου που έχουν υπογραφεί από τα Συμβαλλόμενα Μέρη.

Δεδομένα Πελάτη (Client Data) – δεδομένα που εισάγονται στο IBM SaaS από τον Πελάτη ή για λογαριασμό του Πελάτη. Πρόκειται είτε για δεδομένα του ίδιου του Πελάτη είτε για δεδομένα που εισάγονται από ή για λογαριασμό πελατών του Πελάτη ή οποιουδήποτε τρίτου μέρους,

συμπεριλαμβανομένων δεδομένων που προέρχονται από συσκευή διάγνωσης και ευεξίας τρίτου παρόχου.

Νόμοι περί Προστασίας Δεδομένων (Data Laws) – οι Εφαρμοστέοι Νόμοι που σχετίζονται με την προστασία, την εμπιστευτικότητα ή την ασφάλεια δεδομένων.

Υποκείμενο Δεδομένων (Data Subject) – ένα προσδιορισμένο ή προσδιορίσιμο άτομο στο οποίο αντιστοιχούν Δεδομένα Προσωπικού Χαρακτήρα.

Καθορισμένο Κέντρο Πληροφοριακών Συστημάτων (Designated Data Center) – το (τα) κέντρο(-α) πληροφοριακών συστημάτων που έχουν οριστεί ως κύριο(-α) κέντρο(-α) πληροφοριακών συστημάτων και (primary data center) κέντρο(-α) αποκατάστασης μετά από καταστροφή (disaster recovery data center) στο Έγγραφο Συναλλαγής που διέπει την περίπτωση χρήσης του IBM SaaS που έχει προμηθευτεί ο Πελάτης, ανάλογα με την περίπτωση.

Δεδομένα Υγείας (Health Data) – δεδομένα ή πληροφορίες, συμπεριλαμβανομένων εικόνων, που αποτελούν Πληροφορίες Προσωπικού Χαρακτήρα που σχετίζονται με την υγεία.

Πλήρωση Προϋποθέσεων για Δεδομένα Υγείας (Health Data Enabled) – σημαίνει, αναφορικά με το IBM SaaS, τη δυνατότητα του IBM SaaS να ανταποκρίνεται στα ισχύοντα πρότυπα, νόμους και κανονισμούς περί ασφάλειας και προστασίας δεδομένων προσωπικού χαρακτήρα σε Εντός Εμβέλειας Δικαιοδοσίες για Δεδομένα Υγείας, συμπεριλαμβανομένης των προδιαγραφών εφαρμογής που καθορίζονται στο Τμήμα (Part) 164, επιμέρους Τμήματα (Subparts) A και C, των κανονισμών που εφαρμόζουν το Νόμο HIPAA (στην τροποποιημένη του μορφή σύμφωνα με το Νόμο HITECH) και άλλους Εφαρμοστέους Νόμους που διέπουν τα Δεδομένα Υγείας, αλλά δεν σημαίνει ότι η IBM ενεργεί με την ιδιότητα ενός Επιχειρηματικού Εταίρου ή Υπεύθυνου Επεξεργασίας Δεδομένων (Data Controller).

Νόμος HIPAA – ο Νόμος περί Φορητότητας και Ευθύνης της Ασφάλισης Υγείας (Health Insurance Portability and Accountability Act) των Ηνωμένων Πολιτειών του 1996, στην τροποποιημένη του μορφή, συμπεριλαμβανομένης της τροποποίησής του σύμφωνα με το Νόμο περί Τεχνολογίας Πληροφοριών Υγείας για την Οικονομική και Κλινική Υγεία (Health Information Technology for Economic & Clinical Health Act) του Νόμου περί Αμερικανικής Ανάκαμψης και Επανεπένδυσης του 2009 ("Νόμος "HITECH""), ορισμένων κανονισμών που εκδόθηκαν βάσει του Νόμου HIPAA από το Υπουργείο Υγείας και Κοινωνικών Υπηρεσιών (Department of Health and Human Services) των ΗΠΑ στο 45 C.F.R. Parts 160 και 164 και ορισμένων κανονισμών που εκδόθηκαν βάσει του Νόμου HITECH.

Νόμοι περί Προστασίας Δεδομένων που Ισχύουν για την IBM (IBM Applicable Data Laws) – οι Νόμοι περί Προστασίας Δεδομένων που διέπουν την εκπλήρωση από την IBM των υποχρεώσεών της που απορρέουν από τη Σύμβαση, τα Σχετικά Έγγραφα και τις αντίστοιχες Περιγραφές Υπηρεσιών, Έγγραφα Παραγγελίας και Περιγραφές Έργου που έχουν υπογραφεί από τα Συμβαλλόμενα Μέρη.

Προσωπικό IBM (IBM Personnel) – (α) η IBM, οι Συνδεδεμένες με αυτήν Εταιρείες και οι υπεργολάβους της, και οι υπάλληλοι κάθε ενός των ανωτέρω, και (β) οποιοιδήποτε τρίτοι προμηθευτές οι οποίοι παρέχουν υπηρεσίες για λογαριασμό της IBM σύμφωνα με τη Σύμβαση και τα όποια Σχετικά Έγγραφα ή τους οποίους η IBM εξουσιοδοτεί κατά άλλον τρόπο να αποκτούν πρόσβαση σε Δεδομένα Προσωπικού Χαρακτήρα του Πελάτη.

Εντός Εμβέλειας Χώρες (In-scope Countries) – τα 28 Κράτη-Μέλη της Ευρωπαϊκής Ένωσης και η Ελβετία, συν εκείνες τις χώρες που μπορεί να προσθέσει η IBM κατά διαστήματα σε αυτή τη λίστα.

Δεδομένα Προσωπικού Χαρακτήρα (Personal Data) ή **Πληροφορίες Προσωπικού Χαρακτήρα (Personal Information)** – πληροφορίες που βρίσκονται σε οποιοδήποτε μέσο και σε οποιαδήποτε μορφή, συμπεριλαμβανομένων ηλεκτρονικών και έντυπων εγγράφων, που σχετίζονται με ένα ταυτοποιημένο ή ταυτοποιήσιμο άτομο, όπου "ταυτοποιήσιμο άτομο" είναι κάποιος ή κάποια που μπορεί να ταυτοποιηθεί, άμεσα ή έμμεσα, ειδικότερα με την παραπομπή σε έναν αριθμό ταυτότητας ή βάσει ενός ή περισσότερων παραγόντων που αφορούν στην εξωτερική εμφάνιση, στα φυσικά, ψυχολογικά και πνευματικά χαρακτηριστικά, στην οικονομική κατάσταση και στην πολιτισμική ή κοινωνική ταυτότητα του εν λόγω ατόμου.

Επεξεργασία (Process(-ing)) (με ή χωρίς κεφαλαίο Ε) – οποιαδήποτε πράξη ή σειρά πράξεων που εκτελούνται με δεδομένα, με αυτόματα ή μη αυτόματα μέσα, όπως π.χ. η συλλογή, καταγραφή, οργάνωση, αποθήκευση, προσαρμογή ή τροποποίηση, ανάκτηση, μελέτη, χρήση, αποκάλυψη μέσω μετάδοσης, διάδοσης ή κατά άλλον τρόπο διάθεσης, ευθυγράμμιση ή συνδυασμός, φραγή, διαγραφή ή καταστροφή.

Υπό Επεξεργασία Δεδομένα (Processed Data) – οποιαδήποτε δεδομένα, πληροφορίες ή υλικά εμπιστευτικού ή ιδιοκτησιακού χαρακτήρα, συμπεριλαμβανομένων Δεδομένων Υγείας και Δεδομένων Προσωπικού Χαρακτήρα, τα οποία επεξεργάζεται η IBM σύμφωνα με τη Σύμβαση, ένα Σχετικό Έγγραφο ή/και μια Περιγραφή Υπηρεσιών, Έγγραφο Παραγγελίας ή/και Περιγραφή Έργου.

Περιστατικό Ασφάλειας (Security Incident) – έχει τη σημασία που ορίζεται στο Παράρτημα SBCA.

7. Διαχείριση Λογαριασμών

Το IBM SaaS είναι προσβάσιμο μόνο από εξουσιοδοτημένους χρήστες (**"Εξουσιοδοτημένους Διαχειριστές"** ή **"Εξουσιοδοτημένα Άτομα"**) του Πελάτη. Ο Πελάτης θα ελέγχει τους λογαριασμούς που έχουν εξουσιοδοτηθεί να αποκτούν πρόσβαση στο IBM SaaS, στους οποίους μπορεί να περιλαμβάνονται εξουσιοδοτημένες εφαρμογές, προσωπικό του Πελάτη και τρίτοι πάροχοι υπηρεσιών και εργολάβοι του Πελάτη, και θα είναι αποκλειστικά υπεύθυνος (i) για τον έλεγχο όλων των εξουσιοδοτημένων χρηστών, συμπεριλαμβανομένης, ενδεικτικά και όχι περιοριστικά, της επαλήθευσης της ταυτότητας οποιουδήποτε εξουσιοδοτημένου χρήστη, και (ii) για την εξασφάλιση ότι μόνο εξουσιοδοτημένοι χρήστες αποκτούν πρόσβαση στο IBM SaaS.

Στα Εξουσιοδοτημένα Άτομα που είναι πελάτες, ασθενείς ή συμμετέχοντες σε μια μελέτη του Πελάτη μπορεί να χορηγηθεί πρόσβαση αποκλειστικά για το σκοπό της μεταφόρτωσης (upload) δεδομένων στο IBM SaaS και στην περίπτωση αυτή τα εν λόγω Εξουσιοδοτημένα Άτομα δεν θα έχουν άλλες δυνατότητες πρόσβασης στο IBM SaaS.

8. Δεδομένα Προσωπικού Χαρακτήρα

8.1 Γενικές Απαιτήσεις

Σε ό,τι αφορά τα Συμβαλλόμενα Μέρη, ο Πελάτης είναι ο μοναδικός υπεύθυνος επεξεργασίας (controller) όλων των Δεδομένων Προσωπικού Χαρακτήρα του Πελάτη και ο Πελάτης ορίζει την IBM ως εκτελούντα την επεξεργασία των δεδομένων (data processor). Σύμφωνα με τους Ισχύοντες Νόμους περί Προστασίας Δεδομένων, ο Πελάτης έχει το δικαίωμα να δώσει οδηγίες στην IBM αναφορικά με την επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα του Πελάτη από την IBM.

Στο βαθμό που η IBM επεξεργάζεται Δεδομένα Προσωπικού Χαρακτήρα του Πελάτη, η IBM:

α. θα συμμορφώνεται με όλους του Νόμους περί Προστασίας Δεδομένων που Ισχύουν για την IBM και

β. δεν θα συνδυάζει Δεδομένα Προσωπικού Χαρακτήρα του Πελάτη με δεδομένα που προέρχονται από άλλες πηγές, με την εξαίρεση των εξής περιπτώσεων:

- όταν είναι απαραίτητο για την παροχή του IBM SaaS και για κανέναν άλλο σκοπό, εκτός εάν η IBM έχει λάβει ρητές οδηγίες από τον Πελάτη να το πράξει, ή
- σύμφωνα με τους όρους των παρόντων Όρων Χρήσης και του Παραρτήματος SBCA.

Στο βαθμό που η IBM επεξεργάζεται Δεδομένα Προσωπικού Χαρακτήρα του Πελάτη, ο Πελάτης:

α. θα συμμορφώνεται με όλους του Νόμους περί Προστασίας Δεδομένων που Ισχύουν για τον Πελάτη,

β. θα είναι υπεύθυνος για κάθε επικοινωνία του Πελάτη με τις Συνδεδεμένες με τον Πελάτη Εταιρείες, τους ασθενείς, τους τελικούς χρήστες, τα Υποκείμενα Δεδομένων ή/και άλλους τρίτους με τους οποίους συνεργάζεται ο Πελάτης,

γ. θα προβαίνει στη σύναψη συμβάσεων επεξεργασίας δεδομένων με τους υπευθύνους επεξεργασίας (controllers) του οι οποίες είναι απαραίτητες για την επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα από την IBM ως εκτελούντα την επεξεργασία δεδομένων (data processor) και από τους υπεργολάβους επεξεργασίας (sub-processors) της, και

δ. θα λειτουργεί ως μοναδικό σημείο επαφής για την IBM και θα είναι αποκλειστικά υπεύθυνος για τον εσωτερικό συντονισμό, την εξέταση και την υποβολή οδηγιών ή αιτημάτων Συνδεδεμένων με τον Πελάτη Εταιρειών που λειτουργούν ως πρόσθετοι υπεύθυνοι επεξεργασίας (controllers) για την IBM. Η IBM θα απαλλάσσεται από την υποχρέωσή της να ενημερώνει ή να ειδοποιεί οποιαδήποτε Συνδεδεμένη με τον Πελάτη Εταιρεία που λειτουργεί ως υπεύθυνος επεξεργασίας όταν η IBM έχει παράσχει τις εν λόγω πληροφορίες ή ειδοποίηση στον Πελάτη. Η IBM δικαιούται να αρνηθεί να λάβει οδηγίες που παρέχονται απευθείας από μια Συνδεδεμένη με τον Πελάτη Εταιρεία που λειτουργεί ως υπεύθυνος επεξεργασίας και δεν είναι ο Πελάτης.

Κανένα από τα συμβαλλόμενα μέρη δεν θα υποχρεούται να προβαίνει σε πράξεις που συνιστούν παραβίαση των Νόμων περί Προστασίας Δεδομένων που ισχύουν για το εν λόγω συμβαλλόμενο μέρος.

8.2 Δικαιώματα επί Δεδομένων Πελάτη

Ο Πελάτης βεβαιώνει και εγγυάται ότι (α) έχει την κυριότητα των δεδομένων που θα εισάγει στο IBM SaaS ή (β) ότι έχει αποκτήσει, και είναι υπεύθυνος να διατηρεί, όλα τα απαιτούμενα δικαιώματα, άδειες, συναινέσεις και εξουσιοδοτήσεις προκειμένου να χορηγήσει στην IBM τα δικαιώματα πρόσβασης, χρήσης και αποκάλυψης των Δεδομένων Πελάτη σύμφωνα με τους όρους που προβλέπονται στους παρόντες Όρους Χρήσης ή στη Σύμβαση ή όπως κατά άλλον τρόπο κρίνεται απαραίτητο για την παροχή του IBM SaaS από την IBM. Ο Πελάτης βεβαιώνει και εγγυάται επίσης ότι τα Δεδομένα Πελάτη είτε (α) θα σχετίζονται με άτομα που διαμένουν στις Ηνωμένες Πολιτείες και θα εισάγονται στο IBM SaaS μόνο στο κέντρο πληροφοριακών συστημάτων στις Ηνωμένες Πολιτείες, είτε (β) θα σχετίζονται με άτομα που διαμένουν σε μία ή περισσότερες Εντός Εμβέλειας Χώρες και θα εισάγονται στο IBM SaaS στο (στα) Καθορισμένο(-α) Κέντρο(-α) Πληροφοριακών Συστημάτων.

8.3 Υπηρεσίες Δεδομένων και Υποχρεώσεις

α. Ο Πελάτης συμφωνεί ότι θα εκτελεί αναλύσεις ή θα ζητά από την IBM να εκτελέσει αναλύσεις των Δεδομένων Πελάτη μόνο σε συνάρτηση με δραστηριότητες που συνιστούν είτε "δραστηριότητες υγειονομικής περίθαλψης" (health care operations) είτε "έρευνα" (research) από τον Πελάτη, σύμφωνα με τους ορισμούς των εν λόγω δραστηριοτήτων που παρέχονται στο νόμο HIPAA ή σύμφωνα με τους ορισμούς παρόμοιων όρων που παρέχονται σε άλλους Ισχύοντες Νόμους περί Προστασίας Δεδομένων, και ότι ο Πελάτης θα χρησιμοποιεί τα Δεδομένα Πελάτη ή θα καθοδηγεί την IBM να χρησιμοποιεί τα Δεδομένα Πελάτη μόνο σύμφωνα με όλες τις ισχύουσες απαιτήσεις (όπως π.χ. απόφαση ή εγγραφο παραίτησης από Διεθνές Συμβούλιο Ελέγχου όπου απαιτείται) που προβλέπονται στους εν λόγω νόμους και σε άλλους Νόμους περί Προστασίας Δεδομένων που Ισχύουν για τον Πελάτη.

β. Ο Πελάτης είναι αποκλειστικά υπεύθυνος να εξασφαλίζει όλες τις εγγραφές, συναινέσεις, εξουσιοδοτήσεις και άδειες που απαιτούνται από τους Νόμους περί Προστασίας Δεδομένων που Ισχύουν για τον Πελάτη σε κάθε Εντός Εμβέλειας Χώρας όπου δραστηριοποιείται, συμπεριλαμβανομένων, ενδεικτικά και όχι περιοριστικά, του νόμου HIPAA και οποιωνδήποτε άλλων ισχυόντων νόμων, κανόνων και κανονισμών περί προστασίας και ασφάλειας δεδομένων προσωπικού χαρακτήρα, προκειμένου τα Δεδομένα Πελάτη να εισάγονται στο IBM SaaS και να χρησιμοποιούνται και να αποκαλύπτονται όπως προβλέπεται στους παρόντες Όρους Χρήσης και στη Σύμβαση από τον Πελάτη και από την IBM και τους εγκεκριμένους υπεργολάβους της. Η IBM δεν φέρει ευθύνη για την παρακολούθηση του πότε λαμβάνονται ή απαιτούνται οι εν λόγω εγγραφές, συναινέσεις, εξουσιοδοτήσεις και άδειες.

γ. Ο Πελάτης είναι αποκλειστικά υπεύθυνος να εξασφαλίζει ότι όλα τα Δεδομένα Πελάτη που εισάγονται στο IBM SaaS περιορίζονται σε δεδομένα που σχετίζονται με άτομα που διαμένουν στις Ηνωμένες Πολιτείες ή σε κάποια Εντός Εμβέλειας Χώρα.

δ. Η IBM θα διαθέτει κέντρα υποστήριξης με προσωπικό που είναι εκπαιδευμένο στις διατάξεις του νόμου HIPA και άλλων Νόμων περί Προστασίας Δεδομένων που Ισχύουν για την IBM σε Εντός Εμβέλειας Χώρες.

8.4 Μέτρα Ασφάλειας και Περιστατικά Ασφάλειας

α. Η IBM θα εφαρμόζει, θα διατηρεί και θα συμμορφώνεται με τα τεχνικά και οργανωτικά μέτρα (συμπεριλαμβανομένων οργανωτικών διεργασιών και διαδικασιών και οποιωνδήποτε συγκεκριμένων υποχρεώσεων ασφάλειας που ορίζονται ή στις οποίες υπάρχει παραπομπή στους παρόντες Όρους Χρήσης και στο Παράρτημα SBCA) για την προστασία των Δεδομένων Προσωπικού Χαρακτήρα του Πελάτη από μη εξουσιοδοτημένη χρήση ή πρόσβαση, τυχαία απώλεια, καταστροφή, τροποποίηση, καταστροφή, κλοπή ή μη εξουσιοδοτημένη αποκάλυψη.

β. Σε περίπτωση που ένα Περιστατικό Ασφάλειας (σύμφωνα με τον ορισμό που παρέχεται στο Παράρτημα SBCA) που αφορά σε Επεξεργασμένα Δεδομένα του Πελάτη υποπέσει στην αντίληψη της IBM, η IBM θα ενημερώσει τον Πελάτη παρέχοντάς του σχετική ειδοποίηση σύμφωνα με τους όρους του Παραρτήματος SBCA και των Νόμων περί Προστασίας Δεδομένων που Ισχύουν για την IBM και στην εν λόγω ειδοποίηση θα περιλαμβάνονται πληροφορίες για τις όποιες γνωστές επιπτώσεις στον Πελάτη ή σε οποιαδήποτε Υποκείμενα Δεδομένων (αν υπάρχουν) που επηρεάζονται από το εν λόγω Περιστατικό Ασφάλειας και για τις διορθωτικές ενέργειες στις οποίες έχει προβεί ή προτείνεται να προβεί η IBM.

8.5 Λήψη Ερωτήσεων και Παραπόνων

Η IBM θα ενημερώνει τον Πελάτη χωρίς καθυστέρηση εγγράφως και, στο βαθμό που επιτρέπεται από τους Νόμους περί Προστασίας Δεδομένων που Ισχύουν για την IBM, όχι αργότερα από πέντε (5) εργάσιμες ημέρες από την ημερομηνία κατά την οποία ο Υπεύθυνος Προστασίας Προσωπικών Δεδομένων Υγείας του IBM Watson έλαβε οποιαδήποτε ερώτηση, επικοινωνία ή παράπονο που εστάλη στην IBM αναφορικά με Δεδομένα Προσωπικού Χαρακτήρα του Πελάτη από:

α. οποιοδήποτε Υποκείμενο Δεδομένων, σχετικά με την Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα του εν λόγω Υποκειμένου Δεδομένων από την IBM. Ο Πελάτης θα αποκρίνεται σε οποιαδήποτε τέτοια αιτήματα από Υποκείμενα Δεδομένων και η IBM θα συμμορφώνεται με τις εύλογες οδηγίες του Πελάτη βοηθώντας τον Πελάτη να αποκρίνεται στα αιτήματα αυτά. Εάν απαιτείται από Νόμους που Ισχύουν για την IBM, η IBM μπορεί να αποκρίνεται απευθείας σε τέτοια αιτήματα, υπό την προϋπόθεση ότι η IBM έχει ειδοποιήσει τον Πελάτη εκ των προτέρων για την εν λόγω απόκριση και συνεργάζεται ευλόγως με τον Πελάτη αναφορικά με τη μορφή και το περιεχόμενο της εν λόγω απόκρισης, εφόσον αυτό επιτρέπεται από τους Νόμους που Ισχύουν για τον Πελάτη ή καθίσταται κατά άλλον τρόπο εφικτό.

β. οποιαδήποτε δικαστική ή ρυθμιστική αρχή, σχετικά με την Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα του Πελάτη από την IBM, υπό την προϋπόθεση ότι η IBM μπορεί να αποκρίνεται σε τέτοια αιτήματα που ελήφθησαν από κρατική υπηρεσία με τη μορφή μιας κλήτευσης ή παρόμοιου νομικού εγγράφου που υποχρεώνει την IBM να προβεί σε αποκάλυψη ή όπως άλλως απαιτείται από τον Εφαρμοστέο Νόμο περί Προστασίας Δεδομένων, υπό την προϋπόθεση ότι η IBM έχει ειδοποιήσει τον Πελάτη εκ των προτέρων για την εν λόγω αποκάλυψη και συνεργάζεται ευλόγως με τον Πελάτη αναφορικά με τη μορφή και το περιεχόμενο της εν λόγω αποκάλυψης, εφόσον αυτό επιτρέπεται από το νόμο ή καθίσταται κατά άλλον τρόπο εφικτό.

8.6 Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα του Πελάτη

Η IBM θα περιορίζει την αποκάλυψη Δεδομένων Προσωπικού Χαρακτήρα του Πελάτη σε εκείνα τα μέλη του Προσωπικού IBM που μπορεί να χρειαστεί να τη βοηθήσουν στην παροχή των Υπηρεσιών.

Η IBM θα συμμορφώνεται με οποιοδήποτε εύλογο αίτημα του Πελάτη με το οποίο ζητά από την IBM να προβεί στην τροποποίηση, διόρθωση, διαγραφή ή φραγή Δεδομένων Προσωπικού Χαρακτήρα του Πελάτη σύμφωνα με το Εφαρμοστέο Δίκαιο.

Κατόπιν αιτήματος οποιουδήποτε από τα Συμβαλλόμενα Μέρη, η IBM, ο Πελάτης και οι Συνδεδεμένες με αυτούς Εταιρείες θα προβούν στη σύναψη πρότυπων συμβάσεων που απαιτούνται από το νόμο για την προστασία Δεδομένων Προσωπικού Χαρακτήρα του Πελάτη. Τα Συμβαλλόμενα Μέρη συμφωνούν (και θα μεριμνούν για τη συμφωνία των αντίστοιχων Συνδεδεμένων Εταιρειών τους) ότι οι εν λόγω συμβάσεις θα υπόκεινται στους περιορισμούς και στους αποκλεισμούς ευθύνης που ορίζονται στην παρούσα Σύμβαση αναφορικά με την έγερση αξιώσεων μεταξύ των Συμβαλλόμενων Μερών. Τα Συμβαλλόμενα Μέρη θα συνεργάζονται (ή θα μεριμνούν ότι οι Συνδεδεμένες με αυτά Εταιρείες προβαίνουν) στη σύναψη και συμμόρφωση με τυχόν περαιτέρω από κοινού συμφωνηθέντες όρους ή συμβάσεις που μπορεί να απαιτούνται από τους Εφαρμοστέους Νόμους περί Προστασίας Δεδομένων.

8.7 Επιστροφή Δεδομένων Προσωπικού Χαρακτήρα του Πελάτη

Μετά τη λήξη ή καταγγελία της Σύμβασης, η IBM θα διακόψει, ή θα μεριμνήσει ότι όλο το Προσωπικό IBM διακόπτει, τη χρήση ή επεξεργασία Πληροφοριών Ιδιοκτησιακού Χαρακτήρα του Πελάτη και Δεδομένων Προσωπικού Χαρακτήρα του Πελάτη και θα προβεί, κατ' επιλογή ή κατόπιν αιτήματος του Πελάτη:

α. στην επιστροφή στον Πελάτη, στη μορφή και στα μέσα αποθήκευσης που μπορεί ευλόγως να ζητήσει ο Πελάτης, όλων των Πληροφοριών Ιδιοκτησιακού Χαρακτήρα και Δεδομένων Προσωπικού Χαρακτήρα του Πελάτη τα οποία αποθηκεύονται από την IBM σε ηλεκτρονική μορφή και, κατόπιν επιβεβαίωσης παραλαβής των εν λόγω Πληροφοριών και Δεδομένων από τον Πελάτη, στη διαγραφή ή καταστροφή των Πληροφοριών Ιδιοκτησιακού Χαρακτήρα και Δεδομένων Προσωπικού Χαρακτήρα του Πελάτη ή κατά άλλον τρόπο στη μετατροπή τους σε μη αναγνώσιμη ή μη αποκωδικοποιήσιμη μορφή, συμπεριλαμβανομένων οποιωνδήποτε αντιτύπων ή εφεδρικών (backup) αντιγράφων τους. Η IBM μπορεί να χρεώσει τον Πελάτη για το κόστος των μέσων αποθήκευσης και για ορισμένες δραστηριότητες που εκτελέστηκαν κατόπιν αιτήματος του Πελάτη (όπως π.χ. η παράδοση Πληροφοριών Ιδιοκτησιακού Χαρακτήρα και Δεδομένων Προσωπικού Χαρακτήρα του Πελάτη σε μια συγκεκριμένη μορφή ή η καταστροφή Πληροφοριών Ιδιοκτησιακού Χαρακτήρα και Δεδομένων Προσωπικού Χαρακτήρα με ένα συγκεκριμένο τρόπο), και

β. στην άμεση διαγραφή ή καταστροφή των Πληροφοριών Ιδιοκτησιακού Χαρακτήρα και Δεδομένων Προσωπικού Χαρακτήρα του Πελάτη ή κατά άλλον τρόπο στη μετατροπή τους σε μη αναγνώσιμη ή μη αποκωδικοποιήσιμη μορφή, συμπεριλαμβανομένων οποιωνδήποτε αντιτύπων ή εφεδρικών (backup) αντιγράφων τους.

8.8 Σύμβαση Επιχειρηματικού Εταίρου

Στο βαθμό που είναι απαραίτητο και απαιτείται από το νόμο HIPAA, η IBM και ο Πελάτης θα προβούν στη σύναψη μιας Σύμβασης Επιχειρηματικού Εταίρου (Business Associate Agreement - "Σύμβαση BAA"), η οποία θα διέπει τις υποχρεώσεις της IBM ως Επιχειρηματικού Εταίρου του Πελάτη αναφορικά με την παροχή του IBM SaaS. Χωρίς να τίθεται περιορισμός στις ρητές υποχρεώσεις της IBM που απορρέουν από τη Σύμβαση και τη Σύμβαση BAA, ανάλογα με την περίπτωση, ο Πελάτης αποδέχεται και συμφωνεί ότι είναι υπεύθυνος να προσδιορίζει την ισχύ και να συμμορφώνεται με όλους τους Εφαρμοστέους Νόμους και απαιτήσεις απόκτησης αδειών χρήσης που διέπουν τη χρήση του IBM SaaS από τον Πελάτη ή άλλες δραστηριότητες του Πελάτη σχετικά με το IBM SaaS (συμπεριλαμβανομένων της χρήσης ή άλλων δραστηριοτήτων από Εξουσιοδοτημένους Χρήστες).

8.9 Πρόσθετη Πράξη για την Επεξεργασία Δεδομένων στην Ευρωπαϊκή Ένωση

Εάν ο Πελάτης ζητήσει από την IBM την επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα στην Ευρωπαϊκή Ένωση, η IBM και ο Πελάτης θα προβούν στη σύναψη μιας Πρόσθετης Πράξης για την Επεξεργασία Δεδομένων στην οποία θα περιλαμβάνονται οι κατάλληλες Πρότυπες Ρήτρες της ΕΕ, από τις οποίες έχουν αφαιρεθεί η προαιρετικές ρήτρες.

9. Πρόσθετοι Όροι για Προσφορά IBM SaaS

9.1 Ασφάλεια

Αυτό το IBM SaaS συμμορφώνεται με τις βασικές αρχές προστασίας και ασφάλειας δεδομένων της IBM, οι οποίες καθίστανται διαθέσιμες στην ιστοσελίδα http://www.ibm.com/cloud/data-security και με τους πρόσθετους όρους που προβλέπονται παρακάτω και στο Παράρτημα Ασφάλειας και Επιχειρησιακής Συνέχειας των παρόντων Όρων Χρήσης. Τυχόν αλλαγές στις βασικές αρχές ασφάλειας δεδομένων της IBM δεν θα υποβαθμίζουν την ασφάλεια του IBM SaaS.

Το IBM Watson Health Core υλοποιεί πολιτικές, πρότυπα και διαδικασίες ασφάλειας που βασίζονται στο πλαίσιο ISO 27001, όπως περιγράφεται πιο αναλυτικά στην Περιγραφή Ασφάλειας. Μερικές από τις λειτουργίες ασφάλειας που παρέχει η λύση είναι οι εξής:

α. Ζώνες Ασφαλούς Λειτουργίας (Secure Operating Zones)

Το IBM Watson Health Core υλοποιεί μια στρατηγική "άμυνας σε βάθος", χρησιμοποιώντας διαφορετικές ζώνες ασφάλειας για τη διαχείριση σημείων ενοποίησης με το cloud (cloud integration points), όπως π.χ. για την ένταξη δεδομένων και την ανάπτυξη προσαρμοσμένων εφαρμογών.

β. Κρυπτογράφηση (Encryption)

Όλα τα Δεδομένα Πελάτη κρυπτογραφούνται τόσο στο σημείο αποθήκευσής τους όσο και κατά τη μετάδοσή τους. Όλα τα δεδομένα που μεταβιβάζονται προς και από το IBM Watson Health Core κρυπτογραφούνται. Μια κοινόχρηστη υπηρεσία παρέχει τη δυνατότητα διαχείρισης κλειδιών κρυπτογράφησης. Ο Πελάτης είναι υπεύθυνος για όλες τις δικτυακές συνδέσεις και την ποιότητα των συνδέσεων μεταξύ της Υπηρεσίας IBM Watson Health και του εξυπηρετητή μεσολάβησης (proxy server) του Πελάτη.

γ. Παρακολούθηση Συμβάντων Ασφαλείας (Security Event Monitoring)

Η IBM αξιοποιεί την πλατφόρμα διαχείρισης πληροφοριών ασφάλειας της για τη διαχείριση πληροφοριών και συμβάντων ασφάλειας, τη διαχείριση αρχείων καταγραφής (logs), την εξερεύνηση περιστατικών, τον εντοπισμό απειλών και τη διαχείριση τρωτών σημείων.

δ. Διαχείριση Ταυτοτήτων (Identity Management)

- Το Watson Health Core υποστηρίζει παρόχους στοιχείων ταυτότητας ανοιχτών προτύπων για τη διαχείριση μεγάλων πληθυσμών ασθενών και χρηστών χρησιμοποιώντας το OpenID Connect.
- Για τους πληθυσμούς χρηστών για τους οποίους η IBM είναι ο πάροχος στοιχείων ταυτότητας, το Watson Health Core αξιοποιεί τις κατάλληλες υπηρεσίες καταλόγου και λειτουργίες διαχείρισης ταυτοτήτων για το χειρισμό των διαδικασιών ταυτοποίησης.

ε. Ισχυρή Ταυτοποίηση (Strong Authentication) και Πρόσβαση Βάσει Ρόλων (Role Based Access)

- Το Watson Health Core υποστηρίζει την ταυτοποίηση μέσω SAML ως μηχανισμό για την ενσωμάτωση των υπηρεσιών καταλόγου ή ενιαίας πρόσβασης (Single Sign On - SSO) των Πελατών.
- Το Watson Health Core αξιοποιεί μια λύση διαχείρισης πρόσβασης και ένα σχετικό σύνολο λειτουργιών για τη διαχείριση πολιτικών ασφάλειας, όπου απαιτείται.
- Το Watson Health Core υποστηρίζει τη βασιζόμενη σε λογισμικό ταυτοποίηση δύο παραγόντων (two-factor authentication).
- Το Watson Health Core παρέχει τη δυνατότητα βασικού ελέγχου βάσει ρόλων, ανάλογα με τις απαιτήσεις. Το Watson Health Core υποστηρίζει την παραμετροποίηση ομάδων μελέτης, προφίλ χρηστών, ρόλων και ομάδων χρηστών μέσω API (application programming interfaces) που επιτρέπουν την πρόσβαση βάσει ρόλων.

9.2 Cookies

Ο Πελάτης είναι ενήμερος και συμφωνεί ότι η IBM μπορεί, στο πλαίσιο της κανονικής λειτουργίας και υποστήριξης του IBM SaaS, να προβαίνει στη συλλογή δεδομένων προσωπικού χαρακτήρα του Πελάτη (των υπαλλήλων και των εργολάβων του) σχετικά με τη χρήση του IBM SaaS, μέσω τεχνολογιών παρακολούθησης και άλλων τεχνολογιών. Με αυτό τον τρόπο η IBM συγκεντρώνει στατιστικά στοιχεία χρήσης και πληροφορίες για την αποτελεσματικότητα του IBM SaaS με σκοπό τη βελτίωση της γενικής εμπειρίας των χρηστών ή/και την εξατομικευμένη αλληλεπίδραση με τον Πελάτη. Ο Πελάτης επιβεβαιώνει ότι θα αποκτήσει ή έχει ήδη αποκτήσει την απαιτούμενη συναίνεση προκειμένου η IBM να προβεί στην επεξεργασία πληροφοριών προσωπικού χαρακτήρα για τον ανωτέρω σκοπό εντός της IBM, άλλων εταιρειών IBM και των υπεργολάβων τους, οπουδήποτε δραστηριοποιούμαστε επιχειρηματικά, συμμορφούμενοι με το εφαρμοστέο δίκαιο. Η IBM θα ανταποκρίνεται στα αιτήματα των υπαλλήλων και των εργολάβων του Πελάτη αναφορικά με την πρόσβαση, ενημέρωση, διόρθωση ή διαγραφή των συλλεχθεισών πληροφοριών προσωπικού χαρακτήρα τους.

9.3 Τοποθεσίες Αντλούμενων Οφελών

Κατά περίπτωση, οι φόροι βασίζονται στην τοποθεσία ή στις τοποθεσίες που προσδιορίζονται από τον Πελάτη ως αντλούσες τα οφέλη του IBM SaaS. Η IBM θα εφαρμόζει φόρους με βάση την επαγγελματική διεύθυνση που δηλώνεται κατά την παραγγελία του IBM SaaS ως κύρια επωφελούμενη τοποθεσία, εκτός εάν ο Πελάτης παράσχει πρόσθετες πληροφορίες στην IBM. Ο Πελάτης είναι υπεύθυνος για την έγκαιρη ενημέρωση των εν λόγω πληροφοριών και την κοινοποίηση οποιωνδήποτε αλλαγών στην IBM.

9.4 Συνεχής Παράδοση

Ο Πελάτης δικαιούται να χρησιμοποιεί τις δυνατότητες και βελτιώσεις που προστίθενται στη λύση και τίθενται σε εφαρμογή από την IBM μέσω ενός μοντέλου συνεχούς παράδοσης στο cloud.

9.5 Εφεδρική Αποθήκευση και Αποκατάσταση

Το IBM Watson Health Core παρέχει τη δυνατότητα εφεδρικής αποθήκευσης (backup) Δεδομένων Πελάτη στο περιβάλλον παραγωγής (συμπεριλαμβανομένων των χώρων αποθήκευσης Data Lake ("Λίμνη Δεδομένων") και Data Reservoir (Δεξαμενή Δεδομένων)) ώστε να είναι δυνατή η αποκατάστασή τους στην τελευταία γνωστή έγκυρη κατάσταση σε περίπτωση βλάβης του συστήματος.

9.6 Υψηλή Διαθεσιμότητα

Τα λειτουργικά τμήματα του IBM Watson Health Core στο περιβάλλον παραγωγής λειτουργούν σε διατάξεις υψηλής διαθεσιμότητας, όπου οι εξυπηρετητές βάσης δεδομένων (database servers) σχηματίζουν ένα σύμπλεγμα (cluster) που επιτρέπει την εφεδρική υποστήριξη, την κατανομή φορτίων εργασίας και την παράκαμψη μοναδικών σημείων βλάβης.

9.7 Αποκατάσταση μετά από Καταστροφή

Η προσέγγιση της IBM για την αποκατάσταση μετά από καταστροφή συνίσταται στη λειτουργία διαφορετικών κέντρων πληροφοριακών συστημάτων σε διαφορετικές γεωγραφικές περιοχές για την επίτευξη των εξής στόχων αναφορικά με την επιχειρησιακή συνέχεια στο περιβάλλον παραγωγής:

- Στόχος για το Χρόνο Απόκρισης (Response Time Objective - RTO) – εντός 36 ωρών από τη δήλωση καταστροφής
- Στόχος για το Σημείο Αποκατάστασης (Recovery Point Objective - RPO) – μέγιστη απώλεια περιεχομένου του Πελάτη: 24 ώρες

9.8 Εργαλεία Μέτρησης

Το IBM SaaS χρησιμοποιεί μια λύση συνθετικής παρακολούθησης (synthetic monitoring) για την παρακολούθηση, καταμέτρηση και αναφορά στοιχείων διαθεσιμότητας ή διακοπών λειτουργίας και τη σύγκριση των εν λόγω στοιχείων με τα δεσμευτικά επίπεδα παροχής υπηρεσιών. Η λύση αυτή προσομοιώνει και παρακολουθεί τις αποκρίσεις και τη γενική εμπειρία χρηστών σε παγκόσμιο επίπεδο, συγκεντρώνοντας στοιχεία τόσο για τη στατική διαθεσιμότητα όσο και για τις συναλλαγές.

Το IBM SaaS χρησιμοποιεί επίσης ένα εσωτερικό σύστημα παρακολούθησης για τη συγκέντρωση μετρικών στοιχείων και στοιχεία για συμβάντα και προειδοποιήσεις για ολόκληρη τη λύση.

9.9 Δημοσιότητα

Ο Πελάτης συμφωνεί ότι η IBM μπορεί να αναφέρει τον Πελάτη δημοσίως ως συνδρομητή του IBM SaaS σε διαφημίσεις και σε δημοσιεύσεις στον τύπο.

Παράρτημα Α

1. IBM Watson Health Core

Το IBM Watson Health Core είναι μια πλατφόρμα ως υπηρεσία (platform as a service - "PaaS") που Πληροί τις Προϋποθέσεις για Δεδομένα Υγείας, μια πλατφόρμα ανάπτυξης και ένα λειτουργικό υποσύστημα για την αποθήκευση, επιμέλεια και επεξεργασία Προστατευμένων Πληροφοριών Υγείας (Protected Health Information - "Πληροφορίες PHI"), όπως αυτές ορίζονται στο Νόμο HIPAA, και άλλων Δεδομένων Υγείας σύμφωνα με τους Νόμους περί Προστασίας Δεδομένων που Ισχύουν για την IBM τα οποία βρίσκονται σε ένα κέντρο πληροφοριακών συστημάτων που βρίσκεται στην κυριότητα ή υπό τον έλεγχο της IBM. Ο Πελάτης πρέπει να αποκτήσει τα κατάλληλα δικαιώματα χρήσης του IBM Watson Health Core και του IBM Watson Health Core Access προκειμένου να καταστεί δυνατή η χρήση των λειτουργιών και δυνατοτήτων που περιγράφονται παρακάτω.

1.1 Περιβάλλοντα Λειτουργίας του Watson Health Core

Το δικαίωμα χρήσης του Watson Health Core περιλαμβάνει τρία διαφορετικά περιβάλλοντα λειτουργίας cloud που Πληρούν τις Προϋποθέσεις για Δεδομένα Υγείας και έχουν σχεδιαστεί ώστε να επιτρέπουν την επεξεργασία Δεδομένων Υγείας από τον Πελάτη:

- Πιλοτικό Περιβάλλον (Pilot)

  Παρέχει ένα περιβάλλον πιλοτικής λειτουργίας ("sandbox") όπου οι Πελάτες μπορούν να αναπτύξουν εφαρμογές με χρήση του IBM SaaS και να διενεργήσουν δοκιμές με αυτές. Το πιλοτικό περιβάλλον εφαρμόζει όλους τους μηχανισμούς ελέγχου ασφάλειας του Νόμου HIPAA, με την εξαίρεση της Αποκατάστασης μετά από Καταστροφή, της υψηλής διαθεσιμότητας και της εφεδρικής αποθήκευσης συστημάτων οργανωτικής διάρθρωσης (systems of record).

- Περιβάλλον Παραγωγής (Production)

  Παρέχει ένα ολοκληρωμένο περιβάλλον λειτουργίας που επιτρέπει την εκτέλεση φορτίων εργασίας με Δεδομένα Υγείας από τους Πελάτες. Το περιβάλλον παραγωγήςπαρέχει υψηλή διαθεσιμότητα και εξισορρόπηση φορτίων και επιτρέπει την αυτόματη μεταγωγή σε μια τοποθεσία Αποκατάστασης μετά από Καταστροφή.

- Περιβάλλον Αποκατάστασης μετά από Καταστροφή (Disaster Recovery)

  Παρέχει ένα κατοπτρικό αντίγραφο του Περιβάλλοντος Παραγωγής. Βρίσκεται σε ένα χωριστό κέντρο πληροφοριακών συστημάτων.

1.2 Ανάπτυξη Εφαρμογών

Το IBM Watson Health Core επιτρέπει την ανάπτυξη εφαρμογών και την ασφαλή συλλογή δεδομένων από συσκευές του Πελάτη ή εξουσιοδοτημένων χρηστών του Πελάτη. Παρέχονται API και αντίστοιχη τεκμηρίωση που επιτρέπουν την ανάπτυξη εφαρμογών και την ανταλλαγή δεδομένων με το IBM SaaS από τους εξουσιοδοτημένους χρήστες του Πελάτη, συμπεριλαμβανομένων των τρίτων παρόχων υπηρεσιών του Πελάτη. Η χρήση των API από τον Πελάτη ή τις εταιρείες ανάπτυξης προγραμμάτων με τις οποίες συνεργάζεται γίνεται με την επιφύλαξη της συμμόρφωσης με τις Απαιτήσεις για την Ανάπτυξη API (API Developer Requirements).

- REST API

  Το Watson Health Core παρέχει μια σειρά από REST API και υπηρεσίες για την πλατφόρμα Watson Health Core. Στις δυνατότητες των API περιλαμβάνονται, ενδεικτικά, μηχανισμοί για την πρόσβαση σε υποδομές αποθήκευσης δεδομένων, η υπηρεσία επιμέλειας δεδομένων (data curation), η διαχείριση χρηστών και τα αρχεία καταγραφής ελέγχου (audit logs).

- Apple HealthKit και Apple ResearchKit

  Το Watson Health Core υποστηρίζει την ενοποίηση με το πλαίσιο Apple ResearchKit API για βασιζόμενες στο iOS ερευνητικές μελέτες, και με το Apple HealthKit για τη συλλογή δεδομένων ευεξίας.

1.3 Διακυβέρνηση Δεδομένων

- Διαχείριση Συναινέσεων (Consent Management)

  Το Watson Health Core παρέχει το πλαίσιο για την καταγραφή της συναίνεσης που παρέχεται από ασθενείς ή από τους συμμετέχοντες σε μια μελέτη και την ασφαλή αποθήκευση στοιχείων συναίνεσης χωριστά από τα φορτία δεδομένων κατά την εγγραφή ενός ατόμου μέσω μιας εφαρμογής του Πελάτη που απαιτεί μια δήλωση συναίνεσης.

- Μάσκες Δεδομένων (Data Masking)

  Το Watson Health Core παρέχει τη δυνατότητα διαχωρισμού στοιχείων ταυτότητας ατόμων από δομημένα φορτία δεδομένων. Το Watson Health Core λαμβάνει τα δεδομένα στο cloud μέσω διαφόρων API. Τα API επιτρέπουν το διαχωρισμό στοιχείων για την ταυτότητα ασθενών ή ατόμων από το υπόλοιπο φορτίο δεδομένων και την αποθήκευσή τους σε μια χωριστή κρυπτογραφημένη αποθήκη δεδομένων (data store). Στο φορτίο δεδομένων αποδίδεται ένας ανωνυμοποιημένος δείκτης που μπορεί να χρησιμοποιηθεί στη συνέχεια για την παρακολούθηση προέλευσης (provenance tracking).

1.4 Υπηρεσίες Δεδομένων Υγείας

Το Watson Health Core επιτρέπει τη συλλογή, αποθήκευση και συγχρονισμό δεδομένων, συμπεριλαμβανομένων εξωγενών Δεδομένων Υγείας και άλλων Πληροφοριών Προσωπικού Χαρακτήρα, δομημένων και μη.

- Απορρόφηση Δεδομένων (Data Ingestion)

  Το Watson Health Core παρέχει τη δυνατότητα απορρόφησης δεδομένων από εφαρμογές ή συσκευές ασθενών μέσω API. Το Watson Health Core χορηγεί σε κάθε ένα από τα Εξουσιοδοτημένα Άτομα του Πελάτη το δικαίωμα μεταφόρτωσης (upload) έως 25 MB δεδομένων στο Health Core κατά τη διάρκεια κάθε έτους της συμβατικής περιόδου. Η υπηρεσία επιτρέπει έως 10 διαδικασίες μεταφόρτωσης ανά Άτομο ανά ημέρα.

- Λειτουργική "Λίμνη Δεδομένων" (Operational Data Lake)

  Τα μη επεξεργασμένα Δεδομένα Πελάτη ή δεδομένα ασθενών αποθηκεύονται στο Watson Health Core στην αρχική τους μορφή έως ότου χρησιμοποιηθούν για σκοπούς ανάλυσης και μοντελοποίησης.

- Εξαγωγή/Μετασχηματισμός/Φόρτωση (Extract Transform Load - ETL)

  Τα δεδομένα μετασχηματίζονται σε μια κανονικοποιημένη μορφή στο λειτουργικό υποσύστημα. Ένα βασιζόμενο στα πρότυπα του κλάδου Enterprise Service Bus για υπηρεσίες υγειονομικής περίθαλψης επιτρέπει την ενοποίηση με διάφορες εφαρμογές και πρωτόκολλα του Πελάτη.

- Δεξαμενή Δεδομένων (Data Reservoir)

  Αφού ολοκληρωθεί η επιμέλειά τους, τα δεδομένα μεταφέρονται στη Δεξαμενή Δεδομένων. Το Watson Health Core αξιοποιεί διάφορες πτυχές του IBM Unified Data Model for Healthcare για την κανονικοποίηση επιχειρηματικών και τεχνικών δεδομένων υγείας για αναλυτική χρήση.

- Κύριο Ευρετήριο Προσώπων (Master Person Index)

  Το Watson Health παρέχει εργαλεία Διαχείρισης Κρίσιμων Δεδομένων (Master Data Management) για τη συγκέντρωση δεδομένων από διαφορετικές πηγές με σκοπό τη δημιουργία μιας Διαχρονικής Εγγραφής Προσώπου (Longitudinal Person Record - "Εγγραφή LPR").

2. Προαιρετικές Επιλογές

2.1 IBM Watson Health Core Terminology Service

Αυτή η πρόσθετη υπηρεσία επιτρέπει την ενοποίηση και διαλειτουργικότητα δεδομένων μεταξύ διαφορετικών συστημάτων υγείας, εξασφαλίζοντας τη χρήση μιας ενιαίας ιατρικής ορολογίας σε όλες τις εφαρμογές Watson Health στο Cloud. Αυτή η υπηρεσία παρέχει μια λειτουργική πλατφόρμα για την εκτέλεση εργασιών αναφορικά με ορολογίες, συστήματα κωδικοποίησης και δομημένο περιεχόμενο, όπως π.χ.:

- δημιουργία νέων συστημάτων κωδικοποίησης,
- μετάφραση διεθνών συστημάτων κωδικοποίησης, και
- συσχέτιση τοπικών καταλόγων κωδικών με διεθνή πρότυπα.

Παράρτημα Β

Η IBM παρέχει την ακόλουθη σύμβαση επιπέδου παροχής υπηρεσιών ("SLA") αναφορικά με τη διαθεσιμότητα του IBM SaaS, όπως καθορίζεται σε μια Απόδειξη Δικαιώματος. Η Σύμβαση SLA δεν συνιστά εγγύηση. Η Σύμβαση SLA είναι διαθέσιμη μόνο στον Πελάτη και ισχύει μόνο για τη χρήση σε περιβάλλοντα παραγωγής.

1. Πιστώσεις Διαθεσιμότητας

Οι επιστροφές χρημάτων λόγω μειωμένης διαθεσιμότητας αφορούν μόνο στις χρεώσεις συνδρομής για δικαιώματα επί Ατόμων.

Ο Πελάτης πρέπει να υποβάλει ένα δελτίο υποστήριξης για Ζήτημα Κρισιμότητας 1 στο Help Desk τεχνικής υποστήριξης της IBM, εντός 24 ωρών από τη στιγμή που ο Πελάτης παρατηρεί για πρώτη φορά ότι προέκυψε ένα συμβάν που έχει επιπτώσεις στη διαθεσιμότητα του IBM SaaS. Ο Πελάτης πρέπει εύλογα να βοηθά την IBM στη διάγνωση και επίλυση προβλημάτων.

Μια αξίωση βάσει δελτίου υποστήριξης για τη μη ανταπόκριση στις απαιτήσεις μιας Σύμβασης SLA πρέπει να υποβάλλεται εντός τριών εργάσιμων ημερών από το τέλος του συμβατικού μήνα. Η αποζημίωση για μια έγκυρη αξίωση μη ανταπόκρισης στις απαιτήσεις μιας Σύμβασης SLA θα συνίσταται σε μια πίστωση έναντι ενός μελλοντικού τιμολογίου για το IBM SaaS η οποία θα βασίζεται στη διάρκεια του χρονικού διαστήματος κατά το οποίο δεν ήταν διαθέσιμη η δυνατότητα επεξεργασίας στο σύστημα παραγωγής του IBM SaaS ("Χρόνος Διακοπής Λειτουργίας"). Ο Χρόνος Διακοπής Λειτουργίας μετράται από τη χρονική στιγμή που ο Πελάτης αναφέρει το συμβάν έως τη χρονική στιγμή που αποκαθίσταται το IBM SaaS και δεν περιλαμβάνει το χρόνο που σχετίζεται με μια προγραμματισμένη ή ανακοινωθείσα διακοπή λειτουργίας για σκοπούς συντήρησης, αιτίες πέραν από τον έλεγχο της IBM, προβλήματα με το περιεχόμενο ή την τεχνολογία, το σχεδιασμό ή τις οδηγίες του Πελάτη ή τρίτων, μη υποστηριζόμενες διατάξεις συστημάτων και πλατφορμών ή άλλα σφάλματα του Πελάτη, ή προκληθέντα από τον Πελάτη περιστατικά ασφάλειας ή δοκιμές ασφάλειας του Πελάτη. Η IBM θα παρέχει την υψηλότερη ισχύουσα αποζημίωση με βάση τη σωρευτική διαθεσιμότητα του IBM SaaS κατά τη διάρκεια κάθε Συμβατικού Μήνα, όπως αναφέρεται στον παρακάτω πίνακα. Η συνολική αποζημίωση που παρέχεται για οποιονδήποτε συμβατικό μήνα δεν μπορεί να υπερβαίνει το 20 τοις εκατό (20%) του εν δωδέκατου (1/12) της ετήσιας χρέωσης για το IBM SaaS.

2. Επίπεδα Παροχής Υπηρεσιών

Διαθεσιμότητα του IBM SaaS κατά τη διάρκεια ενός συμβατικού μήνα

Διαθεσιμότητα κατά τη διάρκεια ενός Συμβατικού Μήνα	**Αποζημίωση (% της μηνιαίας χρέωσης συνδρομής* για Άτομα για το συμβατικό μήνα που αποτελεί αντικείμενο αξίωσης)**
< 99,95%	10%
< 99,0%	20%

* Εάν το IBM SaaS αποκτήθηκε από έναν Εμπορικό Συνεργάτη της IBM, η μηνιαία χρέωση συνδρομής θα βασίζεται στην εκάστοτε ισχύουσα τιμή καταλόγου του IBM SaaS για το συμβατικό μήνα που αποτελεί αντικείμενο αξίωσης, με έκπτωση 50%. Η IBM θα προβαίνει σε μια άμεση επιστροφή χρημάτων στον Πελάτη.

Η Διαθεσιμότητα, η οποία εκφράζεται ως ποσοστό, υπολογίζεται ως εξής: ο συνολικός αριθμός λεπτών σε ένα συμβατικό μήνα, μείον το συνολικό αριθμό λεπτών του Χρόνου Διακοπής Λειτουργίας κατά τη διάρκεια του συμβατικού μήνα, διαιρούμενος διά του συνολικού αριθμού λεπτών στο συμβατικό μήνα.

Παράδειγμα: Χρόνος Διακοπής Λειτουργίας 108 λεπτών συνολικά κατά τη διάρκεια ενός Συμβατικού Μήνα

Σύνολο λεπτών κατά τη διάρκεια ενός Συμβατικού Μήνα 30 ημερών = 43.200 λεπτά - 108 λεπτά Χρόνου Διακοπής Λειτουργίας = 43,092 λεπτά _____ Συνολική διάρκεια Συμβατικού Μήνα = 43.200 λεπτά	= 10% Πίστωση Διαθεσιμότητας για 99,75% διαθεσιμότητα κατά τη διάρκεια του Συμβατικού Μήνα

3. Εξαιρέσεις

Η παρούσα Σύμβαση SLA δεν ισχύει για τα εξής:

- Πέρα από την παρακολούθηση των εξυπηρετητών, η Σύμβαση SLA δεν ισχύει για "φιλοξενούμενες" (hosted) εικονικές μηχανές για την υποστήριξη προσαρμοσμένων εφαρμογών ή εφαρμογών του Πελάτη.
- Όταν ο Πελάτης έχει αθετήσει οποιεσδήποτε ουσιώδεις συμβατικές υποχρεώσεις.

Παράρτημα Γ

Στο παρόν Παράρτημα Ασφάλειας και Επιχειρησιακής Συνέχειας (Security and Business Continuity Appendix - "Παράρτημα SBCA") ορίζονται ορισμένες απαιτήσεις και υποχρεώσεις της IBM αναφορικά με την παροχή του IBM SaaS στον Πελάτη. Οι απαιτήσεις και υποχρεώσεις που ορίζονται στο παρόν είναι επιπρόσθετες σε εκείνες που ορίζονται στην περιγραφή των αρχών ασφάλειας δεδομένων για IBM SaaS που διατίθεται στην ιστοσελίδα http://www.ibm.com/cloud/data-security. Οι όροι με κεφαλαία γράμματα στην αρχή των λέξεων για τους οποίους δεν παρέχεται ορισμός στο παρόν έχουν τη σημασία που τους αποδίδεται στη Σύμβαση ή στους Όρους Χρήσης.

1. Πρόγραμμα Ασφάλειας Πληροφοριών

Η IBM διαθέτει πολιτικές, πρότυπα και διαδικασίες ασφάλειας που βασίζονται στο πλαίσιο και τις περιοχές ελέγχου του προτύπου ISO 27001. Επιπλέον της διακυβέρνησης που ασκεί ο Οργανισμός Εταιρικής Ασφάλειας της IBM (IBM Corporate Security Organization), οι εν λόγω πολιτικές, πρότυπα και διαδικασίες υπόκεινται σε τακτικούς εσωτερικούς ελέγχους.

Η IBM τηρεί ένα πρόγραμμα ασφάλειας πληροφοριών που ορίζει οργανωτικά, λειτουργικά, διαχειριστικά, φυσικά και τεχνικά προστατευτικά μέτρα που διέπουν την επεξεργασία, αποθήκευση και μετάδοση περιεχομένου του Πελάτη και τα οποία ανταποκρίνονται κατ' ελάχιστο στις απαιτήσεις του παρόντος Παραρτήματος SBCA.

Η IBM θα κοινοποιήσει στον Πελάτη, κατόπιν σχετικού αιτήματος του τελευταίου, πληροφορίες για το πρόγραμμα ασφάλειας πληροφοριών του IBM Watson Health ώστε να μπορεί ο Πελάτης εύλογα να αξιολογήσει την αδιάλειπτη καταλληλότητα, επάρκεια και αποτελεσματικότητα του εν λόγω προγράμματος. Το πρόγραμμα ασφάλειας πληροφοριών του IBM Watson Health θα ενημερώνεται κατά διαστήματα ώστε να ακολουθεί να ανταποκρίνεται στις απαιτήσεις των γενικά αποδεκτών προτύπων του κλάδου και των Νόμων που Ισχύουν για την IBM.

2. Έλεγχοι Πρόσβασης

Η IBM θα αποκαλύπτει περιεχόμενο του Πελάτη μόνο στους υπαλλήλους, υπεργολάβους και τρίτους συνεργάτες της οι οποίοι έχουν μια θεμιτή επιχειρηματική ανάγκη για την πρόσβαση στο εν λόγω περιεχόμενο του Πελάτη προκειμένου να βοηθούν την IBM στην εκπλήρωση των υποχρεώσεών της προς τον Πελάτη ή προς άλλα πρόσωπα αναφορικά με την παροχή του IBM SaaS σύμφωνα με τους Εφαρμοστέους Νόμους, τη Σύμβαση ή ένα Σχετικό Έγγραφο, ανάλογα με την περίπτωση. Σε περίπτωση που η IBM είναι Επιχειρηματικός Εταίρος του Πελάτη, η IBM και ο Πελάτης θα αποκαλύπτουν Προσωπικές Πληροφορίες Υγείας μόνο σύμφωνα με τους όρους μιας ισχύουσας Σύμβασης Επιχειρηματικού Εταίρου μεταξύ των Συμβαλλόμενων Μερών.

Η IBM χρησιμοποιεί μια τυπική, εσωτερική διαδικασία διαχείρισης πρόσβασης χρηστών που επιβάλλει την υποβολή επίσημου αιτήματος για την πρόσβαση ενός χρήστη, το οποίο εγκρίνεται μετά την επαλήθευση της ταυτότητάς του, ενώ το χορηγούμενο επίπεδο πρόσβασης εξαρτάται από τις πληροφορίες που πρέπει να γνωρίζει ο χρήστης και βασίζεται στην αρχή του ελάχιστου απαιτούμενου προνομίου. Η πρόσβαση σε περιεχόμενο του Πελάτη θα περιορίζεται αποκλειστικά σε ενεργούς χρήστες και ενεργούς λογαριασμούς χρηστών. Η IBM έχει μια τυπική διαδικασία για τον περιοδικό εσωτερικό επανέλεγχο της πρόσβασης ενεργών λογαριασμών χρηστών.

Η IBM χρησιμοποιεί ασφαλή πρωτόκολλα ταυτοποίησης χρηστών, τα οποία περιλαμβάνουν τον ορισμό μοναδικών ταυτοτήτων και ισχυρών κωδικών πρόσβασης για ενεργούς λογαριασμούς χρηστών στα συστήματα που χρησιμοποιούνται για την παροχή υπηρεσιών στον Πελάτη σύμφωνα με τα εταιρικά πρότυπα και τις πολιτικές ασφάλειας της IBM:

α. Οι κωδικοί πρόσβασης δεν θα είναι οι προκαθορισμένοι από τον προμηθευτή κωδικοί και θα φυλάσσονται σε μια θέση ή/και μορφή που δεν θέτουν σε κίνδυνο την ασφάλεια των δεδομένων που προστατεύουν.

β. Η εμφάνιση σε οθόνη και η εκτύπωση κωδικών πρόσβασης πρέπει να συγκαλύπτεται, να αποκρύπτεται ή κατά άλλον τρόπο να καταστέλλεται ώστε να μην είναι δυνατή η ανάγνωση ή η μετέπειτα αποκατάστασή τους από μη εξουσιοδοτημένα άτομα. Οι κωδικοί πρόσβασης δεν πρέπει να καταγράφονται ή να αποτυπώνονται κατά την καταχώρησή τους. Οι κωδικοί πρόσβασης των χρηστών δεν πρέπει να αποθηκεύονται σε μη κρυπτογραφημένη ("clear text") μορφή.

γ. Οι κωδικοί πρόσβασης για κάθε τεχνολογία που περιλαμβάνει το IBM SaaS επιλέγονται ώστε να περιορίζουν τους κινδύνους που απορρέουν από γνωστά τρωτά σημεία που σχετίζονται με το μήκος των κωδικών πρόσβασης και πρέπει να είναι τεκμηριωμένοι.

δ. Όταν απαιτείται η χρήση εσωτερικών, προνομιούχων, κοινόχρηστων λειτουργικών ταυτοτήτων για επιχειρησιακούς σκοπούς, η IBM διαχειρίζεται τις εν λόγω κοινόχρηστες, λειτουργικές ταυτότητες ή/και ταυτότητες συστήματος απαιτώντας την ανάληψη ελέγχου (check out) των κωδικών πρόσβασης από τους χρήστες ώστε να εξασφαλίζεται η δυνατότητα απόδοσης προσωπικής ευθύνης.

Καθορίζονται προθεσμίες αδράνειας για όλα τα συστήματα και τις εφαρμογές στις οποίες αποθηκεύεται περιεχόμενο του Πελάτη.

Εάν είναι απαραίτητο, θα επιτραπεί η εξ αποστάσεως πρόσβαση στο δίκτυο, στα συστήματα και στις εφαρμογές της IBM όπου αποθηκεύεται περιεχόμενο του Πελάτη, κατόπιν σχετικού αιτήματος του Πελάτη και κατόπιν επίσημης έγκρισης από την IBM, και όλες οι εν λόγω εξ αποστάσεως συνδέσεις θα προστατεύονται μέσω πρωτοκόλλων ισχυρής ταυτοποίησης και κρυπτογράφησης. Οι δραστηριότητες εξ αποστάσεως πρόσβασης θα καταγράφονται και θα παρακολουθούνται.

Στο βαθμό που για την παράδοση του IBM SaaS απαιτείται η εξ αποστάσεως πρόσβαση της IBM σε οποιοδήποτε σύστημα εντός των εσωτερικών δικτύων της IBM, η εν λόγω εξ αποστάσεως πρόσβαση θα πραγματοποιείται αποκλειστικά με χρήση των ασφαλών συστημάτων και πρωτοκόλλων εξ αποστάσεως πρόσβασης και με χρήση των στοιχείων ταυτότητας που παρέχονται από τον Πελάτη στην IBM. Η εξ αποστάσεως πρόσβαση σε δίκτυο του Πελάτη θα πραγματοποιείται μόνο κατόπιν αιτήματος από την IBM και κατόπιν έγκρισης από τον Πελάτη, και σύμφωνα με τις εκάστοτε ισχύουσες πολιτικές του Πελάτη, οι οποίες θα κοινοποιούνται στην IBM εκ των προτέρων. Η χρήση των εσωτερικών δικτύων του Πελάτη από την IBM θα υπόκειται στις πολιτικές χρήσης και ασφάλειας πληροφορικής του Πελάτη, οι οποίες θα κοινοποιούνται στην IBM εκ των προτέρων.

Η IBM εφαρμόζει την αρχή του διαχωρισμού καθηκόντων για τη διαχείριση ασφάλειας, τον έλεγχο πρόσβασης και τη διερεύνηση περιστατικών παραβίασης ασφάλειας.

Η αποθήκευση, "φιλοξενία" και επεξεργασία περιεχομένου του Πελάτη που αφορά συγκεκριμένα στον Πελάτη γίνεται μέσω του λογικού διαχωρισμού του εν λόγω περιεχομένου από το περιεχόμενο άλλων πελατών που εξυπηρετούνται από την IBM. Σε περίπτωση που ο Πελάτης εγκρίνει τη χρήση ενός κοινόχρηστου χώρου εργασίας για την αποθήκευση, φιλοξενία ή επεξεργασία περιεχομένου, η IBM θα έχει θεσπίσει τις απαιτούμενες διαδικασίες και προστατευτικά μέτρα που θα ανταποκρίνεται στις απαιτήσεις που ορίζονται στο παρόν Παράρτημα SBCA και θα είναι σχεδιασμένα για την αποτροπή της μη εξουσιοδοτημένης αποκάλυψης του εν λόγω περιεχομένου του Πελάτη.

Η IBM εφαρμόζει πολιτικές "καθαρού γραφείου" και "καθαρής οθόνης" ώστε να αποφεύγεται η μη εποπτευόμενη έκθεση περιεχομένου του Πελάτη σε οποιονδήποτε δημόσιο χώρο οποιαδήποτε στιγμή.

3. Διαβίβαση και Κρυπτογράφηση

Η IBM θα λαμβάνει τις αναγκαίες προφυλάξεις κατά τη μετάδοση περιεχομένου του Πελάτη (μέσω fax, email, ταχυμεταφοράς κ.ο.κ.) ώστε να εξασφαλίζεται η χρήση των σωστών πληροφοριών επικοινωνίας για τον παραλήπτη και θα κανονίζει εκ των προτέρων την ασφαλή παραλαβή των εν λόγω πληροφοριών από τον σκοπούμενο παραλήπτη.

Η IBM θα χρησιμοποιεί, και θα εξασφαλίζει ότι το Προσωπικό IBM χρησιμοποιεί, πάντοτε τις κατάλληλες μορφές κρυπτογράφησης ή άλλες ασφαλείς τεχνολογίες για την επεξεργασία περιεχομένου του Πελάτη, συμπεριλαμβανομένου της επεξεργασίας που σχετίζεται με τη διαβίβαση, μετάδοση, εξ αποστάσεως πρόσβαση ή αποθήκευση (συμπεριλαμβανομένης εφεδρικής (backup) αποθήκευσης) περιεχομένου του Πελάτη. Για παράδειγμα, η IBM θα κρυπτογραφεί, χρησιμοποιώντας κάποια κατάλληλη πρότυπη τεχνολογία κρυπτογράφησης, όλα τα δεδομένα και αρχεία που περιλαμβάνουν περιεχόμενο του Πελάτη:

α. τα οποία είναι αποθηκευμένα σε φορητούς υπολογιστές και άλλες φορητές συσκευές ή ηλεκτρονικά μέσα της IBM, συμπεριλαμβανομένων ταινιών εφεδρικής αποθήκευσης, κατά τη μεταφορά τους σε μια εξωτερική τοποθεσία αποθήκευσης,

β. τα οποία είναι αποθηκευμένα ή μεταφέρονται από την IBM εκτός των γραφείων και εγκαταστάσεων του Πελάτη και της IBM που προστατεύονται από μέτρα φυσικής ασφάλειας, με την εξαίρεση των έντυπων εγγράφων,

γ. κατά τη μετάδοσή τους μέσω δημόσιων δικτύων από την IBM,

δ. κατά τη διαβίβασή τους από τα συστήματα της IBM στον Πελάτη,

ε. κατά την ασύρματη μετάδοσή τους από την IBM, και

στ. τα οποία είναι αποθηκευμένα από την IBM σε εξυπηρετητές (servers) και βάσεις δεδομένων.

4. Ασφάλεια Δικτύου

Η IBM χρησιμοποιεί εύλογα τις πιο πρόσφατες εκδόσεις λογισμικού ασφάλειας συστημάτων, όπως π.χ. τείχη προστασίας (firewalls), εξυπηρετητές μεσολάβησης (proxies), και τείχη προστασίας και διεπαφές διαδικτυακών εφαρμογών. Το εν λόγω λογισμικό πρέπει να περιλαμβάνει προστασία από επιβλαβή κώδικα και στο βαθμό που είναι ευλόγως εφικτό τις πιο προσφατές επιδιορθώσεις και ορισμούς ιών. Σύμφωνα με τα εταιρικά πρότυπα, θα υπάρχει εγκατεστημένο λογισμικό αντιμετώπισης ιών (antivirus) σε σταθμούς εργασίας, εξυπηρετητές και αντίστοιχα τελικά σημεία όπου είναι τεχνικά εφικτό και η διαχείριση του εν λόγω λογισμικού σύμφωνα με τις εταιρικές πολιτικές θα γίνεται με εσωτερικές λύσεις διαχείρισης.

Η IBM παρακολουθεί το IBM SaaS για τον εντοπισμό και προσδιορισμό περιστατικών ασφάλειας όσο το δυνατό νωρίτερα. Η IBM θα μεριμνά κατ' ελάχιστο για την τήρηση πρότυπων εργαλείων εντοπισμού μη εξουσιοδοτημένης πρόσβασης και διαδικασιών πρόληψης, παρακολούθησης και ανταπόκρισης που έχουν σχεδιαστεί με τέτοιον τρόπο ώστε να εντοπίζουν εσωτερικά και εξωτερικά τρωτά σημεία και κινδύνους που μπορούν να έχουν ως αποτέλεσμα τη μη εξουσιοδοτημένη αποκάλυψη, κατάχρηση, αλλοίωση ή καταστροφή περιεχομένου ή συστημάτων πληροφοριών του Πελάτη που χρησιμοποιούνται για την παράδοση υπηρεσιών στον Πελάτη.

Η IBM θα διαθέτει συνδρομές για υπηρεσίες παροχής πληροφοριών για τρωτά σημεία ή για συμβουλευτικές υπηρεσίες ασφάλειας πληροφοριών και άλλες σχετικές πηγές που παρέχουν ενημερωμένες πληροφορίες για τρωτά σημεία στα συστήματά της. Η IBM διενεργεί τακτικές αξιολογήσεις τρωτών σημείων και εργασίες για τη διόρθωση της λειτουργίας του δικτύου της.

Η IBM παρακολουθεί το IBM SaaS για τον εντοπισμό, τον προσδιορισμό, τον περιορισμό και την επίλυση Περιστατικών Ασφάλειας.

Η IBM ελέγχει τη διαθεσιμότητα, την ακεραιότητα και την αποτελεσματικότητα της υποδομής ασφάλειας δικτύου στην οποία το IBM SaaS καθίσταται διαθέσιμο, μέσω των διαδικασιών διαχείρισης εκδόσεων της IBM.

5. Διαχείριση Περιστατικών και Προειδοποιήσεις

Οι ομάδες εργασίας του IBM Watson Health συνεργάζονται με την Ομάδα Ανταπόκρισης σε Περιστατικά Ασφάλειας στον Κυβερνοχώρο (Cybersecurity Incident Response Team) της IBM, μια διεθνής ομάδα που διαχειρίζεται τη λήψη, τη διερεύνηση και τον εσωτερικό συντονισμό της ανταπόκρισης σε περιστατικά ασφάλειας που σχετίζονται με προσφορές της IBM, εφαρμόζοντας τα απαραίτητα προληπτικά μέτρα για τον περιορισμό ζητημάτων ασφάλειας που σχετίζονται με λογισμικό. Ως "Περιστατικό Ασφάλειας" (Security Incident) ορίζεται η επιτυχής, μη εξουσιοδοτημένη πρόσβαση, χρήση, αποκάλυψη, τροποποίηση ή παρέμβαση σε λειτουργίες ή δεδομένα σε ένα σύστημα πληροφοριών που χρησιμοποιείται από την IBM για την παροχή του IBM SaaS. Όταν αποκαλυφθεί ένα Περιστατικό Ασφάλειας (μέσω μιας προγραμματισμένης διαδικασίας σάρωσης, με την εμφάνιση ενός προειδοποιητικού σήματος, εξαιτίας της υπέρβασης ενός καθορισμένου ορίου κ.ο.κ.), η IBM θα ενημερώνει και θα ειδοποιεί τον Πελάτη:

α. για οποιοδήποτε επιβεβαιωμένο Περιστατικό Ασφάλειας που αφορά περιεχόμενο του Πελάτη το συντομότερο δυνατό και όχι αργότερα από 2 εργάσιμες ημέρες από τη διερεύνηση και επιβεβαίωση του εν λόγω Περιστατικού Ασφάλειας,

β. ανταποκρινόμενη άμεσα σε οποιοδήποτε αίτημα πρόσβασης ή παροχής πληροφοριών για οποιοδήποτε περιεχόμενο του Πελάτη από οποιαδήποτε κυβερνητική αρχή (συμπεριλαμβανομένης οποιασδήποτε υπηρεσίας προστασίας δεδομένων ή διωκτικής αρχής), εκτός εάν αυτό απαγορεύεται από το νόμο ή σχετικό ένταλμα, και

γ. με την εξαίρεση των περιπτώσεων που επιτρέπονται στο άρθρο Έλεγχοι Πρόσβασης του παρόντος Παραρτήματος SBCA, πριν από οποιαδήποτε αποκάλυψη ή διαβίβαση περιεχομένου του Πελάτη σε τρίτο μέρος, ή πριν από την πρόσβαση σε περιεχόμενο του Πελάτη από τρίτο μέρος.

6. Καταγραφή Δραστηριοτήτων

Η IBM μεριμνά, σύμφωνα με τις πολιτικές και πρακτικές της IBM και τις γενικά αποδεκτές πρακτικές που προβλέπονται από τα πρότυπα του κλάδου, για την εύλογη παρακολούθηση των συστημάτων της για τον εντοπισμό περιπτώσεων μη εξουσιοδοτημένης χρήσης ή πρόσβασης σε Επεξεργασμένα Δεδομένα του Πελάτη. Οποιεσδήποτε πραγματικές ή επιχειρούμενες παραβιάσεις σύνδεσης και πρόσβασης θα καταγράφονται.

Η IBM τηρεί στοιχεία για όλα τα αιτήματα πρόσβασης και αρχεία καταγραφής όλων των δραστηριοτήτων πρόσβασης για όλα τα συστήματα στα οποία γίνεται επεξεργασία, πρόσβαση, επεξεργασία και μετάδοση περιεχομένου του Πελάτη και Δεδομένων Υγείας για όσο χρονικό διάστημα απαιτείται από το Νόμο HIPA και τους άλλους Νόμους περί Προστασίας Δεδομένων που Ισχύουν για την IBM.

Στα αρχεία καταγραφής και τις αναφορές περιλαμβάνονται, κατ' ελάχιστο, τα ακόλουθα στοιχεία: (i) πληροφορίες για όλες τις προσπάθειες σύνδεσης, επιτυχείς και μη, συμπεριλαμβανομένων εύλογων πληροφοριών ταυτότητας, (ii) πληροφορίες για όλες τις αλλαγές στην παραμετροποίηση συστημάτων και δικτύου, συμπεριλαμβανομένων πληροφοριών για την εγκατάσταση εφαρμογών και αλλαγές στη διαχείριση χρηστών και στα δικαιώματα πρόσβασης σε αρχεία, (iii) πληροφορίες για προσπάθειες πρόσβασης σε πόρους, επιτυχείς και μη, συμπεριλαμβανομένων προσπαθειών πρόσβασης σε οποιοδήποτε αρχείο, κοινόχρηστη μονάδα δικτύου, αρχείο καταγραφής ή άλλο πόρο του συστήματος, και (iv) πληροφορίες για δραστηριότητες μεταφόρτωσης (download) δεδομένων, συμπεριλαμβανομένων πληροφοριών για το είδος δεδομένων και το πρωτόκολλο πρόσβασης που χρησιμοποιήθηκε για την επίτευξη της μεταφόρτωσης.

7. Ανάπτυξη Εφαρμογών Λογισμικού και Διαχείριση Αλλαγών

Η IBM ακολουθεί ασφαλείς πρακτικές ανάπτυξης και κωδικοποίησης εφαρμογών που προστατεύουν την ακεραιότητα εφαρμογών στο περιβάλλον παραγωγής και του αντίστοιχου πηγαίου κώδικα από μη εξουσιοδοτημένη και μη δοκιμασμένη τροποποίηση.

Η IBM ακολουθεί μια διαδικασία διαχείρισης αλλαγών που περιλαμβάνει (α) την καταγραφή και επίσημη έγκριση αλλαγών και τα απαιτούμενα βήματα για την αναίρεση αλλαγών, και (β) την επαρκή δοκιμή των εν λόγω αλλαγών, συμπεριλαμβανομένων δοκιμών αποδοχής από τους χρήστες, όπου απαιτείται, και δοκιμών ασφάλειας.

Η IBM ακολουθεί μια διαδικασία διαχείρισης επιδιορθώσεων που περιλαμβάνει τη δοκιμή επιδιορθώσεων (patches) πριν την εγκατάστασή τους σε όλα τα συστήματα που χρησιμοποιούνται για την αποθήκευση, πρόσβαση και μετάδοση περιεχομένου του Πελάτη ή για την παράδοση υπηρεσιών, συμπεριλαμβανομένου του IBM SaaS, στον Πελάτη.

Η IBM απαιτεί από τους διαχειριστές συστημάτων να τηρούν πλήρεις, ακριβείς και ενημερωμένες πληροφορίες για την παραμετροποίηση όλων των συστημάτων πληροφοριών που χρησιμοποιούνται για την αποθήκευση, πρόσβαση και μετάδοση περιεχομένου του Πελάτη.

8. Φυσική και Περιβαλλοντική Ασφάλεια

Η πλατφόρμα IBM Watson Health Core εγκαθίσταται στην υποδομή δεδομένων του IBM SoftLayer. Το IBM SoftLayer μεριμνά για τη διατήρηση της φυσικής και περιβαλλοντικής ασφάλειας, του ελέγχου πρόσβασης, και των ελέγχων και διαδικασιών για την προστασία του Πελάτη από ανθρώπινες, περιβαλλοντικές και τεχνικές παραβιάσεις ή επιπτώσεις.

Η γενική πρόσβαση στις κτιριακές εγκαταστάσεις όπου "φιλοξενείται" το IBM SaaS ελέγχεται με τη χρήση ενός συστήματος πρόσβασης μέσω καρτών. Στις εγκαταστάσεις έχουν τοποθετηθεί κάμερες κλειστού συστήματος τηλεόρασης (CCTV) οι οποίες παρακολουθούνται από προσωπικό ασφάλειας. Επιλεγμένες θύρες πρόσβασης προστατεύονται με συστήματα συναγερμού τα οποία παρακολουθούνται από προσωπικό ασφάλειας.

Η πρόσβαση στις ελεγχόμενες περιοχές περιορίζεται με τη χρήση μιας κάρτας ή/και την πρόσθετη βιομετρική εξακρίβωση. Όλα τα άτομα χωρίς εξουσιοδοτημένη πρόσβαση στις ελεγχόμενες περιοχές πρέπει να υπογράφουν κατά την είσοδό τους στην περιοχή και να συνοδεύονται από κάποιο άτομο του οποίου έχει εγκριθεί η πρόσβαση στην εν λόγω ελεγχόμενη περιοχή. Όλες οι έξοδοι κινδύνου των ελεγχόμενων περιοχών έχουν συστήματα ηχητικού συναγερμού τα οποία παρακολουθούνται από προσωπικό ασφαλείας. Πραγματοποιείται περιοδικός έλεγχος της σωστής λειτουργίας των συστημάτων συναγερμού. Τα αποτελέσματα των εν λόγω ελέγχων τεκμηριώνονται και φυλάσσονται. Σε τριμηνιαία βάση γίνεται εκ νέου επικύρωση όλων των δικαιωμάτων πρόσβασης στις ελεγχόμενες περιοχές. Το δικαίωμα πρόσβασης ενός υπαλλήλου στις ελεγχόμενες περιοχές ανακαλείται με τη λήξη της απασχόλησής του.

Οι κτιριακές εγκαταστάσεις προστατεύονται από περιβαλλοντικούς παράγοντες όπως φωτιά, νερό και θερμότητα μέσω συστημάτων συναγερμού φωτιάς, πυροσβεστήρων, συστημάτων ανίχνευσης καπνού και συστημάτων καταστολής και κατάσβεσης φωτιάς. Οι κτιριακές εγκαταστάσεις προστατεύονται από διακοπές ή βλάβες στην ηλεκτροδότηση μέσω συστημάτων αδιάλειπτης τροφοδοσίας (UPS) και εφεδρικών γεννητριών, οι οποίες συντηρούνται και ελέγχονται σε τακτικά χρονικά διαστήματα.

Για πληροφορίες και αναφορές σχετικά με τη συμμόρφωση του IBM SoftLayer, ανατρέξτε στην ιστοσελίδα: http://www.softlayer.com/compliance.

9. Συνέχεια Επιχειρησιακών Λειτουργιών

Η IBM διαθέτει σχέδια επιχειρησιακής συνέχειας και αποκατάστασης μετά από καταστροφή που έχουν σχεδιαστεί για την εξασφάλιση ενός επιπέδου παροχής υπηρεσιών που ανταποκρίνεται στις υποχρεώσεις της IBM βάσει της Σύμβασης. Τα εν λόγω σχέδια επιχειρησιακής συνέχειας και αποκατάστασης μετά από καταστροφή θα ενημερώνονται και θα δοκιμάζονται σε περιοδική βάση (τουλάχιστον μία φορά ετησίως). Η IBM θα εφαρμόζει όλες τις εύλογες αλλαγές στα σχέδια επιχειρησιακής συνέχειας και αποκατάστασης μετά από καταστροφή που είναι απαραίτητες προκειμένου να συνεχίζει να συμμορφώνεται με τις γενικά αποδεκτές πρακτικές του κλάδου, σε κάθε περίπτωση χωρίς να παρεμβαίνει χωρίς εύλογη αιτία στη λειτουργία του IBM SaaS ή του περιβάλλοντος παραγωγής που χρησιμοποιείται από τον Πελάτη.

Σε περίπτωση που προκύψει μια καταστροφή που καθιστά το IBM SaaS μη διαθέσιμο στον Πελάτη, η IBM θα ειδοποιήσει άμεσα τον Πελάτη και θα θέσει σε εφαρμογή το σχέδιο επιχειρησιακής συνέχειας ή/και αποκατάστασης μετά από καταστροφή. Όταν δηλωθεί μια καταστροφή, ο στόχος για την επιχειρησιακή συνέχεια του IBM SaaS είναι να αποκατασταθεί η πρόσβαση του Πελάτη στο IBM SaaS ως εξής: σε περίπτωση διακοπής λειτουργίας, ο Στόχος για το Χρόνο Αποκατάστασης (RTO) για την αποκατάσταση του περιβάλλοντος παραγωγής του IBM Watson Health είναι εντός 36 ωρών από τη δήλωση της καταστροφής. Ο Στόχος για το Σημείο Αποκατάστασης (RPO) είναι ότι η μέγιστη απώλεια περιεχομένου του Πελάτη στο περιβάλλον παραγωγής είναι 24 ώρες. Οι στόχοι για την επιχειρησιακή συνέχεια συγκεκριμένων λύσεων Watson Health μπορεί να διαφέρουν.

Η προσέγγιση της IBM για την αποκατάσταση μετά από καταστροφή συνίσταται στη λειτουργία διαφορετικών κέντρων πληροφοριακών συστημάτων σε διαφορετικές γεωγραφικές περιοχές.

Όλα τα κέντρα πληροφοριακών συστημάτων του IBM SoftLayer διαθέτουν περισσότερες από μία παροχές ρεύματος, συνδέσεις οπτικών ινών, γεννήτριες αποκλειστικής χρήσης και μπαταρίες εφεδρικής υποστήριξης. Διαθέτουν κορυφαίας ποιότητας υλικό εξοπλισμό, παρέχοντας τα υψηλότερα δυνατά επίπεδα απόδοσης, αξιοπιστίας και διαλειτουργικότητας. Όλες οι μονάδες των κέντρων πληροφοριακών συστημάτων που διαθέτουν παράλληλη εφεδρική υποστήριξη τροφοδοσίας (n+1) και μονάδες ψύξης ελέγχονται τακτικά ώστε να εξασφαλίζεται η σταθερή τους λειτουργία.

10. Συμμόρφωση

Οι πρακτικές ασφάλειας της IBM βασίζονται στα πρότυπα ISO 27001-27002. Οι πρακτικές αυτές παρέχουν τις απαιτούμενες ελεγκτικές δομές, ενδεικτικά και όχι περιοριστικά, για την Ανάλυση Κινδύνων, τη Φυσική Ασφάλεια, το Σχεδιασμό της Αντιμετώπισης Εκτάκτων Καταστάσεων, τη Διενέργεια Ερευνών, την Προστασία Πληροφοριών, τις Δραστηριότητες Εκπαίδευσης, την Προστασία Δεδομένων και τις Επιχειρησιακές Λειτουργίες.

Η IBM ελέγχει τη συμμόρφωση των δραστηριοτήτων της στον τομέα της ασφάλειας και της προστασίας δεδομένων προσωπικού χαρακτήρα με τις πρακτικές ασφάλειάς της.

Η IBM συμμορφώνεται με τους Νόμους περί Προστασίας Δεδομένων που Ισχύουν για την IBM στις Εντός Εμβέλειας Δικαιοδοσίες.

Ο κατάλληλος χειρισμός εμπιστευτικών πληροφοριών των Πελατών επιβάλλεται επίσης από τις Κατευθυντήριες Αρχές Επιχειρηματικής Συμπεριφοράς (Business Conduct Guidelines) της IBM, τις οποίες πρέπει να διαβάσουν όλοι οι υπάλληλοι της IBM σε ετήσια βάση (και να πιστοποιήσουν τη συμμόρφωσή τους με αυτές).

11. Λοιπές Διατάξεις

Η IBM θα διασφαλίζει ότι οι συμβάσεις της με όλους τους υπεργολάβους ή/και τρίτους που συμμετέχουν στην παράδοση του IBM SaaS περιλαμβάνουν όρους που παρέχουν κατ' ελάχιστο το ίδιο επίπεδο προστασίας για το περιεχόμενο του Πελάτη με τους όρους του παρόντος Παραρτήματος SBCA και οποιουδήποτε Σχετικού Εγγράφου, στο βαθμό που οι εν λόγω όροι διέπουν τις υπηρεσίες που θα παρέχονται από τους εν λόγω υπεργολάβους ή/και τρίτους.

Σημαντικό: Οι παρόντες Όροι Χρήσης συντάχθηκαν στην αγγλική γλώσσα. Μπορείτε να βρείτε και να εκτυπώσετε αντίγραφο των παρόντων Όρων Χρήσης στην αγγλική από την εξής ιστοσελίδα:

http://www-03.ibm.com/software/sla/sladb.nsf/sla/saas

Η ελληνική μετάφραση παρέχεται μόνο για λόγους διευκόλυνσης. Σε περίπτωση ασυμφωνίας μεταξύ του αγγλικού κειμένου και της ελληνικής του μετάφρασης, το αγγλικό κείμενο υπερισχύει. Εάν για οποιονδήποτε λόγο δεν έχετε πρόσβαση στο αγγλικό κείμενο, παρακαλούμε όπως επικοινωνήσετε με τον τοπικό εκπρόσωπο της IBM προκειμένου να σας το αποστείλουμε άμεσα.