| ATC | Principio attivo | NOTE |
|---|---|---|
| A10AE04 | INSULINA GLARGINE | |
| A10AE05 | INSULINA DETEMIR | |
| A10AE06 | INSULINA DEGLUDEC | |
| **A10AE54** | **INSULINA GLARGINE + EXENATIDE** | |
| **A10AE56** | **INSULINA DEGLUDEC + LIRAGLUTIDE** | |
| A10BD05 | METFORMINA E PIOGLITAZONE | |
| A10BD06 | GLIMEPRIDE E PIOGLITAZONE | |
| A10BD07 | METFORMINA E SITAGLIPTIN | |
| A10BD08 | METFORMINA E VILDAGLIPTIN | |
| A10BD09 | PIOGLITAZONE E ALOGLIPTIN | |
| A10BD10 | METFORMINA E SAXAGLIPTIN | |
| A10BD11 | METFORMINA E LINAGLIPTIN | |
| A10BD13 | METFORMINA E ALOGLIPTIN | |
| A10BD15 | METFORMINA E DAPAGLIFLOZIN | |
| A10BD16 | CANAGLIFOZIN EMIDRATO/METFORMINA CLORIDRATO | |
| A10BD20 | EMPAGLIFLOZIN/METFORMINA | |
| A10BH01 | SITAGLIPTIN | |
| A10BH02 | VILDAGLIPTIN | |
| A10BH03 | SAXAGLIPTIN | |
| A10BH04 | ALOGLIPTIN | |
| A10BH05 | LINAGLIPTIN | |
| A10BJ01 | EXENATIDE | |
| A10BJ02 | LIRAGLUTIDE | |
| A10BJ03 | LIXISENATIDE | |
| A10BK01 | DAPAGLIFLOZIN | |
| A10BJ05 | DULAGLUTIDE | |
| A10BK02 | CANAGLIFLOZIN | |
| A10BK03 | EMPAGLIFLOZIN | |
| A16AA01 | LEVOCARNITINA | |
| B01AB05 | ENOXAPARINA | Indicazione autorizzata all'impiego in PHT delle EBPM (e quindi in DPC) è la seguente. "Profilassi della TVP dopo intervento di chirurgia generale maggiore e dopo intervento ortopedico |
| B01AB06 | NADROPARINA | |
| B01AB07 | PARNAPARINA | |
| B01AB12 | BEMIPARINA | |
| B01AC22 | PRASUGREL | |
| B01AC24 | TICAGRELOR | |
| B01AC30 | ASSOCIAZIONI (CLOPIDOGREL+ASA) | |
| B01AE07 | DABIGATRAN ETEXILATO | |
| B01AF01 | RIVAROXABAN | |
| B01AF02 | APIXABAN | |
| B01AF03 | EDOXABAN TOSILATO | |
| B01AX05 | FONDAPARINUX | |
| **B03XA01** | **ERITROPOIETINA** | |
| B03XA02 | DARBEPOETINA ALFA | |
| **B03XA03** | **METOSSIPOLIETINGLICOLE EPOETINA BETA** | |
| C01BD07 | DRONEDARONE | |
| **C01EB17** | **IVABRADINA** | |

| ATC | Principio attivo | NOTE |
|---|---|---|
| C01EB18 | RANOLAZINA | |
| D06BB10 | IMIQUIMOD | |
| **D11AH01** | **TACROLIMUS** | |
| **G03BA03** | **TESTOSTERONE** | Solo gel |
| G03GA02 | GONADOTROPINA UMANA DELLA MENOPAUSA (MENOTROPINA) | |
| G03GA04 | UROFOLLITROPINA | |
| G03GA05 | FOLLITROPINA ALFA | |
| G03GA06 | FOLLITROPINA BETA | |
| G03GA07 | LUTROPINA ALFA | |
| G03GA08 | CORIOGONADOTROPINA ALFA | |
| G03GA09 | CORIFOLLITROPINA ALFA | |
| G03GA30 | ASSOCIAZIONI (FOLLITROPINA ALFA+LUTROPINA ALFA) | |
| G03XB02 | ULIPRISTAL | |
| H01AX01 | PEGVISOMANT | |
| H01BA02 | DESMOPRESSINA | |
| H01CA01 | GONADORELINA | |
| H01CB02 | OCTREOTIDE | |
| H01CB03 | LANREOTIDE | |
| H01CB05 | PASIREOTIDE | |
| H05BX01 | CINACALCET | |
| H05BX02 | PARACALCITOLO | |
| J05AP01 | RIBAVIRINA | |
| J05AB11 | VALACICLOVIR | |
| J05AB14 | VALGANCICLOVIR | |
| L01XX14 | TRETINOINA | |
| L02AE01 | BUSERELINA | |
| L02AE02 | LEUPRORELINA | |
| L02AE03 | GOSERELIN | |
| L02AE04 | TRIPTORELINA | |
| L02BB03 | BICALUTAMIDE | |
| L02BX02 | DEGARELIX | |
| **L03AA02** | **FILGRASTIM** | |
| L03AA10 | LENOGRASTIM | |
| L03AA13 | PEGFILGRASTIM | |
| L03AA14 | LIPEGFILGRASTIM | |
| L03AB04 | INTERFERONA ALFA-2A | |
| L03AB05 | INTERFERONE ALFA-2B | |
| L03AB10 | PEGINTERFERONE ALFA-2B | |
| L03AB11 | PEGINTERFERONE ALFA-2A | |
| L04AA06 | MICOFENOLATO MOFETILE | |
| L04AA10 | SIROLIMUS | |
| L04AA13 | LEFLUNOMIDE | |
| L04AA18 | EVEROLIMUS | |
| L04AD02 | TACROLIMUS | |
| M05BX04 | DENOSUMAB | |
| N03AF04 | ESLICARBAZEPINA | |
| N03AX22 | PERAMPANEL | |

| ATC | Principio attivo | NOTE |
|---|---|---|
| N04BA03 | INIBITORI DELLA DECARBOSSILASI E INIBITORI DELLA COMT | |
| N04BX01 | TOLCAPONE | |
| N04BX02 | ENTACAPONE | |
| N05AE04 | ZIPRASIDONE | |
| N05AH05 | ASENAPINA | |
| N05AX08 | RISPERIDONE | |
| N05AX12 | ARIPIPRAZOLO | |
| N05AX13 | PALIPERIDONE | |
| N06BA07 | MODAFINIL | |
| N06BA09 | ATOMOXETINA | |
| **N06DA02** | **DONEPEZIL** | |
| N06DA03 | RIVASTIGMINA | |
| **N06DA04** | **GALANTAMINA** | |
| N06DX01 | MEMANTINA | |
| N07BB03 | ACAMPROSATO | |
| **N07BB04** | **NALTREXONE** | |
| P01CX01 | PENTAMIDINA ISETIONATO | |
| R03DX05 | OMALIZUMAB | |
| R03DX07 | ROFLUMILAST | |
| R03DX09 | MEPOLIZUMAB | |
| V03AC01 | DEFEROXAMINA | |
| V03AE02 | SEVELAMER | |
| V03AE03 | LANTANIO CARBONATO | |
| V03AF01 | MESNA | |

In grassetto i principi attivi in via di aggiudicazione per dosaggio mancante o intero principio attivo

All. 2

| ATC | Descrizione | NOTA AIFA | Tipologia di PIANO TERAPEUTICO | PRESCRIVIBILITA' |
|---|---|---|---|---|
| A | Apparato Gastrointestinale e metabolismo | | | |
| A10A | INSULINE ED ANALOGHI | | | |
| A10AE | Insuline ed analoghi iniettabili ad azione lenta | | | |
| A10AE06 | INSULINA DEGLUDEC | | Template Insulina Degludec | Strutt. diabetologiche osp. o terr. del SSN |
| A10B | IPOGLICEMIZZANTI, ESCLUSE LE INSULINE | | | |
| A10BD | Associazioni di antidiabetici orali | | | |
| A10BD07 | METFORMINA E SITAGLIPTIN | | Antidiabetici orali (incretine) | Strutt. diabetologiche osp. o terr. del SSN |
| A10BD08 | METFORMINA E VILDAGLIPTIN | | Antidiabetici orali (incretine) | Strutt. diabetologiche osp. o terr. del SSN |
| A10BD09 | PIOGLITAZONE E ALOGLIPTIN | | Antidiabetici orali (incretine) | Strutt. diabetologiche osp. o terr. del SSN |
| A10BD10 | METFORMINA E SAXAGLIPTIN | | Antidiabetici orali (incretine) | Strutt. diabetologiche osp. o terr. del SSN |
| A10BD11 | METFORMINA E LINAGLIPTIN | | Antidiabetici orali (incretine) | Strutt. diabetologiche osp. o terr. del SSN |
| A10BD13 | METFORMINA E ALOGLIPTIN | | Antidiabetici orali (incretine) | Strutt. diabetologiche osp. o terr. del SSN |
| A10BD15 | METFORMINA E DAPAGLIFLOZIN | | Antidiabetici orali Dapaglifozin | Strutt. diabetologiche osp. o terr. del SSN |
| A10BD16 | METFORMINA E CANAGLIFLOZIN | | Antidiabetici orali Canagliflozin | Strutt. diabetologiche osp. o terr. del SSN |
| A10BD20 | METFORMINA E EMPAGLIFLOZIN | | Antidiabetici orali Empagliflozin | Strutt. diabetologiche osp. o terr. del SSN |
| A10BH | Inibitori della dipeptidil peptidasi 4 (DPP-4) | | | |
| A10BH01 | SITAGLIPTIN | | Antidiabetici orali (incretine) | Strutt. diabetologiche osp. o terr. del SSN |
| A10BH02 | VILDAGLIPTIN | | Antidiabetici orali (incretine) | Strutt. diabetologiche osp. o terr. del SSN |
| A10BH03 | SAXAGLIPTIN | | Antidiabetici orali (incretine) | Strutt. diabetologiche osp. o terr. del SSN |
| A10BH04 | ALOGLIPTIN | | Antidiabetici orali (incretine) | Strutt. diabetologiche osp. o terr. del SSN |
| A10BH05 | LINAGLIPTIN | | Antidiabetici orali (incretine) | Strutt. diabetologiche osp. o terr. del SSN |
| A10BJ | Analoghi del recettore GLP-1 | | | |
| A10BJ01 | EXENATIDE | | Antidiabetici orali (incretine) | Strutt. diabetologiche osp. o terr. del SSN |
| A10BJ02 | LIRAGLUTIDE | | Antidiabetici orali (incretine) | Strutt. diabetologiche osp. o terr. del SSN |
| A10BJ03 | LIXISENATIDE | | Antidiabetici orali (incretine) | Strutt. diabetologiche osp. o terr. del SSN |
| A10BJ05 | DULAGLUTIDE | | Antidiabetici orali (incretine) | Strutt. diabetologiche osp. o terr. del SSN |
| A10BK | Inibitori del cotrasportatore SGLT2 | | | |
| A10BK01 | DAPAGLIFLOZIN | | Antidiabetici orali Dapaglifozin | Strutt. diabetologiche osp. o terr. del SSN |
| A10BK02 | CANAGLIFLOZIN | | Antidiabetici orali Canagliflozin | Strutt. diabetologiche osp. o terr. del SSN |
| A10BK03 | EMPAGLIFLOZIN | | Antidiabetici orali Empagliflozin | Strutt. diabetologiche osp. o terr. del SSN |
| A16A | ALTRI FARMACI DELL'APPARATO GASTROINTESTINALE E DEL METABOLISMO | | | |
| A16AA | Aminoacidi e derivati | | | |
| A16AA01 | LEVOCARNITINA per carenza primaria di carnitina | 8 | PT generale | Cardiologia, Medicina |
| A16AA01 | LEVOCARNITINA per carenza secondaria di carnitina | 8 | PT generale | Nefrologia e Dialisi |
| B | Sangue ed organi emopoietici | | | |
| B01A | ANTITROMBOTICI | | | |
| B01AC | Antiaggreganti piastrinici esclusa l'eparina | | | |
| B01AC22 | PRASUGREL | | Template Prasugrel | Strutt. cardiologiche osp. e terr.del SSN |
| B01AC24 | TICAGRELOR 60 mg | | Template Ticagrelor 60 | Strutt. cardiologiche osp. e terr.del SSN |
| B01AC24 | TICAGRELOR 90 mg | | Template Ticagrelor 90 | Strutt. cardiologiche osp. e terr.del SSN |
| B01AE | Inibitori diretti della trombina | | | |
| B01AE07 | DABIGATRAN ETEXILATO MESILATO (dosaggio 110 mg e 150 mg) | | PT AIFA web | elenco centri allegato NAO (DA REGISTRI DI MONITORAGGIO AIFA) |
| B01AF | Inibitori diretti del fattore Xa | | | |
| B01AF01 | RIVAROXABAN (dosaggio 15 mg e 20 mg) | | PT AIFA web | elenco centri allegato NAO (DA REGISTRI DI MONITORAGGIO AIFA) |
| B01AF02 | APIXABAN | | PT AIFA web | |
| B01AF03 | EDOXABAN | | PT AIFA web | |
| B03X | ALTRI PREPARATI ANTIANEMICI | | | |
| B03XA | Altri preparati antianemici | | | |
| B03XA01 | EPOETINA alfa | | Template EPO ex Nota 12 | Ematologia, Nefrologia, Medicina, Geriatria, Oncologia, Cardiochirurgia, Emodialisi, Pediatra, Chirurgia, Pneumologia, Centro trapianti |
| B03XA01 | EPOETINA beta | | Template EPO ex Nota 12 | Ematologia, Nefrologia, Medicina, Geriatria, Oncologia, Cardiochirurgia, Emodialisi, Pediatra, Chirurgia, Pneumologia, Centro trapianti |

| ATC | Descrizione | NOTA AIFA | Tipologia di PIANO TERAPEUTICO | PRESCRIVIBILITA' |
|---|---|---|---|---|
| B03XA01 | EPOETINA zeta | | Template EPO ex Nota 12 | Ematologia, Nefrologia, Medicina, Geriatria, Oncologia, Cardiochirurgia, Emodialisi, Pediatra, Chirurgia, Pneumologia, Centro trapianti |
| B03XA01 | EPOETINA teta | | Template EPO ex Nota 12 | Ematologia, Nefrologia, Medicina, Geriatria, Oncologia, Cardiochirurgia, Emodialisi, Pediatra, Chirurgia, Pneumologia, Centro trapianti |
| B03XA02 | DARBEPOETINA ALFA | | Template EPO ex Nota 12 | Ematologia, Nefrologia, Medicina, Geriatria, Oncologia, Cardiochirurgia, Emodialisi, Pediatra, Chirurgia, Pneumologia, Centro trapianti |
| B03XA03 | METOSSIPOLIETILENGLICOLE-EPOETINA BETA | | Template EPO ex Nota 12 | Ematologia, Nefrologia, Medicina, Geriatria, Oncologia, Cardiochirurgia, Emodialisi, Pediatra, Chirurgia, Pneumologia, Centro trapianti |
| **C** | **Apparato cardiovascolare** | | | |
| **C01BD** | **Antiaritmici, classe III** | | | |
| C01BD07 | DRONEDARONE | | Template dronedarone | Strutt. cardiologiche osp. e terr. del SSN, medicina interna, geriatria del SSN |
| **D** | **Dermatologici** | | | |
| **D06BB** | **Antivirali** | | | |
| D06BB10 | IMIQUOD | | Template imiquod | Strutt. oncologiche e dermatologiche osp. e terr. del SSN |
| **D11AH** | **Agenti per dermatiti, esclusi corticosteroidi** | | | |
| D11AH01 | TACROLIMUS | | PT generale | Strutt. dermatologiche, allergologiche e pediatriche osp. e terr. del SSN |
| **G** | **Sistema genito-urinario ed ormoni sessuali** | | | |
| **G03BA** | **Derivati del 3-OXOANDROSTENE (4)** | | | |
| G03BA03 | TESTOSTERONE | 36 | PT generale | Strutt. endocrinologiche, urologiche e pediatriche osp. e terr. del SSN |
| **G03G** | **GONADOTROPINE ED ALTRI STIMOLANTI DELL'OVULAZIONE** | | | |
| **G03GA** | **Gonadotropine** | | | |
| G03GA02 | MENOTROPINA | 74 | PT generale | UU.OO. Di Ginecologia (Pubbliche e Private Convenzionate da Registro Nazionale PMA), Centri per il trattamento dell'infertilità ad esse annessi, UU.OO. Di Urologia del SSN |
| G03GA04 | UROFOLLITROPINA | 74 | PT generale | |
| G03GA05 | FOLLITROPINA ALFA | 74 | PT generale | |
| G03GA06 | FOLLITROPINA BETA | 74 | PT generale | |
| G03GA07 | LUTROPINA ALFA | 74 | PT generale | UU.OO. Di Ginecologia (Pubbliche e Private Convenzionate da Registro Nazionale PMA), Centri per il trattamento dell'infertilità ad esse annessi del SSN |
| G03GA08 | CORIOGONADOTROPINA ALFA | 74 | PT generale | |
| G03GA09 | CORIFOLLITROPINA ALFA | 74 | PT generale | |
| G03GA99 | FOLLITROPINA ALFA, LUTROPINA ALFA | 74 | PT generale | |
| **G03X** | **ALTRI ORMONI SESSUALI E MODULATORI DEL S.G.** | | | |
| **G03XB** | **Modulatori dei recettori del progesterone** | | | |
| G03XB02 | ULIPRISTAL ACETATO | 51 | PT generale | Strutt. ginecologiche osp. e terr. del SSN |
| **H** | **Preparati ormonali sistemici, esclusi gli ormoni sessuali** | | | |
| **H01B** | **ORMONI DEL LOBO POSTERIORE DELL'IPOFISI** | | | |
| **H01BA** | **Vasopressina e analoghi** | | | |
| H01BA02 | DESMOPRESSINA fiale | | PT generale | Ematologia ed Emodialisi |
| **H01C** | **ORMONI IPOTALAMICI** | | | |

| ATC | Descrizione | NOTA AIFA | Tipologia di PIANO TERAPEUTICO | PRESCRIVIBILITA' |
|---|---|---|---|---|
| **H01CA** | **Ormoni liberatori delle gonadotropine** | | | |
| H01CA01 | GONADORELINA | | PT generale | Endocrinologia, Ginecologia-Ostetricia, Pediatria e Urologia |
| **H01CB** | **Somatostatina ed analoghi** | | | |
| H01CB02 | OCTREOTIDE | | PT generale | Endocrinologia, Gastroenterologia, Oncologia, Medicina nucleare, Medicina, Pediatria |
| H01CB03 | LANREOTIDE | | PT generale | Endocrinologia, Gastroenterologia, Oncologia, Medicina nucleare, Medicina, Pediatria |
| **H05B** | **SOSTANZE ANTIPARATIROIDEE** | | | |
| **H05BX** | **Altri preparati antiparatiroidei** | | | |
| H05BX01 | CINACALCET | | PT generale | Endocrinologia, Nefrologia e dialisi, Oncologia |
| H05BX02 | PARACALCITOLO | | PT generale | Endocrinologia, Nefrologia e dialisi, Oncologia |
| **J** | **Antiinfettivi generali per uso sistemico** | | | |
| **J05A** | **ANTIVIRALI AD AZIONE DIRETTA** | | | |
| **J05AB** | **Nucleosidi e nucleotidi, esclusi gli inibitori della transcrittasi inversa** | | | |
| J05AB14 | VALGANCICLOVIR | 84 | PT generale | Centri trapianti, Malattie infettive |
| **L** | **Farmaci antineoplastici ed immunomodulatori** | | | |
| **L01X** | **ALTRI ANTINEOPLASTICI** | | | |
| **L01XX** | **Altri antineoplastici** | | | |
| L01XX14 | TRETINOINA | | PT generale | Centro Trapianti, Ematologia, Oncologia e Pediatria |
| **L02A** | **ORMONI E SOSTANZE CORRELATE** | | | |
| **L02AE** | **Analoghi dell'ormone liberatore delle gonadotropine** | | | |
| L02AE01 | BUSERELINA | 51 | PT generale | Endocrinologia, Oncologia, Urologia |
| L02AE02 | LEUPRORELINA | 51 | PT generale | Strutt. Ospe e Terr. Endocrinologia, Pediatria, Ginecologia-ostetricia, Oncologia, Chirurgia, Radioterapia, Medicina del SSN |
| L02AE03 | GOSERELINA | 51 | PT generale | |
| L02AE04 | TRIPTORELINA | 51 | PT generale | |
| **L02B** | **ANTAGONISTI ORMONALI E SOSTANZE CORRELATE** | | | |
| **L02BX** | **Altri antagonisti ormonali e sostanze correlate** | | | |
| L02BX02 | DEGARELIX | | PT generale | Endocrinologia, Oncologia, Radioterapia,Urologia |
| **L03A** | **IMMUNOSTIMOLANTI** | | | |
| **L03AA** | **Fattori di stimolazione delle colonie** | | | |
| L03AA02 | FILGRASTIM | | Template fattori di crescita | Oncologia, Ematologia, Radioterapia,Medicina, Malattie Infettive, Nefrologia, Pediatria, Pneumologia |
| L03AA10 | LENOGRASTIM | | Template fattori di crescita | Oncologia, Ematologia, Radioterapia,Medicina, Malattie Infettive, Nefrologia, Pediatria, Pneumologia |
| L03AA13 | PEGFILGRASTIM | | Template fattori di crescita | Oncologia, Ematologia, Radioterapia,Medicina, Malattie Infettive, Nefrologia, Pediatria, Pneumologia |

| ATC | Descrizione | NOTA AIFA | Tipologia di PIANO TERAPEUTICO | PRESCRIVIBILITA' |
|---|---|---|---|---|
| .03AA14 | LIPEGFILGRASTIM | | Template fattori di crescita | Oncologia, Ematologia, Radioterapia,Medicina, Malattie Infettive, Nefrologia, Pediatria, Pneumologia |
| **L03AB** | **Interferoni** | | | |
| .03AB04 | INTERFERONE ALFA 2A RICOMBINANTE | | Template Interferoni | Gastroenterologia, Malattie Infettive, Dermatologia, Ematologia, Nefrologia, Urologia, Medicina e Oncologia |
| .03AB05 | INTERFERONE ALFA 2B RICOMBINANTE | | Template Interferoni | |
| .03AB10 | INTERFERONE ALFA 2B PEGHILATO | | Template Interferoni | |
| .03AB11 | INTERFERONE ALFA 2A PEGHILATO | | Template Interferoni | |
| **L04AA** | | | | |
| .04AA10 | SIROLIMUS | | PT generale | Emodialisi, Centri trapianti, Nefrologia, Chirurgia |
| .04AA13 | LEFLUNOMIDE | | PT generale | Reumatologia, Medicina |
| .04AA18 | EVEROLIMUS | | PT generale | Centri trapianti, Nefrologia, Chirurgia, Emodialisi , Gastroenterologia |
| **L04AD** | | | | |
| .04AD02 | TACROLIMUS | | PT generale | Centri trapianti, Gastroenterologia, Nefrologia, Chirurgia, Emodialisi |
| **M** | **Sistema muscolo-scheletrico** | | | |
| **M05B** | **FARMACI CHE AGISCONO SULLA STRUTTURA E MINERALIZZAZIONE** | | | |
| **M05BX** | **Altri farmaci che agiscono sulla struttura e mineralizzazione ossee** | | | |
| M05BX03 | DENOSUMAB 60 mg | 79 | PT AIFA web | vedere Allegato Centri Prescrittori Prolia (da registro di monitoraggio AIFA) |
| M05BX04 | DENOSUMAB 120 mg | 79 | PT AIFA web | vedere Allegato Centri Prescrittori Xgeva (da registro di monitoraggio AIFA) |
| **N** | **Sistema nervoso** | | | |
| **N03A** | **ANTIEPILETTICI** | | | |
| **N03AF** | **Derivati della carbossamide** | | | |
| N03AF04 | ESLICARBAZEPINA | | Template Eslicarbazepina | Strutt Osp. e Terr. Di Neurologia e Neuropsichiatria infantile |
| **N03AX** | **Altri antiepilettici** | | | |
| N03AX22 | PERAMPANEL | | Template Perampanel | Strutt Osp. e Terr. Di Neurologia e Neuropsichiatria infantile |
| **N04B** | **SOSTANZE DOPAMINERGICHE** | | | |
| **N04BA** | **Dopa e suoi derivati** | | | |
| N04BA03 | LEVODOPA+CARBIDOPA+ENTACAPONE | | PT generale | Strutt Osp. e Terr. Di Neurologia del SSN |
| **N04BX** | **Altre sostanze dopaminergiche** | | | |
| N04BX01 | TOLCAPONE | | PT generale | Strutt Osp. e Terr. Di Neurologia del SSN |
| N04BX02 | ENTACAPONE | | PT generale | Strutt Osp. e Terr. Di Neurologia del SSN |
| **N06B** | **PSICOSTIMOLANTI, FARMACI PER ADHD E NOOTROPI** | | | |
| **N06BA** | **Simpaticomimetici ad azione centrale** | | | |
| N06BA07 | MODAFINIL | | PT generale | Strutt Osp. e Terr. Di Neurologia del SSN |
| N06BA09 | ATOMOXETINA | | PT generale | vedere allegato Centri ADHD (da registro Nazionale ADHD) |
| **N06D** | **FARMACI ANTI-DEMENZA** | | | |
| **N06DA** | **Anticolinesterasici** | | | |
| N06DA02 | DONEPEZIL | 85 | PT generale | Centri/Unità di Valutazione Alzheimer |
| N06DA03 | RIVASTIGMINA | 85 | PT generale | Centri/Unità di Valutazione Alzheimer |
| N06DA04 | GALANTAMINA | 85 | PT generale | Centri/Unità di Valutazione Alzheimer |
| **N06DX** | **ALTRI FARMACI ANTI-DEMENZA** | | | |
| N06DX01 | MEMANTINA | 85 | PT generale | Centri/Unità di Valutazione Alzheimer |
| **N07B** | **FARMACI UTILIZZATI NEI DISTURBI DA DIPENDENZA** | | | |
| **N07BB** | **Farmaci utilizzati nella dipendenza da alcool** | | | |
| N07BB04 | NALTREXONE | | PT generale | SERT |
| **P** | | | | |
| **P01C** | **SOSTANZE CONTRO LA LEISHMANIOSI E LA TRIPANOSOMIASI** | | | |
| **P01CX** | **Altre sostanze contro la leishmaniosi e la tripanosomiasi** | | | |
| P01CX01 | PENTAMIDINA ISETIONATO | | PT generale | Oncoematologia, Centri trapianti, Malattie infettive, Pneumologia, Nefrologia |
| **R** | **Sistema Respiratorio** | | | |

| ATC | Descrizione | NOTA AIFA | Tipologia di PIANO TERAPEUTICO | PRESCRIVIBILITA' |
|---|---|---|---|---|
| **R03D** | **ALTRI FARMACI PER LE SINDROMI OSTRUTTIVE DELLE VIE RESPIRATORIE PER USO SISTEMICO** | | | |
| **R03DX** | **Altri farmaci per le sindromi ostruttive delle vie respiratorie per uso sistemico** | | | |
| R03DX05 | OMALIZUMAB per l'indicazione Asma allergica | | Template Omalizumab | Strutt.Osp. e Terr. Di Pneumologia, Allergologia e Pediatria del SSN |
| R03DX05 | OMALIZUMAB per l'indicazione Orticaria cronica spontanea (CSU) | | Template Omalizumab | Strutt.Osp. e Terr. Di Dermatologia, Allergologia del SSN |
| R03DX09 | MEPOLIZUMAB | | Template Mepalizumab | Strutt.Osp. e Terr. Di Pneumologia, Allergologia del SSN |
| **V** | **Vari** | | | |
| **V03A** | **TUTTI GLI ALTRI PRODOTTI TERAPEUTICI** | | | |
| **V03AC** | **Sostanze chelanti del ferro** | | | |
| V03AC01 | DEFEROXAMINA 500 mg | | PT generale | Ematologia, Servizi Trasfusionali e di Immunoematologia, Medicina, Pediatria, Pronto Soccorso |
| **V03AE** | **Farmaci per il trattamento di iperkalemia ed iperfosfatemia** | | | |
| V03AE02 | SEVELAMER | | PT generale | Nefrologia e Dialisi |
| V03AE03 | LANTANIO CARBONATO (IDRATO) | | PT generale | Nefrologia e Dialisi |
| **V03AF** | **Sostenze disisntossicanti per i trattamenti citostatici** | | | |
| V03AF01 | MESNA | | PT generale | Oncologia, Radioterapia, Medicina, Urologia |

ALLEGATO 3)



**REGIONE ABRUZZO** **AZIENDA ASL** **PERIODO: mese anno**

## DISTINTA CONTABILE FARMACIA - Prospetto riepilogativo Farmaci e AIR

**Farmacia** **Codice:**

**Partita IVA:** **C.F.:**

**Indirizzo**

| **Tipologia Farmacia** | | **Fatturato** | | **Sconto SSN** | |
|---|---|---|---|---|---|
| **Rurale** | ☐ | | ☐ **<450.000** | | |
| | | | ☐ **>450.000** | ☐ | **A fasce** |
| **Sussidiata** | ☐ | | ☐ **<300.000** | ☐ | **A fasce ridotto 60%** |
| **Urbana** | ☐ | | ☐ **>300.000** | ☐ | **1,50%** |

| sez | rigo | SEZIONE 1 - FARMACI SOGGETTI A SCONTO | | |
|---|---|---|---|---|
| 1 | A | *Ricette SSN* | | |
| 1 | A1 | *di cui n. ricette ossigeno* | | |
| 1 | A2 | *di cui n. ricette dematerializzate* | | |
| 1 | B | *Importo Lordo SSN* | | |
| 1 | B1 | *di cui ossigeno* | | |
| 1 | B2 | *di cui Dematerializzate* | | |
| 1 | C1 | *Sconto al SSN (art.1, L.662/96)* | | |
| 1 | C2 | *Sconto 0,6% AIFA 30/12/05* | | |
| 1 | C3 | *Sconto 0,64% AIFA 09/02/2007 e succ.* | | |
| 1 | C4 | *Sconto 2,25% Legge 135/2012 art 15 co. 1* | | |
| 1 | D | *Importo lordo SSN al netto degli sconti (B - Cn)* | | |
| 1 | E1 | *Importo ticket quota fissa* | | |
| 1 | E2 | *Importo ticket quota differenziale* | | |
| 1 | F | *Rettifiche in addebito* | | |
| 1 | G | *Rettifiche in accredito* | | |
| 1 | H | **Importo netto [D-(E1+E2)-F+G]** | | |
| 1 | | **Trattenute: (% su D-F+G)** | | |
| 1 | I1 | *Enpaf 0,90%* | | |
| 1 | I2 | *Convenzionali 0,02%* | | |
| 1 | I3 | *Associazione titolari 0,15%* | | |
| 1 | I4 | *Federfarma 0,05%* | | |
| 1 | I | *Totale Trattenute* | | |
| 1 | J | *Importi in accredito non soggetti a trattenute* | | |
| 1 | J1 | *Diritto addizionale (D.A.)* | | |
| 1 | K | *Importi in addebito non soggetti a trattenute* | | |
| 1 | L | *Acconto in detrazione a conguaglio* | | |
| 1 | M | *Acconto in accredito per anno in corso* | | |
| 1 | N | **Totale importo da liquidare FARMACI (H-I+J+J1-K-L+M)** | | |
| **sez** | **rigo** | **SEZIONE 2 - ASSISTENZA INTEGRATIVA** | | |
| 2 | A | *N. ricette/buoni AIR* | | |
| 2 | B | *Importo lordo prodotti/presidi AIR* | | |
| 2 | C | *Addebiti* | | |
| 2 | D | *Accrediti* | | |
| 2 | E | **Totale Importo da liquidare AIR (B-C+D)** | | |

REGIONE ABRUZZO | AZIENDA ASL | PERIODO: mese anno

## DISTINTA CONTABILE FARMACIA - Prospetto riepilogativo DPC

**Farmacia** **Codice:**

**Partita IVA:** **C.F.:**

**Indirizzo**

| Tipologia Farmacia | | Fatturato | | <600.000 | Quota per il servizio | |
|---|---|---|---|---|---|---|
| Rurale | ☐ | | ☐ | >600.000 | ☐ | € 8,40 + IVA 22% |
| | | | ☐ | <258.228 | ☐ | € 7,10 + IVA 22% |
| Urbana | ☐ | | ☐ | >258.228 | ☐ | € 6,10 + IVA 22% |

| sez | rigo | SEZIONE 3 - FARMACI DISPENSATI PER CONTO DELLA REGIONE | |
|---|---|---|---|
| 3 | A | *N. ricette spedite* | |
| 3 | B | *N. confezioni erogate* | |
| 3 | C | *Remunerazione lorda DPC* | |
| 3 | D | *Importo Quote differenza prezzo* | |
| 3 | E | *Rettifiche in addebito* | |
| 3 | F | *Rettifiche in accredito* | |
| 3 | G | *IVA 22% (da calcolarsi su C, E, F) L. n.140 del 23.12.2014 art.1 comma 629, lettera b* | |
| 3 | H | **Remunerazione netta DPC (C-D-E+F-G)** | |
| | X | **TOTALE DA LIQUIDARE ALLA FARMACIA (N(sez.1)+E(sez.2)+H(sez.3))** | |

**Timbro e firma Farmacia** **Timbro e firma ASL**

Allegato 4 : 9

# (INSERIRE LOGO)

## IL DIRETTORE GENERALE


Prot. n. _____/ _____, lì _____

Spett.le Farmacia_____

_____

**Oggetto: Accordo per la Nomina a Responsabile del Trattamento dei Dati Personali della Farmacia Territoriale _____ *Agreement* (DPA) ai sensi dell'Art. 28 del Regolamento Generale sulla Protezione dei Dati n. 679/2016 (GDPR – General Data Protection Regulation). In applicazione della Delibera ASL PE n. 353 del 19 aprile 2017 e della Delibera G.R.A.n. 780 del 20 dicembre 2017.**

Il presente accordo integra e specifica gli obblighi di protezione dei dati gravanti sulla ASL di _____ (di seguito ASL PE o Titolare) e la Farmacia _____ (di seguito anche Responsabile) derivanti dall'esecuzione::

a) dell'Accordo Quadro recepito con Delibera G.R.A. n. 780 del 20 dicembre 2017, avente ad oggetto "Modifica e integrazione Decreto del Commissario ad Acta n. 114 del 28.09.2016 recante "Distribuzione di farmaci del PHT tramite le farmacie convenzionate con la modalità in nome e per conto (DPC) del SSR e attivazione del servizio Farmacup – Approvazione dell'Accordo Quadro Regionale con le associazioni delle farmacie pubbliche e private"- Provvedimenti" (di seguito "Accordo Quadro");

b) della Delibera ASL PE n. 353 del 19 aprile 2017 avente ad oggetto "Approvazione degli esiti della procedura negoziata volta alla aggiudicazione della fornitura – in licenza d'uso – del software per la gestione di una piattaforma web per la realizzazione della distribuzione per conto di farmaci PHT"- o, in ogni caso, derivanti dall'esecuzione, a qualunque titolo, da parte del Responsabile a favore della ASL PE di fornitura di un applicativo Web-DPC per garantire gli ordini dei farmaci oggetto dell'Accordo Quadro, e relativa installazione, manutenzione e/o l'assistenza tecnica, con particolare riferimento ai dati del Titolare e dei Terzi Interessati, ai sensi del Regolamento europeo n. 679 del 27 aprile 2016 **("GDPR");**

La Farmacia e la ASL Titolare di seguito congiuntamente le **"Parti"** e ciascuna singolarmente la **"Parte".**

## Articolo 1 – Oggetto, natura, finalità e durata del trattamento

Il presente DPA si applica al trattamento dei dati personali svolto dalla Farmacia in qualità di responsabile del trattamento ("Responsabile del Trattamento" o "Responsabile") per conto della ASL, quale titolare del

trattamento ("Titolare del Trattamento" o "Titolare"), ai sensi dell'Accordo Quadro e definisce gli obblighi delle Parti in materia di tutela dei dati personali.

Natura e finalità del trattamento: la Farmacia tratta i dati personali nella misura necessaria a fornire i servizi di cui all'Accordo Quadro. I servizi che possono essere svolti dal Responsabile sono indicati nell'Accordo Quadro e nella Delibera ASL PE n. 353/ 2017. I trattamenti autorizzati, ai sensi del presente DPA, sono indicati nell'Allegato 2.

Ciascuna Parte è esclusivamente responsabile per il proprio rispetto delle disposizioni di legge applicabili in materia di protezione dei dati personali.

La durata del trattamento dei dati personali dei Terzi Interessati da parte del Responsabile corrisponde alla durata dell'Accordo Quadro.

## Articolo 2 – Tipologie di dati personali e categorie di interessati

I soggetti i cui dati personali sono oggetto del trattamento da parte del Responsabile ai sensi del presente DPA possono essere, a titolo esemplificativo e non esaustivo, dipendenti e collaboratori della ASL Titolare, terzi incaricati, a qualunque titolo, dalla ASL Titolare, pazienti, controparti contrattuali della ASL Titolare e, in generale, terze parti rispetto alle quali la ASL Titolare agisce come titolare del trattamento dei dati personali ai sensi del GDPR (congiuntamente i "Terzi Interessati"). I dati personali trattati possono consistere, a titolo esemplificativo, in recapiti, dati identificativi, informazioni relative allo stato di salute, prescrizioni mediche, piani terapeutici.

## Articolo 3 – Istruzioni

Il Responsabile effettua il trattamento dei dati personali esclusivamente sulla base delle istruzioni ricevute dalla ASL Titolare in forma scritta: il dettaglio delle operazioni consentite è indicato nell'Allegato 3 al presente DPA. Il presente DPA e l'Accordo Quadro costituiscono parte delle istruzioni della ASL Titolare per il trattamento dei dati personali da parte del Responsabile e potranno essere integrate, in qualunque momento, da eventuali specifiche disposizioni, conformi alla legge applicabile in materia di Protezione dei Dati, ove ritenuto necessario da parte del Titolare.

Qualsiasi istruzione aggiuntiva o diversa rispetto a quanto previsto nell'Accordo Quadro e nel presente DPA dovrà essere trasmessa dalla ASL Titolare al Responsabile per iscritto e comunicata via PEC e/o raccomandata a/r. Tale istruzione aggiuntiva diverrà efficace entro 30 giorni dalla data di comunicazione.

## Articolo 4 – Riservatezza

Il Responsabile garantisce che i soggetti autorizzati al trattamento dei dati personali per proprio conto si siano impegnati contrattualmente a mantenere la riservatezza dei dati e siano soggetti a tale obbligo.

## Articolo 5 – Sicurezza del trattamento

Il Responsabile si impegna ad adottare le misure richieste dall'Art. 32 del GDPR.

In particolare - in considerazione dello stato dell'arte, dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché dei rischi derivanti, in particolare, dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trattati, il Responsabile si impegna a mettere in atto le misure tecniche e organizzative indicate nell'Allegato 1 al presente DPA di cui si richiede la compilazione per la descrizione delle modalità di implementazione.

Qualora il Responsabile intendesse apportare modifiche alle misure tecniche e organizzative descritte nell'Allegato 1, in considerazione del progresso e sviluppo tecnologico, effettuerà una preventiva comunicazione alla ASL Titolare, fermo restando che tali modifiche non potranno comportare l'approntamento di un livello di protezione inferiore rispetto a quanto previsto nell'Allegato 1.

## Articolo 6 – Assistenza

Tenendo conto della natura del trattamento dei dati personali svolto dal Responsabile, come descritto nell'Accordo Quadro, il Responsabile si impegna ad assistere il Titolare, approntando le adeguate misure tecniche e organizzative, nella misura in cui ciò sia possibile, per consentire al Titolare di permettere ai Terzi Interessati l'esercizio dei diritti di cui agli Artt. da 12 a 23 del GDPR.

Il Responsabile dovrà informare il Titolare, senza ingiustificato ritardo, qualora un Terzo Interessato eserciti nei suoi confronti uno dei diritti di cui agli Artt. da 12 a 23 del GDPR.

Tenendo conto della natura del trattamento, come descritto nell'Accordo Quadro e nel presente DPA, e delle informazioni di volta in volta messe a disposizione, il Responsabile si impegna ad assistere il Titolare a garantire il rispetto degli obblighi di cui agli Artt. da 32 a 36 del GDPR

## Articolo 7 – Cancellazione

I dati personali di proprietà del Titolare che siano oggetto di trattamento da parte del Responsabile, nell'ambito dell'esecuzione delle attività previste dall'Accordo Quadro, in base ai termini di conservazione di tali trattamenti, opportunamente previsti nei registri di trattamento, devono essere periodicamente cancellati ove ne ricorra il termine. Alla cessazione dell'Accordo Quadro, ove applicabile, i dati oggetto di Trattamento da parte del Responsabile devono essere restituiti al Titolare, entro un termine di 30 giorni dalla cessazione da parte del Responsabile dei servizi in relazione ai quali viene eseguito il trattamento dei dati personali.

In mancanza di diverse istruzioni successive, il Titolare chiede sin d'ora al Responsabile, (e questi agli eventuali sub-responsabili) di procedere con la cancellazione di tutte le copie di dati personali in proprio possesso a seguito della cessazione, da parte del Responsabile, dei servizi in relazione ai quali esegue il trattamento dei dati personali, salvo che la legge applicabile obblighi il Responsabile alla conservazione dei dati personali trattati.

## Articolo 8 – Violazioni di Dati Personali (cd. "Data Breach")

Il Responsabile si impegna ad informare il Titolare, senza ingiustificato ritardo e comunque entro 12 ore dal momento in cui ne sia venuto a conoscenza, di ogni violazione della sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati Personali trasmessi, conservati o comunque trattati.

Il Responsabile si impegna inoltre, ai sensi dell'art. 28.3, lett. f), tenuto conto della natura del trattamento e delle informazioni a sua disposizione, a prestare ogni necessaria collaborazione al Titolare in relazione all'adempimento degli obblighi sullo stesso gravanti di notifica delle suddette violazioni all'Autorità ai sensi dell'art. 33 del GDPR o di comunicazione della stessa agli interessati ai sensi dell'art. 34 del GDPR.

La comunicazione dovrà avvenire a mezzo PEC/mail rispettivamente agli indirizzi (PEC – Posta Elettronica Certificata) _____ e (PEO – Posta Elettronica Ordinaria) _____.

## Articolo 9 – Valutazione D'impatto (CD. "DATA PROTECTION IMPACT ASSESSMENT")

Il Responsabile, ai sensi dell'art. 28.3, lett. f), s'impegna fin da ora, tenuto conto della natura del trattamento e delle informazioni a sua disposizione, a fornire al Titolare ogni elemento utile all'effettuazione, da parte di quest'ultimo, della valutazione di impatto sulla protezione dei dati, qualora il Titolare sia tenuto ad effettuarla ai sensi dell'art. 35 del Regolamento, nonché ogni collaborazione nell'effettuazione della eventuale consultazione preventiva al Garante da parte di quest'ultimo ai sensi dell'art. 36 del Regolamento stesso.

## Articolo 10 – Soggetti Autorizzati al Trattamento

Fatto salvo quanto previsto all'articolo 11, il Responsabile, garantisce che l'accesso ai Dati Personali sarà limitato esclusivamente ai propri dipendenti e collaboratori, previamente identificati per iscritto, il cui accesso ai Dati Personali sia necessario per l'esecuzione dei Servizi.

Il Responsabile si impegna a fornire ai propri dipendenti e collaboratori, deputati a trattare i Dati Personali del Titolare, le istruzioni necessarie per garantire un corretto, lecito e sicuro trattamento, curarne la formazione, vigilare sul loro operato, vincolarli alla riservatezza su tutte le informazioni acquisite nello svolgimento della loro attività, anche per il periodo successivo alla cessazione del rapporto di lavoro, e a comunicare al Titolare, su specifica richiesta, l'elenco aggiornato degli stessi.

## Articolo 11 – Nomina della Farmacia Territoriale _____ anche in qualità di Sub-responsabile del Trattamento

Per l'esecuzione delle attività previste dall'Accordo Quadro, la ASL di _____, in qualità di Responsabile del Trattamento per conto delle altre ASL della Regione Abruzzo, nomina la Farmacia

_____

anche Sub-responsabile del Trattamento.

## Articolo 12 – Sub-responsabili del Trattamento

Per l'esecuzione di specifiche attività per conto della ASL Titolare, il Responsabile, potrà avvalersi di sub-responsabili del trattamento (ciascuno un "Sub-responsabile del Trattamento") ai sensi del GDPR. I Sub-responsabili del Trattamento sono autorizzati a trattare dati personali dei Terzi Interessati esclusivamente allo scopo di eseguire le attività per le quali tali dati personali siano stati forniti al Responsabile ed è fatto loro divieto di trattare tali dati personali per altre finalità. Se il Responsabile, ricorrerà a Sub-responsabili del Trattamento, essi saranno vincolati, per iscritto, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, agli stessi obblighi in materia di protezione dei dati contenuti nel presente DPA tra il Titolare del trattamento e il Responsabile,, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del regolamento. Qualora il sub-responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile, conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi del Sub-responsabile.

L'elenco completo dei Sub-responsabili del Trattamento che verranno eventualmente incaricati dal Responsabile, per l'esecuzione di attività di trattamento dei dati di cui all'Accordo Quadro dovrà essere previamente fornito alla ASL Titolare per la necessaria autorizzazione; tale autorizzazione dovrà essere richiesta dal Responsabile anche in caso di eventuali aggiornamenti a tale elenco.

Il Responsabile si impegna a informare anticipatamente il Titolare, anche con mezzi elettronici (indirizzi e-mail e/o PEC indicati all'art. 8 del presente DPA), laddove intenda includere un nuovo Sub-responsabile del Trattamento nell'elenco, intenda sostituire o cessare il rapporto con un Sub-responsabile del Trattamento esistente. La modifica si intenderà accettata dal Titolare laddove quest'ultimo non sollevi obiezioni per iscritto entro 3 (tre) mesi dalla ricezione della comunicazione da parte del Responsabile.

Qualora la ASL Titolare sollevi obiezioni su uno o più sub-responsabili del Trattamento, il Titolare darà indicazioni al Responsabile sulle relative motivazioni. In tal caso, il Responsabile potrà:

1. proporre altro Sub-responsabile del Trattamento in sostituzione del Sub-responsabile del Trattamento per il quale la ASL Titolare abbia sollevato obiezioni; o
2. adottare misure tese a superare le obiezioni della ASL Titolare (qualora le obiezioni fossero superabili).

Il Responsabile risponde nei confronti della ASL Titolare per l'adempimento del Sub-responsabile del Trattamento ai propri obblighi.

Nel caso in cui il Responsabile abbia necessità di ricorrere a un Sub-responsabile del Trattamento situato in un Paese terzo (extra UE), il Responsabile dovrà darne preventiva comunicazione al Titolare per l'approvazione e, eventualmente, per definire e concordare le modalità di trasferimento dei dati personali conformi a quanto previsto dagli Artt. 44 e seguenti del GDPR. Il Responsabile dovrà garantire inoltre che siano adottate adeguate misure tecniche e organizzative affinché il trattamento soddisfi i requisiti del GDPR, sia assicurata la protezione dei diritti dei Terzi Interessati e le opportune misure di sicurezza siano documentate.

## Articolo 13 – Amministratori di Sistema

Se applicabile, il Responsabile si impegna a conformarsi al Provvedimento generale del Garante per la protezione dei dati personali del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", così come modificato dal Provvedimento del Garante del 25 giugno 2009, e ad ogni altro pertinente provvedimento dell'Autorità.

In riferimento ai sistemi informatici di trattamento dei dati del Titolare per i quali il Responsabile eserciti attività di Amministrazione di Sistema, egli si impegna a:

1. designare quali amministratori di sistema le figure professionali dedicate alla gestione e alla manutenzione di impianti di elaborazione o di loro componenti con cui vengono effettuati trattamenti di Dati personali, fornendo al Titolare, su richiesta, informazioni sulle valutazioni effettuate per le designazioni;
2. effettuare un'elencazione analitica degli ambiti di operatività consentiti a ciascuno in base al relativo profilo di autorizzazione assegnato e fornendo, su richiesta, informazioni relative alle valutazioni alla base delle designazioni;
3. predisporre e conservare l'elenco contenente gli estremi identificativi delle persone fisiche qualificate quali amministratori di sistema e le funzioni ad essi attribuite;
4. comunicare periodicamente al Titolare l'elenco aggiornato degli amministratori di sistema, specificandone l'ambito di responsabilità (sistemi, database, reti, applicativi, etc.);
5. verificare annualmente l'operato degli amministratori di sistema, informando il Titolare circa le risultanze di tale verifica;
6. mantenere i file di log in conformità a quanto previsto nel suddetto provvedimento (qualora i sistemi siano installati presso le strutture del Responsabile o di suoi sub-Responsabili);
7. garantire una rigida separazione tra chi autorizza e/o assegna i privilegi di accesso e chi effettua le attività tecnico-sistemistiche.

## Articolo 14 – Rapporti con le Autorità

Il Responsabile, su richiesta del Titolare, si impegna a coadiuvare quest'ultimo nella difesa in caso di procedimenti dinanzi all'autorità di controllo o all'autorità giudiziaria che riguardino il trattamento dei Dati Personali di propria competenza.

## Articolo 15 – Ulteriori Obblighi e Responsabilità

Il Responsabile mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui alla normativa in materia di protezione dei dati personali e/o delle istruzioni del Titolare di cui al presente atto di designazione e consente al Titolare del trattamento l'esercizio del potere di controllo e ispezione, prestando ogni ragionevole collaborazione alle attività di audit effettuate dal Titolare stesso o da un altro soggetto da questi incaricato o autorizzato, con lo scopo di controllare l'adempimento degli obblighi e delle istruzioni di cui al presente atto.

Il Titolare darà comunicazione al Responsabile della propria intenzione di svolgere un Audit comunicandone l'oggetto, la tempistica, la data, e la durata dell'Audit.

Il Titolare fornirà al Responsabile una relazione scritta di natura confidenziale contenente il riepilogo dell'oggetto e dei risultati dell'Audit.

Il Responsabile si impegna altresì a:

1. effettuare almeno annualmente un rendiconto in ordine all'esecuzione delle istruzioni ricevute dal Titolare (e agli adempimenti eseguiti) ed alle conseguenti risultanze;
2. collaborare, se richiesto dalla ASL Titolare, con gli altri Responsabili del trattamento, al fine di armonizzare e coordinare l'intero processo di trattamento dei Dati Personali;
3. realizzare quant'altro sia ragionevolmente utile e/o necessario al fine di garantire l'adempimento degli obblighi previsti dalla normativa applicabile in materia di protezione dei dati, nei limiti dei compiti affidati con il presente atto di designazione;
4. informare prontamente il Titolare di ogni questione rilevante ai fini di legge, in particolar modo, a titolo esemplificativo e non esaustivo, nei casi in cui abbia notizia, in qualsiasi modo, che il trattamento dei Dati Personali violi la normativa in materia di protezione dei dati personali o presenti comunque rischi specifici per i diritti, le libertà fondamentali e/o la dignità dell'interessato o qualora, a suo parere, un'istruzione violi la normativa, nazionale o comunitaria, relativa alla protezione dei dati oppure qualora il Responsabile sia soggetto ad obblighi di legge che gli rendono illecito o impossibile agire secondo le istruzioni ricevute dalla ASL Titolare e/o conformarsi alla normativa o a provvedimenti dell'Autorità di Controllo.

Resta inteso che qualora il Responsabile (o eventuali suoi Sub-responsabili) determini autonomamente le finalità e i mezzi di trattamento in violazione delle istruzioni impartite dal Titolare, sarà considerato, a sua volta, Titolare del trattamento, assumendo i conseguenti oneri, rischi e responsabilità.

## Articolo 16 – Disposizioni Finali

Resta inteso che la presente designazione non comporta alcun diritto per il Responsabile ad uno specifico compenso o indennità o rimborso per l'attività svolta, né ad un incremento del compenso spettante allo stesso in virtù del Contratto con la ASL Titolare.

Gli allegati alla presente designazione fanno parte integrante della stessa.

Per tutto quanto non previsto dal presente atto di designazione si rinvia alle disposizioni generali vigenti ed applicabili in materia di protezione dei dati personali.

Il mancato riscontro alle presenti istruzioni non consentirà di dare attuazione di quanto previsto nell'Accordo Quadro.

Una volta dato riscontro positivo alla presente nomina, resta inteso che la mancata esecuzione delle istruzioni ivi contenute, costituisce una violazione del Regolamento UE 2016/679.

| | |
|---|---|
| IL DIRETTORE GENERALE | Per ricezione ed integrale accettazione del Responsabile |
| Dr. | LA FARMACIA |


# ALLEGATO 1 – Principi, Diritti e Misure Tecniche e Organizzative

Si chiede di descrivere le modalità per garantire, per quanto di competenza, il rispetto dei seguenti principi di trattamento e diritti degli interessati, secondo le indicazioni del Regolamento UE 679/2016, nell'ambito delle attività svolte per conto de Titolare; in alternativa indicare se siano ritenute non applicabili e darne motivazione o siano state programmate azioni ed eventuali scadenze.

| Req. | Principi e Diritti (riferimenti agli articoli del Reg. UE 679/2016) | Adottata (SI/NO) | Descrizione |
|---|---|---|---|
| A.1 | Art. 5.1.a e Art. 7 – Liceità e Gestione Consenso al Trattamento | | |
| A.2 | Art. 5.1.c minimizzazione dei dati | | |
| A.3 | Art. 5.1.e Limitazione della conservazione (art. 13 del Regolamento) | | |
| A.4 | Art. 15 Diritto di Accesso | | |
| A.5 | Art. 16 – Diritto di Rettifica | | |
| A.6 | Art. 17 – Diritto alla Cancellazione | | |
| A.7 | Art. 18 – Diritto alla Limitazione del Trattamento | | |
| A.8 | Art. 20 – Diritto alla portabilità dei dati | | |

Si chiede di descrivere quali delle seguenti misure tecniche e organizzative siano state adottate nell'ambito dei prodotti e/o servizi forniti alla ASL Titolare o se siano state programmate azioni di implementazione ed eventuali scadenze; in alternativa indicare se siano ritenute non applicabili e darne motivazione.

| Req. | Misura | Dettaglio | Adottata (SI/NO) | Descrizione/Motivazione |
|---|---|---|---|---|
| B.1 | **Politiche per la protezione dei dati** | Politiche per la protezione dei dati personali, sicurezza delle informazioni e conservazione | | |
| B.2 | **Organizzazione per la protezione dei dati** | Articolazione dell'organizzazione per la Protezione dei Dati Personali (DPO, Responsabili, ecc...) | | |
| B.3 | **Gestione della Sicurezza dei Dati da parte delle risorse umane (dipendenti/collaboratori)** | Procedure di ingresso di nuovi dipendenti/collaboratori, cambiamento di mansioni e/o cessazione del rapporto di lavoro.<br>Piano di Formazione periodica sulla Protezione dei Dati Personali | | |
| B.4 | **Gestione degli asset (dati personali e strumenti di supporto)** | Classificazione, Censimento e Definizione delle Responsabilità dei dati personali e dei relativi supporti/strumenti di trattamento utilizzati | | |
| B.5 | **Controllo degli accessi logici e partizionamento dei dati** | Procedure di gestione degli accessi logici degli utenti a sistemi e applicazioni che trattano dati personali | | |
| B.6 | **Pseudonimizzazione** | Misure per garantire la pseudonimizzazione dei dati personali utilizzati nel servizio erogato | | |
| B.7 | **Cifratura** | Procedure e Criteri di utilizzo della cifratura | | |
| B.8 | **Controllo degli accessi fisici** | Procedura di definizione della sicurezza dei locali, delle aree di trattamento di dati personali e di gestione della sicurezza fisica delle apparecchiature (strumenti di supporto) | | |

| Req. | Misura | Dettaglio | Adottata (SI/NO) | Descrizione/Motivazione |
|---|---|---|---|---|
| B.9 | **Sicurezza delle attività operative e manutenzione** | Policies tecnico-organizzative (es.: Utilizzo dei dispositivi portatili, VPN, dispositivi personali, posta elettronica, ecc.)<br>Misure di sicurezza antivirus-antimalware<br>Procedure di Gestione dei Backup<br>Criteri e procedure per la raccolta di Log e Monitoraggio dei sistemi<br>Procedure di controllo dell'integrità degli strumenti di erogazione del servizio<br>Procedure di controllo delle vulnerabilità tecniche<br>Procedure di gestione delle Manutenzioni | | |
| B.10 | **Sicurezza della rete e delle comunicazioni** | Procedure di gestione della sicurezza della rete<br>Procedure per la gestione del trasferimento di informazioni | | |
| B.11 | **Gestione dei sistemi applicativi** | Criteri per la definizione dei Requisiti di sicurezza dei sistemi utilizzati/da acquisire<br>Procedure operative per le operazioni di acquisizione, sviluppo e di manutenzione dei sistemi | | |
| B.12 | **Relazioni con i sub-fornitori** | Procedure e nomine per garantire la protezione dei dati personali trattati dai sub-fornitori | | |
| B.13 | **Gestione degli incidenti e delle Violazioni di dati personali** | Procedure di gestione degli incidenti sulla Sicurezza delle Informazioni e delle Violazioni di Dati Personali | | |
| B.14 | **Continuità Operativa** | Procedure di Gestione della Continuità Operativa del servizio<br>Misure per garantire la Sicurezza in condizioni di emergenza e degli strumenti atti a garantire la Continuità Operativa. | | |

| Req. | Misura | Dettaglio | Adottata (SI/NO) | Descrizione/Motivazione |
|---|---|---|---|---|
| B.15 | **Conformità e Audit** | Procedure per garantire il tempestivo aggiornamento normativo e l'adeguamento del servizio alle nuove indicazioni<br>Procedure di Audit interne per assicurare la sicurezza dei trattamenti sui sistemi in uso per la ASL Titolare (test, verifica e valutazione dell'efficacia delle misure tecniche e organizzative) | | |
| B.16 | **Misure per il rispetto della Privacy by Design** | Ved. Reg. UE 679/2016 art. 25 | | |
| B.17 | **Misure per il rispetto della Privacy by Default** | Ved. Reg. UE 679/2016 art. 25 | | |
| B.18 | **DPO – Data Protection Officer (Responsabile della Protezione dei Dati)** | Si richiede di dare comunicazione, se nominato, degli estremi e dei riferimenti di contatto del Responsabile della Protezione Dati dell'organizzazione (RPD – DPO/Data Protection Officer) | | |
| B.19 | **Presenza di Polizza Cyber Risk** | Si richiede se la Vostra azienda sia dotata di **polizza cyber-risk e l'eventuale dettaglio della stessa** | | |
| B.20 | **Gestione del Cambiamento** | Si richiede se esista una **procedura di gestione dei cambiamenti (Change Management)** nelle modalità di erogazione del servizio (es.: cambiamenti infrastrutturali, cambiamenti organizzativi, ecc...). Si richiede di fornirne copia. | | |

# ALLEGATO 2 – Ambito del Trattamento

Sulla scorta degli atti d'ufficio risulta che le categorie di attività (art. 30.2 del Regolamento) svolte dal Fornitore, nell'ambito dei servizi erogati per conto della ASL Titolare, siano di supporto ai seguenti trattamenti censiti:

| Cod. | Sub. | Requisito | Descrizione |
|---|---|---|---|
| 1 | | **Trattamento 1** | Distribuzione di Farmaci del PHT tramite le Farmacie convenzionate con la modalità in nome e per conto (DPC) del SSR. |
| | 1.1 | Categorie di interessati | Pazienti |
| | 1.2 | Tipi di Dati Personali oggetto di trattamento (indicare se dati comuni, categorie particolari, dati relativi a condanne penali e reati | - Dati comuni<br>- Categorie particolari di dati personali (dati relativi alla salute) |
| | 1.3 | Finalità del trattamento | - Attività amministrative correlate a quelle di prevenzione, diagnosi, cura e riabilitazione<br>- Programmazione, gestione, controllo e valutazione dell'assistenza sanitaria |
| | 1.4 | Durata del trattamento | Fino alla cessazione per qualunque motivo del Contratto e/o, comunque, dei Servizi ovvero fino alla revoca anticipata per qualsiasi motivo da parte del Titolare |
| | 1.5 | Tempo di Conservazione | 5 anni salvo diverse istruzioni comunicate successivamente |

# ALLEGATO 3 – Categorie di attività di trattamento (30.2) e relativi impatti

In linea con l'approccio basato sul rischio previsto dal GDPR, il Titolare ha individuato per le seguenti categorie di attività relative al trattamento (operazioni di trattamento), secondo quanto previsto dall'Art. 30.2 del GDPR, il livello d'impatto potenziale (quindi considerato **prima dell'applicazione delle misure di sicurezza** adottate dal Titolare che del Responsabile) sui diritti e le libertà degli interessati ed il livello di impatto reale **dopo l'adozione delle misure di sicurezza** come di seguito indicato:

| ID | Trattamento (rif. Trattamenti Allegato 2) | Categorie di attività relative al trattamento (Operazioni di trattamento) | Appl. | Livello di Impatto Potenziale del Trattamento | Livello di Impatto Residuo del Trattamento (calcolato tenendo conto delle misure – All. 1) |
|---|---|---|---|---|---|
| 1 | Distribuzione di Farmaci del PHT tramite le Farmacie convenzionate con la modalità in nome e per conto (DPC) del SSR. | Raccolta | X | **Impatto Massimo** | **Impatto Trascurabile** |
| | | Registrazione | X | | |
| | | Organizzazione | X | | |
| | | Strutturazione | X | | |
| | | Conservazione | | | |
| | | Adattamento o Modifica | X | | |
| | | Estrazione | X | | |
| | | Consultazione | X | | |
| | | Uso | X | | |
| | | Comunicazione mediante trasmissione o qualsiasi altra forma di messa a disposizione | X | | |
| | | Raffronto o Interconnessione | | | |
| | | Limitazione | X | | |
| | | Cancellazione o Distruzione | | | |

Il livello di impatto indicato nella precedente tabella è relativo al valore valutato sia prima dell'adozione delle misure di sicurezza (colonna *"Livello di Impatto Potenziale"*), previste dall'Allegato 1, che successivamente all'implementazione delle stesse (colonna *"Livello di Impatto residuo"*).

I criteri di classificazione dei livelli di impatto adottati dal Titolare sono i seguenti:

- **Impatto trascurabile**: gli interessati coinvolti dal trattamento non saranno affetti da inconvenienti oppure possono incontrare alcuni inconvenienti che possono superare senza alcun problema (es. perdita di tempo per ripetere formalità, etc.);
- **Impatto limitato**: gli interessati coinvolti dal trattamento possono incontrare disagi significativi che però possono superare nonostante alcune difficoltà (es. interruzione temporanea del servizio fino a 8 ore);
- **Impatto significativo**: gli interessati coinvolti dal trattamento possono avere conseguenze significative che dovrebbero essere in grado di superare seppure con gravi difficoltà (es. interruzione temporanea del servizio oltre le 8 ore e fino e non oltre le 24 ore);
- **Impatto massimo**: gli interessati coinvolti dal trattamento possono incontrare conseguenze significative, o addirittura irreversibili, che non possono superare (es.: Interruzione del servizio oltre le 24 ore, impossibilità o perdita della possibilità di accesso ai servizi, mancato rispetto dei diritti dell'interessato – es.: diritto alla salute)

Allegato 4 : b

# AZIENDA SANITARIA LOCALE DI PESCARA

Azienda Pubblica

Sede Legale:
Via Renato Paolini, 45
65124 Pescara
P. IVA 01397530982

## IL DIRETTORE GENERALE

Prot. n. _____/ Pescara, lì _____

Spett.le **Goodmen.it srl**
**Via Assisana, 33/C**
**06135 Piscille - PERUGIA**
**CF \ Partita IVA 03385330547**

**Oggetto: Accordo per la Nomina a Responsabile del Trattamento dei Dati Personali della Ditta Goodmen.it s.r.l.. *Data Processing Agreement* (DPA) ai sensi dell'Art. 28 del Regolamento Generale sulla Protezione dei Dati n. 679/2016 (GDPR – General Data Protection Regulation). In applicazione della Delibera ASL PE n. 353 del 19 aprile 2017 e della Delibera G.R.A.n. 780 del 20 dicembre 2017.**

Il presente accordo integra e specifica gli obblighi di protezione dei dati gravanti sulla ASL di Pescara (di seguito "ASL PE") e la società Goodmen.it srl (di seguito il "Fornitore") derivanti dall'esecuzione:

a) dell'Accordo Quadro recepito con Delibera G.R.A. n. 780 del 20 dicembre 2017, avente ad oggetto "Modifica e integrazione Decreto del Commissario ad Acta n. 114 del 28.09.2016 recante "Distribuzione di farmaci del PHT tramite le farmacie convenzionate con la modalità in nome e per conto (DPC) del SSR e attivazione del servizio Farmacup – Approvazione dell'Accordo Quadro Regionale con le associazioni delle farmacie pubbliche e private"- Provvedimenti" (di seguito "Accordo Quadro");

b) della Delibera ASL PE n. 353 del 19 aprile 2017 avente ad oggetto "Approvazione degli esiti della procedura negoziata volta alla aggiudicazione della fornitura – in licenza d'uso – del software per la gestione di una piattaforma web per la realizzazione della distribuzione per conto di farmaci PHT"- o, in ogni caso, derivanti dall'esecuzione, a qualunque titolo, da parte del Fornitore a favore della ASL PE di fornitura di un applicativo Web-DPC per garantire gli ordini dei farmaci oggetto dell'Accordo Quadro, e relativa installazione, manutenzione e/o l'assistenza tecnica, con particolare riferimento ai dati del Titolare e dei Terzi Interessati, ai sensi del Regolamento europeo n. 679 del 27 aprile 2016 **("GDPR");**

c) del Contratto per l'acquisizione di un software per la gestione di una piattaforma web per la realizzazione della distribuzione per conto di farmaci PHT, in esecuzione della Delibera di affidamento n. 353/2017, CIG 7126983C6A. (il **"Contratto Principale)**

## Articolo 1 – Oggetto, natura, finalità e durata del trattamento

Il presente DPA si applica al trattamento dei dati personali svolto dal Fornitore in qualità di responsabile del trattamento ("Responsabile del Trattamento") per conto della ASL, quale titolare del trattamento ("Titolare del Trattamento"), ai sensi del Contratto Principale e definisce gli obblighi delle Parti in materia di tutela dei dati personali.

Natura e finalità del trattamento: il Fornitore tratta i dati personali nella misura necessaria a fornire i servizi di cui all'Accordo Quadro e al Contratto Principale. I servizi che possono essere svolti dal Fornitore sono indicati nell'Accordo Quadro, nella Delibera ASL PE n. 353/ 2017 e nel Contratto Principale. I trattamenti autorizzati, ai sensi del presente DPA, sono indicati nell'Allegato 2.

Ciascuna Parte è esclusivamente responsabile per il proprio rispetto delle disposizioni di legge applicabili in materia di protezione dei dati personali.

La durata del trattamento dei dati personali dei Terzi Interessati da parte del Fornitore corrisponde alla durata dell'Accordo Quadro e a quanto indicato nel Contratto Principale.

## Articolo 2 – Tipologie di dati personali e categorie di interessati

I soggetti i cui dati personali sono oggetto del trattamento da parte del Fornitore ai sensi del presente DPA possono essere, a titolo esemplificativo e non esaustivo, dipendenti e collaboratori della ASL, terzi incaricati, a qualunque titolo, dalla ASL, pazienti, controparti contrattuali della ASL e, in generale, terze parti rispetto alle quali la ASL agisce come titolare del trattamento dei dati personali ai sensi del GDPR (congiuntamente i "Terzi Interessati"). I dati personali trattati possono consistere, a titolo esemplificativo, in recapiti, dati identificativi, informazioni relative allo stato di salute.

## Articolo 3 – Istruzioni

Il Fornitore effettua il trattamento dei dati personali esclusivamente sulla base delle istruzioni ricevute dalla ASL in forma scritta: il dettaglio delle operazioni consentite è indicato nell'Allegato 3 al presente DPA. Il presente DPA e il Contratto Principale costituiscono parte delle istruzioni della ASL per il trattamento dei dati personali da parte del Fornitore e potranno essere integrate, in qualunque momento, da eventuali specifiche disposizioni, conformi alla legge applicabile in materia di Protezione dei Dati, ove ritenuto necessario da parte del Titolare.

Qualsiasi istruzione aggiuntiva o diversa rispetto a quanto previsto nel Contratto Principale e nel presente DPA dovrà essere trasmessa dalla ASL al Fornitore per iscritto e comunicata via PEC e/o raccomandata a/r. Tale istruzione aggiuntiva diverrà efficace entro 30 giorni dalla data di comunicazione.

## Articolo 4 – Riservatezza

Il Fornitore garantisce che i soggetti autorizzati al trattamento dei dati personali per proprio conto si siano impegnati contrattualmente a mantenere la riservatezza dei dati e siano soggetti a tale obbligo.

## Articolo 5 – Sicurezza del trattamento

Il Fornitore si impegna ad adottare le misure richieste dall'Art. 32 del GDPR.

In particolare - in considerazione dello stato dell'arte, dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché dei rischi derivanti, in particolare, dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trattati, il Fornitore si impegna a mettere in atto le misure tecniche e organizzative indicate nell'Allegato 1 al presente DPA di cui si richiede la compilazione per la descrizione delle modalità di implementazione. Il Fornitore si impegna a comunicare le indicazioni applicabili ai prodotti e/o servizi forniti secondo quanto previsto dall'Allegato 4 (solo per i fornitori di servizi tecnici/tecnologici o per specifici requisiti).

Qualora il Fornitore intendesse apportare modifiche alle misure tecniche e organizzative descritte nell'Allegato 1, in considerazione del progresso e sviluppo tecnologico, effettuerà una preventiva comunicazione alla ASL, fermo restando che tali modifiche non potranno comportare l'approntamento di un livello di protezione inferiore rispetto a quanto previsto nell'Allegato 1.

## Articolo 6 – Assistenza

Tenendo conto della natura del trattamento dei dati personali svolto dal Fornitore, come descritto nel Contratto Principale, il Fornitore si impegna ad assistere il Titolare, approntando le adeguate misure tecniche e organizzative, nella misura in cui ciò sia possibile, per consentire al Titolare di permettere ai Terzi Interessati l'esercizio dei diritti di cui agli Artt. da 12 a 23 del GDPR.

Il Fornitore dovrà informare il Titolare, senza ingiustificato ritardo, qualora un Terzo Interessato eserciti nei suoi confronti uno dei diritti di cui agli Artt. da 12 a 23 del GDPR.

Tenendo conto della natura del trattamento, come descritto nel Contratto Principale e nel presente DPA, e delle informazioni di volta in volta messe a disposizione, il Fornitore si impegna ad assistere il Titolare a garantire il rispetto degli obblighi di cui agli Artt. da 32 a 36 del GDPR

## Articolo 7 – Cancellazione

I dati personali di proprietà del Titolare che siano oggetto di trattamento da parte del Fornitore, nell'ambito dell'esecuzione delle attività previste dal Contratto Principale, in base ai termini di conservazione di tali trattamenti, opportunamente previsti nei registri di trattamento, devono essere periodicamente cancellati ove ne ricorra il termine. Alla cessazione del Contratto Principale, i dati oggetto di Trattamento da parte del Fornitore devono essere restituiti al Titolare, entro un termine di 30 giorni dalla cessazione da parte del Fornitore dei servizi in relazione ai quali viene eseguito il trattamento dei dati personali.

In mancanza di diverse istruzioni successive, il Titolare chiede sin d'ora al Fornitore (e questi agli eventuali sub-responsabili) di procedere con la cancellazione di tutte le copie di dati personali in proprio possesso a seguito della cessazione, da parte del Fornitore, dei servizi in relazione ai quali esegue il trattamento dei dati personali, salvo che la legge applicabile obblighi il Fornitore alla conservazione dei dati personali trattati.

## Articolo 8 – Violazioni di Dati Personali (cd. "Data Breach")

Il Responsabile si impegna ad informare il Titolare, senza ingiustificato ritardo e comunque entro 12 ore dal momento in cui ne sia venuto a conoscenza, di ogni violazione della sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati Personali trasmessi, conservati o comunque trattati.

Il Responsabile si impegna inoltre, ai sensi dell'art. 28.3, lett. f), tenuto conto della natura del trattamento e delle informazioni a disposizione del Fornitore, a prestare ogni necessaria collaborazione al Titolare in relazione all'adempimento degli obblighi sullo stesso gravanti di notifica delle suddette violazioni all'Autorità ai sensi dell'art. 33 del GDPR o di comunicazione della stessa agli interessati ai sensi dell'art. 34 del GDPR.

La comunicazione dovrà avvenire a mezzo PEC/mail rispettivamente agli indirizzi dpo.aslpe@pec.it e dpo@ausl.pe.it.

## Articolo 9 – Valutazione D'impatto (CD. "DATA PROTECTION IMPACT ASSESSMENT")

Il Responsabile, ai sensi dell'art. 28.3, lett. f), s'impegna fin da ora, tenuto conto della natura del trattamento e delle informazioni a disposizione del Fornitore, a fornire al Titolare ogni elemento utile all'effettuazione, da parte di quest'ultimo, della valutazione di impatto sulla protezione dei dati, qualora il Titolare sia tenuto ad effettuarla ai sensi dell'art. 35 del Regolamento, nonché ogni collaborazione

nell'effettuazione della eventuale consultazione preventiva al Garante da parte di quest'ultimo ai sensi dell'art. 36 del Regolamento stesso.

## Articolo 10 – Soggetti Autorizzati al Trattamento

Fatto salvo quanto previsto all'articolo 11, il Fornitore garantisce che l'accesso ai Dati Personali sarà limitato esclusivamente ai propri dipendenti e collaboratori, previamente identificati per iscritto, il cui accesso ai Dati Personali sia necessario per l'esecuzione dei Servizi.

Il Responsabile si impegna a fornire ai propri dipendenti e collaboratori, deputati a trattare i Dati Personali del Titolare, le istruzioni necessarie per garantire un corretto, lecito e sicuro trattamento, curarne la formazione, vigilare sul loro operato, vincolarli alla riservatezza su tutte le informazioni acquisite nello svolgimento della loro attività, anche per il periodo successivo alla cessazione del rapporto di lavoro, e a comunicare al Titolare, su specifica richiesta, l'elenco aggiornato degli stessi.

## Articolo 11 – Nomina della Società Goodmen.it Srl anche in qualità di Sub-responsabile del Trattamento

Per l'esecuzione delle attività previste dal Contratto Principale, la ASL PE, in qualità di Responsabile del Trattamento per conto delle ASL di Lanciano Vasto Chieti, ASL Teramo e ASL Avezzano Sulmona L'Aquila, nomina la Società Goodmen.it Srl anche Sub-responsabile del Trattamento.

## Articolo 12 – Sub-responsabili del Trattamento

Per l'esecuzione di specifiche attività per conto della ASL, il Fornitore potrà avvalersi di sub-responsabili del trattamento (ciascuno un "Sub-responsabile del Trattamento") ai sensi del GDPR. I Sub-responsabili del Trattamento sono autorizzati a trattare dati personali dei Terzi Interessati esclusivamente allo scopo di eseguire le attività per le quali tali dati personali siano stati forniti al Fornitore ed è fatto loro divieto di trattare tali dati personali per altre finalità. Se il Fornitore ricorrerà a Sub-responsabili del Trattamento, essi saranno vincolati, per iscritto, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, agli stessi obblighi in materia di protezione dei dati contenuti nel presente DPA tra il Titolare del trattamento e il Fornitore, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del regolamento. Qualora il sub-responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Fornitore conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi del Sub-responsabile.

L'elenco completo dei Sub-responsabili del Trattamento che verranno eventualmente incaricati dal Fornitore per l'esecuzione di attività di trattamento dei dati di cui al Contratto Principale dovrà essere previamente fornito alla ASL per la necessaria autorizzazione; tale autorizzazione dovrà essere richiesta dal Fornitore anche in caso di eventuali aggiornamenti a tale elenco.

Il Fornitore si impegna a informare anticipatamente il Titolare, anche con mezzi elettronici (indirizzi e-mail e/o PEC indicati all'art. 8 del presente DPA), laddove intenda includere un nuovo Sub-responsabile del Trattamento nell'elenco, intenda sostituire o cessare il rapporto con un Sub-responsabile del Trattamento esistente. La modifica si intenderà accettata dal Titolare laddove quest'ultimo non sollevi obiezioni per iscritto entro 3 (tre) mesi dalla ricezione della comunicazione da parte del Fornitore.

Qualora la ASL sollevi obiezioni su uno o più sub-responsabili del Trattamento, il Titolare darà indicazioni al Fornitore sulle relative motivazioni. In tal caso, il Fornitore potrà:

1. proporre altro Sub-responsabile del Trattamento in sostituzione del Sub-responsabile del Trattamento per il quale la ASL abbia sollevato obiezioni; o
2. adottare misure tese a superare le obiezioni della ASL (qualora le obiezioni fossero superabili).

Il Fornitore è responsabile nei confronti della ASL per l'adempimento del Sub-responsabile del Trattamento ai propri obblighi.

Nel caso in cui il Fornitore abbia necessità di ricorrere a un Sub-responsabile del Trattamento situato in un Paese terzo (extra UE), il Fornitore dovrà darne preventiva comunicazione al Titolare per l'approvazione e, eventualmente, per definire e concordare le modalità di trasferimento dei dati personali conformi a quanto previsto dagli Artt. 44 e seguenti del GDPR. Il Fornitore dovrà garantire inoltre che siano adottate adeguate misure tecniche e organizzative affinché il trattamento soddisfi i requisiti del GDPR, sia assicurata la protezione dei diritti dei Terzi Interessati e le opportune misure di sicurezza siano documentate.

## Articolo 13 – Amministratori di Sistema

Il Fornitore si impegna a conformarsi al Provvedimento generale del Garante per la protezione dei dati personali del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", così come modificato dal Provvedimento del Garante del 25 giugno 2009, e ad ogni altro pertinente provvedimento dell'Autorità.

In riferimento ai sistemi informatici di trattamento dei dati del Titolare per i quali il Fornitore eserciti attività di Amministrazione di Sistema, il Fornitore si impegna a:

1. designare quali amministratori di sistema le figure professionali dedicate alla gestione e alla manutenzione di impianti di elaborazione o di loro componenti con cui vengono effettuati trattamenti di Dati personali, fornendo al Titolare, su richiesta, informazioni sulle valutazioni effettuate per le designazioni;
2. effettuare un'elencazione analitica degli ambiti di operatività consentiti a ciascuno in base al relativo profilo di autorizzazione assegnato e fornendo, su richiesta, informazioni relative alle valutazioni alla base delle designazioni;
3. predisporre e conservare l'elenco contenente gli estremi identificativi delle persone fisiche qualificate quali amministratori di sistema e le funzioni ad essi attribuite;
4. comunicare periodicamente al Titolare l'elenco aggiornato degli amministratori di sistema, specificandone l'ambito di responsabilità (sistemi, database, reti, applicativi, etc.);
5. verificare annualmente l'operato degli amministratori di sistema, informando il Titolare circa le risultanze di tale verifica;
6. mantenere i file di log in conformità a quanto previsto nel suddetto provvedimento (qualora i sistemi siano installati presso le strutture del Responsabile o di suoi sub-Responsabili);
7. garantire una rigida separazione tra chi autorizza e/o assegna i privilegi di accesso e chi effettua le attività tecnico-sistemistiche.

## Articolo 14 – Rapporti con le Autorità

Il Responsabile, su richiesta del Titolare, si impegna a coadiuvare quest'ultimo nella difesa in caso di procedimenti dinanzi all'autorità di controllo o all'autorità giudiziaria che riguardino il trattamento dei Dati Personali di propria competenza.

## Articolo 15 – Ulteriori Obblighi e Responsabilità

Il Responsabile mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui alla normativa in materia di protezione dei dati personali e/o delle istruzioni del Titolare di cui al presente atto di designazione e consente al Titolare del trattamento l'esercizio del potere di controllo e ispezione, prestando ogni ragionevole collaborazione alle attività di audit effettuate dal Titolare stesso o da un altro soggetto da questi incaricato o autorizzato, con lo scopo di controllare l'adempimento degli obblighi e delle istruzioni di cui al presente atto.

Il Titolare darà comunicazione al Fornitore della propria intenzione di svolgere un Audit comunicandone l'oggetto, la tempistica, la data, e la durata dell'Audit.

Il Titolare fornirà al Responsabile una relazione scritta di natura confidenziale contenente il riepilogo dell'oggetto e dei risultati dell'Audit.

Il Responsabile si impegna altresì a:

1. effettuare almeno annualmente un rendiconto in ordine all'esecuzione delle istruzioni ricevute dal Titolare (e agli adempimenti eseguiti) ed alle conseguenti risultanze;
2. collaborare, se richiesto dalla ASL, con gli altri Responsabili del trattamento, al fine di armonizzare e coordinare l'intero processo di trattamento dei Dati Personali;
3. realizzare quant'altro sia ragionevolmente utile e/o necessario al fine di garantire l'adempimento degli obblighi previsti dalla normativa applicabile in materia di protezione dei dati, nei limiti dei compiti affidati con il presente atto di designazione;
4. informare prontamente il Titolare di ogni questione rilevante ai fini di legge, in particolar modo, a titolo esemplificativo e non esaustivo, nei casi in cui abbia notizia, in qualsiasi modo, che il trattamento dei Dati Personali violi la normativa in materia di protezione dei dati personali o presenti comunque rischi specifici per i diritti, le libertà fondamentali e/o la dignità dell'interessato o qualora, a suo parere, un'istruzione violi la normativa, nazionale o comunitaria, relativa alla protezione dei dati oppure qualora il Responsabile sia soggetto ad obblighi di legge che gli rendono illecito o impossibile agire secondo le istruzioni ricevute dalla ASL e/o conformarsi alla normativa o a provvedimenti dell'Autorità di Controllo.

Resta inteso che qualora il Responsabile (o eventuali suoi Sub-responsabili) determini autonomamente le finalità e i mezzi di trattamento in violazione delle istruzioni impartite dal Titolare, sarà considerato, a sua volta, Titolare del trattamento, assumendo i conseguenti oneri, rischi e responsabilità.

## Articolo 16 – Disposizioni Finali

Resta inteso che la presente designazione non comporta alcun diritto per il Responsabile ad uno specifico compenso o indennità o rimborso per l'attività svolta, né ad un incremento del compenso spettante allo stesso in virtù del Contratto con la ASL.

Gli allegati alla presente designazione fanno parte integrante della stessa.

Per tutto quanto non previsto dal presente atto di designazione si rinvia alle disposizioni generali vigenti ed applicabili in materia di protezione dei dati personali.

Il mancato riscontro alle presenti istruzioni non consentirà di dare attuazione di quanto previsto nell'Accordo Quadro.

Una volta dato riscontro positivo alla presente nomina, resta inteso che la mancata esecuzione delle istruzioni ivi contenute, costituisce una violazione del Regolamento UE 2016/679.

IL DIRETTORE GENERALE

Dr. Armando Mancini

Per ricezione ed integrale accettazione del Responsabile

# ALLEGATO 1 – Principi, Diritti e Misure Tecniche e Organizzative

Si chiede di descrivere le modalità per garantire, per quanto di competenza, il rispetto dei seguenti principi di trattamento e diritti degli interessati, secondo le indicazioni del Regolamento UE 679/2016, nell'ambito delle attività svolte per conto dell'Associazione Opera Santa Maria della Pace; in alternativa indicare se siano ritenute non applicabili e darne motivazione o siano state programmate azioni ed eventuali scadenze.

| Req. | Principi e Diritti (riferimenti agli articoli del Reg. UE 679/2016) | Adottata (SI/NO) | Descrizione |
|---|---|---|---|
| A.1 | Art. 5.1.a e Art. 7 – Liceità e Gestione Consenso al Trattamento | | |
| A.2 | Art. 5.1.c minimizzazione dei dati | | |
| A.3 | Art. 5.1.e Limitazione della conservazione (art. 13 del Regolamento) | | |
| A.4 | Art. 15 Diritto di Accesso | | |
| A.5 | Art. 16 – Diritto di Rettifica | | |
| A.6 | Art. 17 – Diritto alla Cancellazione | | |
| A.7 | Art. 18 – Diritto alla Limitazione del Trattamento | | |
| A.8 | Art. 20 – Diritto alla portabilità dei dati | | |

Si chiede di descrivere quali delle seguenti misure tecniche e organizzative siano state adottate nell'ambito dei prodotti e/o servizi forniti alla ASL o se siano state programmate azioni di implementazione ed eventuali scadenze; in alternativa indicare se siano ritenute non applicabili e darne motivazione.

| Req. | Misura | Dettaglio | Adottata (SI/NO) | Descrizione/Motivazione |
|---|---|---|---|---|
| B.1 | **Politiche per la protezione dei dati** | Politiche per la protezione dei dati personali, sicurezza delle informazioni e conservazione | | |
| B.2 | **Organizzazione per la protezione dei dati** | Articolazione dell'organizzazione per la Protezione dei Dati Personali (DPO, Responsabili, ecc...) | | |
| B.3 | **Gestione della Sicurezza dei Dati da parte delle risorse umane (dipendenti/collaboratori)** | Procedure di ingresso di nuovi dipendenti/collaboratori, cambiamento di mansioni e/o cessazione del rapporto di lavoro.<br>Piano di Formazione periodica sulla Protezione dei Dati Personali | | |
| B.4 | **Gestione degli asset (dati personali e strumenti di supporto)** | Classificazione, Censimento e Definizione delle Responsabilità dei dati personali e dei relativi supporti/strumenti di trattamento utilizzati | | |
| B.5 | **Controllo degli accessi logici e partizionamento dei dati** | Procedure di gestione degli accessi logici degli utenti a sistemi e applicazioni che trattano dati personali | | |
| B.6 | **Pseudonimizzazione** | Misure per garantire la pseudonimizzazione dei dati personali utilizzati nel servizio erogato | | |
| B.7 | **Cifratura** | Procedure e Criteri di utilizzo della cifratura | | |
| B.8 | **Controllo degli accessi fisici** | Procedura di definizione della sicurezza dei locali, delle aree di trattamento di dati personali e di gestione della sicurezza fisica delle apparecchiature (strumenti di supporto) | | |

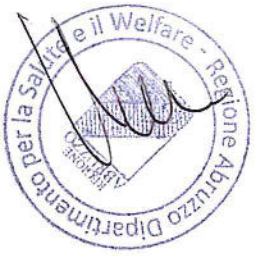
| Req. | Misura | Dettaglio | Adottata (SI/NO) | Descrizione/Motivazione |
|---|---|---|---|---|
| **B.9** | **Sicurezza delle attività operative e manutenzione** | Policies tecnico-organizzative (es.: Utilizzo dei dispositivi portatili, VPN, dispositivi personali, posta elettronica, ecc.)<br>Misure di sicurezza antivirus-antimalware<br>Procedure di Gestione dei Backup<br>Criteri e procedure per la raccolta di Log e Monitoraggio dei sistemi<br>Procedure di controllo dell'integrità degli strumenti di erogazione del servizio<br>Procedure di controllo delle vulnerabilità tecniche<br>Procedure di gestione delle Manutenzioni | | |
| **B.10** | **Sicurezza della rete e delle comunicazioni** | Procedure di gestione della sicurezza della rete<br>Procedure per la gestione del trasferimento di informazioni | | |
| **B.11** | **Gestione dei sistemi applicativi** | Criteri per la definizione dei Requisiti di sicurezza dei sistemi utilizzati/da acquisire<br>Procedure operative per le operazioni di acquisizione, sviluppo e di manutenzione dei sistemi | | |
| **B.12** | **Relazioni con i sub-fornitori** | Procedure e nomine per garantire la protezione dei dati personali trattati dai sub-fornitori | | |
| **B.13** | **Gestione degli incidenti e delle Violazioni di dati personali** | Procedure di gestione degli incidenti sulla Sicurezza delle Informazioni e delle Violazioni di Dati Personali | | |
| **B.14** | **Continuità Operativa** | Procedure di Gestione della Continuità Operativa del servizio<br>Misure per garantire la Sicurezza in condizioni di emergenza e degli strumenti atti a garantire la Continuità Operativa. | | |

| Req. | Misura | Dettaglio | Adottata (SI/NO) | Descrizione/Motivazione |
|---|---|---|---|---|
| B.15 | **Conformità e Audit** | Procedure per garantire il tempestivo aggiornamento normativo e l'adeguamento del servizio alle nuove indicazioni<br>Procedure di Audit interne per assicurare la sicurezza dei trattamenti sui sistemi in uso per la ASL (test, verifica e valutazione dell'efficacia delle misure tecniche e organizzative) | | |
| B.16 | **Misure per il rispetto della Privacy by Design** | Ved. Reg. UE 679/2016 art. 25 | | |
| B.17 | **Misure per il rispetto della Privacy by Default** | Ved. Reg. UE 679/2016 art. 25 | | |
| B.18 | **DPO – Data Protection Officer (Responsabile della Protezione dei Dati)** | Si richiede di dare comunicazione, se nominato, degli estremi e dei riferimenti di contatto del Responsabile della Protezione Dati dell'organizzazione (RPD – DPO/Data Protection Officer) | | |
| B.19 | **Presenza di Polizza Cyber Risk** | Si richiede se la Vostra azienda sia dotata di **polizza cyber-risk e l'eventuale dettaglio della stessa** | | |
| B.20 | **Gestione del Cambiamento** | Si richiede se esista una **procedura di gestione dei cambiamenti (Change Management)** nelle modalità di erogazione del servizio (es.: cambiamenti infrastrutturali, cambiamenti organizzativi, ecc...). Si richiede di fornirne copia. | | |

# ALLEGATO 2 – Ambito del Trattamento

Sulla scorta degli atti d'ufficio risulta che le categorie di attività (art. 30.2 del Regolamento) svolte dal Fornitore, nell'ambito dei servizi erogati per conto della ASL di Pescara, siano di supporto ai seguenti trattamenti censiti:

| Cod. | Sub. | Requisito | Descrizione |
|---|---|---|---|
| 1 | | **Trattamento 1** | Distribuzione di Farmaci del PHT tramite le Farmacie convenzionate con la modalità in nome e per conto (DPC) del SSR. |
| | 1.1 | Categorie di interessati | Pazienti |
| | 1.2 | Tipi di Dati Personali oggetto di trattamento (indicare se dati comuni, categorie particolari, dati relativi a condanne penali e reati | - Dati comuni<br>- Categorie particolari di dati personali (dati relativi alla salute) |
| | 1.3 | Finalità del trattamento | - Attività amministrative correlate a quelle di prevenzione, diagnosi, cura e riabilitazione<br>- Programmazione, gestione, controllo e valutazione dell'assistenza sanitaria |
| | 1.4 | Durata del trattamento | Fino alla cessazione per qualunque motivo del Contratto e/o, comunque, dei Servizi ovvero fino alla revoca anticipata per qualsiasi motivo da parte del Titolare |
| | 1.5 | Tempo di Conservazione | 5 anni salvo diverse istruzioni comunicate successivamente |
| 2 | | **Trattamento 2** (descrizione del Trattamento) | Gestione utenze per l'accesso al sistema informatico per la DPC e relative registrazioni di attività |
| | 2.1 | Categorie di interessati | Dipendenti e collaboratori delle strutture coinvolte (Farmacie, MMG, Distributori, ASL) |
| | 2.2 | Tipo di Dati Personali oggetto di trattamento (indicare se dati comuni, categorie particolari, dati relativi a condanne penali e reati | - Dati comuni (dati anagrafici degli utenti) |
| | 2.3 | Finalità del trattamento | - Gestione delle utenze per il raggiungimento delle finalità di cui al punto 1.3 del presente allegato |
| | 2.4 | Durata del trattamento | Fino alla cessazione per qualunque motivo del Contratto e/o, comunque, dei Servizi ovvero fino alla revoca anticipata per qualsiasi motivo da parte del Titolare |
| | 2.5 | Tempo di Conservazione | 5 anni salvo diverse istruzioni comunicate successivamente |



# ALLEGATO 3 – Categorie di attività di trattamento (30.2) e relativi impatti

In linea con l'approccio basato sul rischio previsto dal GDPR, il Titolare ha individuato per le seguenti categorie di attività relative al trattamento (operazioni di trattamento), secondo quanto previsto dall'Art. 30.2 del GDPR, il livello d'impatto potenziale (quindi considerato **prima dell'applicazione delle misure di sicurezza** adottate dal Titolare che del Responsabile) sui diritti e le libertà degli interessati ed il livello di impatto reale **dopo l'adozione delle misure di sicurezza** come di seguito indicato:

| ID | Trattamento (rif. Trattamenti Allegato 2) | Categorie di attività relative al trattamento (Operazioni di trattamento) | Appl. | Livello di Impatto Potenziale del Trattamento | Livello di Impatto Residuo del Trattamento (calcolato tenendo conto delle misure – All. 1) |
|---|---|---|---|---|---|
| 1 | Distribuzione di Farmaci del PHT tramite le Farmacie convenzionate con la modalità in nome e per conto (DPC) del SSR. | Raccolta | | **Impatto Massimo** | **Impatto Trascurabile** |
| | | Registrazione | X | | |
| | | Organizzazione | X | | |
| | | Strutturazione | X | | |
| | | Conservazione | X | | |
| | | Adattamento o Modifica | | | |
| | | Estrazione | X | | |
| | | Consultazione | | | |
| | | Uso | | | |
| | | Comunicazione mediante trasmissione o qualsiasi altra forma di messa a disposizione | | | |
| | | Raffronto o Interconnessione | | | |
| | | Limitazione | X | | |
| | | Cancellazione o Distruzione | X | | |
| 2 | Gestione utenze per l'accesso al sistema informatico per la DPC e relative registrazioni di attività | Raccolta | X | **Impatto Massimo** | **Impatto Trascurabile** |
| | | Registrazione | X | | |
| | | Organizzazione | X | | |
| | | Strutturazione | X | | |
| | | Conservazione | X | | |
| | | Adattamento o Modifica | X | | |
| | | Estrazione | X | | |
| | | Consultazione (solo delle utenze) | X | | |
| | | Uso | | | |
| | | Comunicazione mediante trasmissione o qualsiasi altra forma di messa a disposizione | | | |
| | | Raffronto o Interconnessione | | | |
| | | Limitazione | X | | |
| | | Cancellazione o Distruzione | X | | |

Il livello di impatto indicato nella precedente tabella è relativo al valore valutato sia prima dell'adozione delle misure di sicurezza (colonna *"Livello di Impatto Potenziale"*), previste dall'Allegato 1, che successivamente all'implementazione delle stesse (colonna *"Livello di Impatto residuo"*).

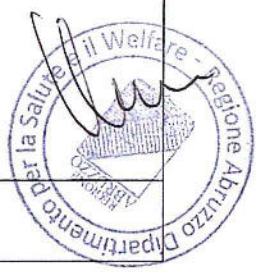
I criteri di classificazione dei livelli di impatto adottati dal Titolare sono i seguenti:

- **Impatto trascurabile**: gli interessati coinvolti dal trattamento non saranno affetti da inconvenienti oppure possono incontrare alcuni inconvenienti che possono superare senza alcun problema (es. perdita di tempo per ripetere formalità, etc.);
- **Impatto limitato**: gli interessati coinvolti dal trattamento possono incontrare disagi significativi che però possono superare nonostante alcune difficoltà (es. interruzione temporanea del servizio fino a 8 ore);
- **Impatto significativo**: gli interessati coinvolti dal trattamento possono avere conseguenze significative che dovrebbero essere in grado di superare seppure con gravi difficoltà (es. interruzione temporanea del servizio oltre le 8 ore e fino e non oltre le 24 ore);
- **Impatto massimo**: gli interessati coinvolti dal trattamento possono incontrare conseguenze significative, o addirittura irreversibili, che non possono superare (es.: Interruzione del servizio oltre le 24 ore, impossibilità o perdita della possibilità di accesso ai servizi, mancato rispetto dei diritti dell'interessato – es.: diritto alla salute)

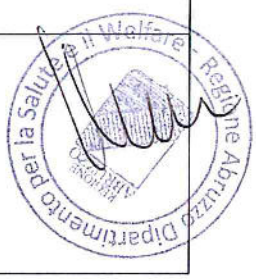
# ALLEGATO 4 – Informazioni specifiche sul servizio

Fornire, se applicabili al servizio fornito, le seguenti informazioni: in caso di non applicabilità del requisito si prega di indicare la dicitura "n.a." e di darne le motivazioni; negli ulteriori casi si prega di indicare la risposta nell'apposito riquadro o, se la risposta rimanda ad un documento, di indicare il riferimento all'allegato nel riquadro e di fornire copia del documento stesso.

| Req. | Sub. | Descrizione requisito | **Risposta** (nota o riferimento a documento allegato) |
|---|---|---|---|
| 1 | | **Elencazione completa e schema riepilogativo delle attrezzature e dei software di vostra produzione/fornitura/gestione** installati presso le strutture della ASL di Pescara o in strutture remote (hosting, cloud, ecc...) in uso presso l'Azienda Sanitaria, con particolare riferimento a: | |
| | 1.1 | • Sistemi applicativi: indicare i moduli componenti il sistema fornito | |
| | 1.2 | • Sistemi di interfaccia con piattaforme software o apparecchiature di vostra produzione/fornitura o di terzi | |
| | 1.3 | • Infrastruttura HW, Sistemistica e di comunicazione (se di fornitura) | |
| 2 | | Descrizione **dell'architettura fisica** relativa all'installazione delle apparecchiature e dei SW di vostra fornitura/produzione sia presso le strutture della ASL di Pescara (Centro Elaborazione Dati del SIT o altra locazione ASL - es. presso Unità Operative) che, eventualmente, presso strutture esterne (di vostra proprietà o di terzi), indicando la tipologia di infrastruttura prescelta (server fisici o virtuali, hosting, cloud privato, cloud pubblico, ecc...). | |
| 3 | | Specificare la **finalità di ogni componente del sistema** fornito (hardware, software, infrastruttura di comunicazione), indicando le tipologie di dati trattate da ogni componente (dati personali, sanitari, genetici, ecc...). | |
| 4 | | Specificare in maniera dettagliata **l'architettura di eventuali software di raccolta e monitoraggio di eventi** (o comunque di dati) dalle attrezzature fornite. | |
| 5 | | **Per ognuno dei software forniti**, specificare se siano moduli propri o di terzi (anche in caso di componenti, Web Services o altro), l'ubicazione della loro installazione ed il **dettaglio dell'architettura sistemistica asservita** (n. server fisici/virtuali, middleware utilizzati e relative versioni, DB principali e DB "intermedi" e/o di confine per gestire la comunicazione tra i vari moduli di propria fornitura e/o di terzi). | |
| 6 | | In caso di installazione dei **moduli SW presso strutture esterne rispetto alle sedi della ASL di Pescara**, si richiede la sede e la nazionalità in cui gli applicativi ed i sistemi utilizzati dall'Azienda Sanitaria siano installati (non sono ammesse installazioni, anche parziali, in paesi extra-UE): è necessario darne evidenza documentale. | |
| 7 | | Per ogni modulo software fornito è necessario fornire una **scheda tecnica** che indichi: | |



| Req. | Sub. | Descrizione requisito | **Risposta** (nota o riferimento a documento allegato) |
|---|---|---|---|
| | 7.1 | • Una descrizione generale delle funzionalità e delle relative finalità di utilizzo; | |
| | 7.2 | • Una descrizione dell'architettura logica, lo scenario degli "use case" e la mappatura dei flussi operativi di utilizzo delle funzionalità dei software; | |
| | 7.3 | • Quali dati personali/sanitari siano trattati dal modulo ed una descrizione del ciclo di vita delle informazioni (creazione, uso, trasferimento, dismissione); | |
| | 7.4 | • Se e come sia possibile gestire tempi limitati di conservazione delle informazioni in base a quanto potrà essere previsto dal massimario di conservazione; | |
| | 7.5 | • Quale sia l'ultima versione rilasciata di ogni singolo modulo software di gestione prodotto/fornito dalla vs società (al maggior livello di dettaglio possibile); | |
| | 7.6 | • Quale sia la versione attuale del singolo modulo software di gestione fornito **nell'installazione esistente per conto della ASL di Pescara**; | |
| | 7.7 | • Quali interazioni e/o interfacce siano presenti verso altri moduli software/attrezzature di vostra fornitura e/o di terzi (es.: interazioni del vostro modulo anagrafico con l'anagrafe centralizzata dei pazienti, interazioni con il sistema RIS e/o con il sistema PACS, ecc...). È necessario indicare le interazioni dei moduli/attrezzature di vostra produzione/fornitura tra loro e con quelli di altri produttori/fornitori, indicando il dettaglio dei dati scambiati e conservati anche dai moduli di interfaccia (con particolare riguardo a quelli personali) fornendo i tracciati record; | |
| | 7.8 | • Quali protocolli di comunicazione siano utilizzati dal modulo, con indicazione dell'eventuale cifratura, dei canali di comunicazione interna e/o verso l'esterno (verso altri moduli software o attrezzature proprie o di terzi) ed eventuali porte di comunicazione; | |
| | 7.9 | • Indicare se esistano software o apparecchiature di terze parti che accedano ai moduli o alle attrezzature di vostra fornitura mediante API, Web Services o altra modalità (anche semplicemente condividendo l'infrastruttura HW fornita a supporto); | |
| | 7.10 | • Indicare se l'infrastruttura software utilizzata dagli applicativi prodotti/forniti dalla Vostra Società sia basata su sistemi operativi, middleware ed altri software dichiarati dai produttori "fuori supporto" (out of support – es.: Sistema Operativo Windows XP); | |
| | 7.11 | • Indicare se la sicurezza sistemistica dell'infrastruttura HW/SW da voi fornita (aggiornamenti firmware, patch di sistema operativo e dei middleware, sistemi Endpoint (Antivirus), ecc...) sia sotto la responsabilità della Vostra Società o se sia a carico della ASL di Pescara e se tale responsabilità sia documentata (fornire documentazione a supporto). | |



| Req. | Sub. | Descrizione requisito | **Risposta** (nota o riferimento a documento allegato) |
|---|---|---|---|
| | 7.12 | • Indicare se il/i Database utilizzati adottino **tecniche di cifratura** dei dati: indicare quali dati siano sottoposti a queste tecniche di sicurezza, con dettaglio implementativo ed organizzativo conseguente; | |
| | 7.13 | • Indicare se il/i Database utilizzati adottino tecniche di **pseudonimizzazione**: indicare quali dati siano sottoposti a tali tecniche con eventuale dettaglio implementativo (architettura DB) ed organizzativo conseguente; indicare le modalità di protezione e gestione dei dati per la ricostruzione dell'associazione tra dati identificativi e dati personali; | |
| | 7.14 | • Indicare se e come siano adottate tecniche di Privacy by Design e secondo quali criteri; | |
| | 7.15 | • Indicare se e come siano adottate tecniche di Privacy by Default e secondo quali criteri; | |
| | 7.16 | • Indicare come siano gestiti i Profili di utenza con indicazione del livello di dettaglio che è possibile raggiungere per le abilitazioni (permessi a livello di modulo, funzionalità, utente o a livello di singolo dato); | |
| | 7.17 | • Indicare la previsione di un diritto alla portabilità e le eventuali modalità e formati gestiti; | |
| | 7.18 | • Indicare quali siano le modalità di accesso ai sistemi, con indicazione se sia previsto un accesso da parte di personale della vostra società o di soggetti esterni e in che modalità (in locale o da remoto – es.: via web/VPN ecc.); | |
| | 7.20 | • Indicare quali siano i modelli di rilascio delle credenziali (se esista un processo formale di richiesta/rilascio) e di gestione dell'identità degli utenti (es.: strong authentication); | |
| | 7.21 | • Indicare se l'attività di Amministrazione di Sistema sia svolta da personale della ASL di Pescara e/o della vostra società e/o da parte di terzi; indicare le ubicazioni da cui opera tale personale; | |
| | 7.22 | • Indicare l'elenco delle terze parti coinvolte nel supporto al sistema informativo che abbiano accesso alle attrezzature e/o ai software e/o ai dati personali: indicare specificamente anche il grado di accessibilità (a quali dati possano accedere e con quali permessi) a tali informazioni e le ubicazioni da cui operano. | |
| | 7.23 | • Indicare quali siano le procedure di sicurezza nell'ambito delle attività di manutenzione eseguite che abbiano impatto sulle informazioni gestite dai sistemi: ad esempio indicare, in caso di sostituzione di componenti contenenti dati (es.: Hard disks), se e come sia prevista la distruzione delle informazioni in essi contenute; | |
| | 7.24 | • Indicare la previsione di un diritto alla limitazione del trattamento e le eventuali modalità operative gestite; | |

| Req. | Sub. | Descrizione requisito | **Risposta** (nota o riferimento a documento allegato) |
|---|---|---|---|
| 8 | | Si richiede se nell'ambito dei servizi erogati presso la ASL di Pescara, riguardo alle **interazioni tra i vostri prodotti ed eventuali Software di terzi**, la **visualizzazione di dati provenienti dai Software di Terze parti** (es.: referti, dati strutturati o immagini) sia a carico del software/attrezzatura di vostra produzione/fornitura o se sia a carico del software/attrezzatura di terzi (es.: risultati di laboratorio analisi); specificare se esista una situazione "mista" e fornire le evidenze di quali siano le tipologie di utenze abilitate all'accesso in entrambi i casi. Si richiede inoltre se sia possibile "scaricare" localmente le risultanze diagnostiche dalla postazione di lavoro su cui viene effettuata l'interrogazione e, in caso affermativo, se sia tecnicamente possibile inibire tale funzionalità. | |
| 9 | | Si richiede se gli **accessi alle informazioni/dati sia sottoposto a log** e con quale livello di dettaglio (solo accessi, dettaglio utente, dettaglio operazioni effettuate, ecc...) e relative modalità e tempistiche di conservazione; | |
| 10 | | Si richiede se **l'utenza di accesso al Database** di ogni modulo corrisponda all'accesso utente degli applicativi (con mappatura "uno-a-uno") o se la gestione delle utenze sia gestito a livello applicativo con unica utenza verso il DB (mappatura "N-a-uno"). | |
| 11 | | Si richiede inoltre se esistano **procedure per la gestione degli aggiornamenti** dei software di vostra fornitura ed il dettaglio delle stesse (es.: patch management). | |
| 12 | | Si richiede se siano stati forniti i **manuali operativi per l'utilizzo dei prodotti** da voi forniti ed i relativi aggiornamenti in caso di upgrade delle versioni dei Software di vostra fornitura. | |
| 13 | | Si richiede se esista un **Piano di Continuità Operativa e Disaster Recovery** con indicazione della pianificazione dei backup programmati per i moduli/attrezzature forniti all'Azienda Sanitaria e le relative tempistiche e modalità di attuazione. In caso di interazione con moduli di terzi, specificare le modalità di attivazione in sinergia con le terze parti coinvolte. Specificare inoltre se esista un **piano di conservazione e cancellazione di dati e media**: fornire eventuali indicazioni di dettaglio. | |
| 14 | | Si richiede se sia attivo un **contratto di assistenza** e manutenzione per i sistemi da voi forniti con relativi ambiti di copertura e scadenze. | |
| 15 | | Si richiede se esista, in fase di "upgrade" dei sistemi o di conclusione del contratto, un **piano di "dismissione"** delle installazioni dei moduli SW/attrezzature di vostra fornitura con procedure dettagliate per la salvaguardia delle informazioni (es.: copie accessibili), della relativa distruzione sui sistemi dismessi e delle operazioni da effettuarsi sui sistemi client e server. | |

Allegato 4 : 6

# (INSERIRE LOGO)

## IL DIRETTORE GENERALE


Prot. n. _____/ _____, lì _____

Spett.le **Spett.le DRG - Direzione Generale della Regione**
Via L. Da Vinci, 6 - L'Aquila
drg@regione.abruzzo.it

**Oggetto: Accordo per la Nomina a Responsabile del Trattamento dei Dati Personali della Direzione Generale della Regione -DRG. *Data Processing Agreement* (DPA) ai sensi dell'Art. 28 del Regolamento Generale sulla Protezione dei Dati n. 679/2016 (GDPR – General Data Protection Regulation). In applicazione della Delibera ASL PE n. 353 del 19 aprile 2017 e della Delibera G.R.A.n. 780 del 20 dicembre 2017.**

Il presente accordo integra e specifica gli obblighi di protezione dei dati gravanti sulla ASL di

_____ (di seguito ASL Titolare) e la Direzione Generale della Regione - DRG. (di seguito anche Responsabile o ASL Responsabile) derivanti dall'esecuzione::

a) dell'Accordo Quadro recepito con Delibera G.R.A. n. 780 del 20 dicembre 2017, avente ad oggetto "Modifica e integrazione Decreto del Commissario ad Acta n. 114 del 28.09.2016 recante "Distribuzione di farmaci del PHT tramite le farmacie convenzionate con la modalità in nome e per conto (DPC) del SSR e attivazione del servizio Farmacup – Approvazione dell'Accordo Quadro Regionale con le associazioni delle farmacie pubbliche e private"- Provvedimenti" (di seguito "Accordo Quadro");

b) della Delibera ASL PE n. 353 del 19 aprile 2017 avente ad oggetto "Approvazione degli esiti della procedura negoziata volta alla aggiudicazione della fornitura – in licenza d'uso – del software per la gestione di una piattaforma web per la realizzazione della distribuzione per conto di farmaci PHT"- o, in ogni caso, derivanti dall'esecuzione, a qualunque titolo, da parte del Responsabile a favore della ASL PE di fornitura di un applicativo Web-DPC per garantire gli ordini dei farmaci oggetto dell'Accordo Quadro, e relativa installazione, manutenzione e/o l'assistenza tecnica, con particolare riferimento ai dati del Titolare e dei Terzi Interessati, ai sensi del Regolamento europeo n. 679 del 27 aprile 2016 **("GDPR");**

Il Responsabile e la ASL Titolare di seguito congiuntamente le **"Parti"** e ciascuna singolarmente la **"Parte".**

## Articolo 1 – Oggetto, natura, finalità e durata del trattamento

Il presente DPA si applica al trattamento dei dati personali svolto dal Responsabile ("Responsabile del Trattamento") per conto della ASL, quale titolare del trattamento ("Titolare del Trattamento"), ai sensi dell'Accordo Quadro e definisce gli obblighi delle Parti in materia di tutela dei dati personali.

Natura e finalità del trattamento: il Responsabile tratta i dati personali nella misura necessaria a fornire i servizi di cui all'Accordo Quadro. I servizi che possono essere svolti dal Responsabile sono indicati nell'Accordo Quadro e nella Delibera ASL PE n. 353/ 2017. I trattamenti autorizzati, ai sensi del presente DPA, sono indicati nell'Allegato 2.

Ciascuna Parte è esclusivamente responsabile per il proprio rispetto delle disposizioni di legge applicabili in materia di protezione dei dati personali.

La durata del trattamento dei dati personali dei Terzi Interessati da parte del Responsabile corrisponde alla durata dell'Accordo Quadro.

## Articolo 2 – Tipologie di dati personali e categorie di interessati

I soggetti i cui dati personali sono oggetto del trattamento da parte del Responsabile ai sensi del presente DPA possono essere, a titolo esemplificativo e non esaustivo, dipendenti e collaboratori della ASL Titolare, terzi incaricati, a qualunque titolo, dalla ASL Titolare, pazienti, controparti contrattuali della ASL Titolare e, in generale, terze parti rispetto alle quali la ASL Titolare agisce come titolare del trattamento dei dati personali ai sensi del GDPR (congiuntamente i "Terzi Interessati"). I dati personali trattati possono consistere, a titolo esemplificativo, in recapiti, dati identificativi, informazioni relative allo stato di salute, prescrizioni mediche, piani terapeutici.

## Articolo 3 – Istruzioni

Il Responsabile effettua il trattamento dei dati personali esclusivamente sulla base delle istruzioni ricevute dalla ASL Titolare in forma scritta: il dettaglio delle operazioni consentite è indicato nell'Allegato 3 al presente DPA. Il presente DPA e l'Accordo Quadro costituiscono parte delle istruzioni della ASL Titolare per il trattamento dei dati personali da parte del Responsabile e potranno essere integrate, in qualunque momento, da eventuali specifiche disposizioni, conformi alla legge applicabile in materia di Protezione dei Dati, ove ritenuto necessario da parte del Titolare.

Qualsiasi istruzione aggiuntiva o diversa rispetto a quanto previsto nell'Accordo Quadro e nel presente DPA dovrà essere trasmessa dalla ASL Titolare al Responsabile per iscritto e comunicata via PEC e/o raccomandata a/r. Tale istruzione aggiuntiva diverrà efficace entro 30 giorni dalla data di comunicazione.

## Articolo 4 – Riservatezza

Il Responsabile garantisce che i soggetti autorizzati al trattamento dei dati personali per proprio conto si siano impegnati contrattualmente a mantenere la riservatezza dei dati e siano soggetti a tale obbligo.

## Articolo 5 – Sicurezza del trattamento

Il Responsabile si impegna ad adottare le misure richieste dall'Art. 32 del GDPR.

In particolare - in considerazione dello stato dell'arte, dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché dei rischi derivanti, in particolare, dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trattati, il Responsabile si impegna a mettere in atto le misure tecniche e organizzative indicate nell'Allegato 1 al presente DPA di cui si richiede la compilazione per la descrizione delle modalità di implementazione.

Qualora il Responsabile intendesse apportare modifiche alle misure tecniche e organizzative descritte nell'Allegato 1, in considerazione del progresso e sviluppo tecnologico, effettuerà una preventiva

comunicazione alla ASL Titolare, fermo restando che tali modifiche non potranno comportare l'approntamento di un livello di protezione inferiore rispetto a quanto previsto nell'Allegato 1.


## Articolo 6 – Assistenza

Tenendo conto della natura del trattamento dei dati personali svolto dal Responsabile, come descritto nell'Accordo Quadro, il Responsabile si impegna ad assistere il Titolare, approntando le adeguate misure tecniche e organizzative, nella misura in cui ciò sia possibile, per consentire al Titolare di permettere ai Terzi Interessati l'esercizio dei diritti di cui agli Artt. da 12 a 23 del GDPR.

Il Responsabile dovrà informare il Titolare, senza ingiustificato ritardo, qualora un Terzo Interessato eserciti nei suoi confronti uno dei diritti di cui agli Artt. da 12 a 23 del GDPR.

Tenendo conto della natura del trattamento, come descritto nell'Accordo Quadro e nel presente DPA, e delle informazioni di volta in volta messe a disposizione, il Responsabile si impegna ad assistere il Titolare a garantire il rispetto degli obblighi di cui agli Artt. da 32 a 36 del GDPR

## Articolo 7 – Cancellazione

I dati personali di proprietà del Titolare che siano oggetto di trattamento da parte del Responsabile, nell'ambito dell'esecuzione delle attività previste dall'Accordo Quadro, in base ai termini di conservazione di tali trattamenti, opportunamente previsti nei registri di trattamento, devono essere periodicamente cancellati ove ne ricorra il termine. Alla cessazione dell'Accordo Quadro, ove applicabile, i dati oggetto di Trattamento da parte del Responsabile devono essere restituiti al Titolare, entro un termine di 30 giorni dalla cessazione da parte del Responsabile dei servizi in relazione ai quali viene eseguito il trattamento dei dati personali.

In mancanza di diverse istruzioni successive, il Titolare chiede sin d'ora al Responsabile, (e questi agli eventuali sub-responsabili) di procedere con la cancellazione di tutte le copie di dati personali in proprio possesso a seguito della cessazione, da parte del Responsabile, dei servizi in relazione ai quali esegue il trattamento dei dati personali, salvo che la legge applicabile obblighi il Responsabile alla conservazione dei dati personali trattati.

## Articolo 8 – Violazioni di Dati Personali (cd. "Data Breach")

Il Responsabile si impegna ad informare il Titolare, senza ingiustificato ritardo e comunque entro 12 ore dal momento in cui ne sia venuto a conoscenza, di ogni violazione della sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati Personali trasmessi, conservati o comunque trattati.

Il Responsabile si impegna inoltre, ai sensi dell'art. 28.3, lett. f), tenuto conto della natura del trattamento e delle informazioni a sua disposizione, a prestare ogni necessaria collaborazione al Titolare in relazione all'adempimento degli obblighi sullo stesso gravanti di notifica delle suddette violazioni all'Autorità ai sensi dell'art. 33 del GDPR o di comunicazione della stessa agli interessati ai sensi dell'art. 34 del GDPR.
La comunicazione dovrà avvenire a mezzo PEC/mail rispettivamente agli indirizzi _____ e _____.

## Articolo 9 – Valutazione D'impatto (CD. "DATA PROTECTION IMPACT ASSESSMENT")

Il Responsabile, ai sensi dell'art. 28.3, lett. f), s'impegna fin da ora, tenuto conto della natura del trattamento e delle informazioni a sua disposizione, a fornire al Titolare ogni elemento utile all'effettuazione, da parte di quest'ultimo, della valutazione di impatto sulla protezione dei dati, qualora il Titolare sia tenuto ad effettuarla ai sensi dell'art. 35 del Regolamento, nonché ogni collaborazione nell'effettuazione della eventuale consultazione preventiva al Garante da parte di quest'ultimo ai sensi dell'art. 36 del Regolamento stesso.

## Articolo 10 – Soggetti Autorizzati al Trattamento

Fatto salvo quanto previsto all'articolo 11, il Responsabile, garantisce che l'accesso ai Dati Personali sarà limitato esclusivamente ai propri dipendenti e collaboratori, previamente identificati per iscritto, il cui accesso ai Dati Personali sia necessario per l'esecuzione dei Servizi.

Il Responsabile si impegna a fornire ai propri dipendenti e collaboratori, deputati a trattare i Dati Personali del Titolare, le istruzioni necessarie per garantire un corretto, lecito e sicuro trattamento, curarne la formazione, vigilare sul loro operato, vincolarli alla riservatezza su tutte le informazioni acquisite nello svolgimento della loro attività, anche per il periodo successivo alla cessazione del rapporto di lavoro, e a comunicare al Titolare, su specifica richiesta, l'elenco aggiornato degli stessi.

## Articolo 11 – Sub-responsabili del Trattamento

Per l'esecuzione di specifiche attività per conto della ASL Titolare, il Responsabile, potrà avvalersi di sub-responsabili del trattamento (ciascuno un "Sub-responsabile del Trattamento") ai sensi del GDPR. I Sub-responsabili del Trattamento sono autorizzati a trattare dati personali dei Terzi Interessati esclusivamente allo scopo di eseguire le attività per le quali tali dati personali siano stati forniti al Responsabile ed è fatto loro divieto di trattare tali dati personali per altre finalità. Se il Responsabile, ricorrerà a Sub-responsabili del Trattamento, essi saranno vincolati, per iscritto, mediante un Accordo Quadro o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, agli stessi obblighi in materia di protezione dei dati contenuti nel presente DPA tra il Titolare del trattamento e il Responsabile,, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del regolamento. Qualora il sub-responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile, conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi del Sub-responsabile.

L'elenco completo dei Sub-responsabili del Trattamento che verranno eventualmente incaricati dal Responsabile, per l'esecuzione di attività di trattamento dei dati di cui all'Accordo Quadro dovrà essere previamente fornito alla ASL Titolare per la necessaria autorizzazione; tale autorizzazione dovrà essere richiesta dal Responsabile anche in caso di eventuali aggiornamenti a tale elenco.

Il Responsabile si impegna a informare anticipatamente il Titolare, anche con mezzi elettronici (indirizzi e-mail e/o PEC indicati all'art. 8 del presente DPA), laddove intenda includere un nuovo Sub-responsabile del Trattamento nell'elenco, intenda sostituire o cessare il rapporto con un Sub-responsabile del Trattamento esistente. La modifica si intenderà accettata dal Titolare laddove quest'ultimo non sollevi obiezioni per iscritto entro 3 (tre) mesi dalla ricezione della comunicazione da parte del Responsabile.

Qualora la ASL Titolare sollevi obiezioni su uno o più sub-responsabili del Trattamento, il Titolare darà indicazioni al Responsabile sulle relative motivazioni. In tal caso, il Responsabile potrà:

1. proporre altro Sub-responsabile del Trattamento in sostituzione del Sub-responsabile del Trattamento per il quale la ASL Titolare abbia sollevato obiezioni; o
2. adottare misure tese a superare le obiezioni della ASL Titolare (qualora le obiezioni fossero superabili).

Il Responsabile risponde nei confronti della ASL Titolare per l'adempimento del Sub-responsabile del Trattamento ai propri obblighi.

Nel caso in cui il Responsabile abbia necessità di ricorrere a un Sub-responsabile del Trattamento situato in un Paese terzo (extra UE), il Responsabile dovrà darne preventiva comunicazione al Titolare per l'approvazione e, eventualmente, per definire e concordare le modalità di trasferimento dei dati personali conformi a quanto previsto dagli Artt. 44 e seguenti del GDPR. Il Responsabile dovrà garantire inoltre che siano adottate adeguate misure tecniche e organizzative affinché il trattamento soddisfi i requisiti del GDPR, sia assicurata la protezione dei diritti dei Terzi Interessati e le opportune misure di sicurezza siano documentate.

## Articolo 12 – Amministratori di Sistema

Se applicabile, il Responsabile si impegna a conformarsi al Provvedimento generale del Garante per la protezione dei dati personali del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", così come modificato dal Provvedimento del Garante del 25 giugno 2009, e ad ogni altro pertinente provvedimento dell'Autorità.

In riferimento ai sistemi informatici di trattamento dei dati del Titolare per i quali il Responsabile eserciti attività di Amministrazione di Sistema, egli si impegna a:

1. designare quali amministratori di sistema le figure professionali dedicate alla gestione e alla manutenzione di impianti di elaborazione o di loro componenti con cui vengono effettuati trattamenti di Dati personali, fornendo al Titolare, su richiesta, informazioni sulle valutazioni effettuate per le designazioni;
2. effettuare un'elencazione analitica degli ambiti di operatività consentiti a ciascuno in base al relativo profilo di autorizzazione assegnato e fornendo, su richiesta, informazioni relative alle valutazioni alla base delle designazioni;
3. predisporre e conservare l'elenco contenente gli estremi identificativi delle persone fisiche qualificate quali amministratori di sistema e le funzioni ad essi attribuite;
4. comunicare periodicamente al Titolare l'elenco aggiornato degli amministratori di sistema, specificandone l'ambito di responsabilità (sistemi, database, reti, applicativi, etc.);
5. verificare annualmente l'operato degli amministratori di sistema, informando il Titolare circa le risultanze di tale verifica;
6. mantenere i file di log in conformità a quanto previsto nel suddetto provvedimento (qualora i sistemi siano installati presso le strutture del Responsabile o di suoi sub-Responsabili);
7. garantire una rigida separazione tra chi autorizza e/o assegna i privilegi di accesso e chi effettua le attività tecnico-sistemistiche.

## Articolo 13 – Rapporti con le Autorità

Il Responsabile, su richiesta del Titolare, si impegna a coadiuvare quest'ultimo nella difesa in caso di procedimenti dinanzi all'autorità di controllo o all'autorità giudiziaria che riguardino il trattamento dei Dati Personali di propria competenza.

## Articolo 14 – Ulteriori Obblighi e Responsabilità

Il Responsabile mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui alla normativa in materia di protezione dei dati personali e/o delle istruzioni del Titolare di cui al presente atto di designazione e consente al Titolare del trattamento l'esercizio del potere di controllo e ispezione, prestando ogni ragionevole collaborazione alle attività di audit effettuate dal Titolare stesso o da un altro soggetto da questi incaricato o autorizzato, con lo scopo di controllare l'adempimento degli obblighi e delle istruzioni di cui al presente atto.

Il Titolare darà comunicazione al Responsabile della propria intenzione di svolgere un Audit comunicandone l'oggetto, la tempistica, la data, e la durata dell'Audit.

Il Titolare fornirà al Responsabile una relazione scritta di natura confidenziale contenente il riepilogo dell'oggetto e dei risultati dell'Audit.

Il Responsabile si impegna altresì a:

1. effettuare almeno annualmente un rendiconto in ordine all'esecuzione delle istruzioni ricevute dal Titolare (e agli adempimenti eseguiti) ed alle conseguenti risultanze;
2. collaborare, se richiesto dalla ASL Titolare, con gli altri Responsabili del trattamento, al fine di armonizzare e coordinare l'intero processo di trattamento dei Dati Personali;

3. realizzare quant'altro sia ragionevolmente utile e/o necessario al fine di garantire l'adempimento degli obblighi previsti dalla normativa applicabile in materia di protezione dei dati, nei limiti dei compiti affidati con il presente atto di designazione;
4. informare prontamente il Titolare di ogni questione rilevante ai fini di legge, in particolar modo, a titolo esemplificativo e non esaustivo, nei casi in cui abbia notizia, in qualsiasi modo, che il trattamento dei Dati Personali violi la normativa in materia di protezione dei dati personali o presenti comunque rischi specifici per i diritti, le libertà fondamentali e/o la dignità dell'interessato o qualora, a suo parere, un'istruzione violi la normativa, nazionale o comunitaria, relativa alla protezione dei dati oppure qualora il Responsabile sia soggetto ad obblighi di legge che gli rendono illecito o impossibile agire secondo le istruzioni ricevute dalla ASL Titolare e/o conformarsi alla normativa o a provvedimenti dell'Autorità di Controllo.

Resta inteso che qualora il Responsabile (o eventuali suoi Sub-responsabili) determini autonomamente le finalità e i mezzi di trattamento in violazione delle istruzioni impartite dal Titolare, sarà considerato, a sua volta, Titolare del trattamento, assumendo i conseguenti oneri, rischi e responsabilità.

## Articolo 15 – Disposizioni Finali

Resta inteso che la presente designazione non comporta alcun diritto per il Responsabile ad uno specifico compenso o indennità o rimborso per l'attività svolta, né ad un incremento del compenso spettante allo stesso in virtù del Accordo Quadro con la ASL Titolare.

Gli allegati alla presente designazione fanno parte integrante della stessa.

Per tutto quanto non previsto dal presente atto di designazione si rinvia alle disposizioni generali vigenti ed applicabili in materia di protezione dei dati personali.

Il mancato riscontro alle presenti istruzioni non consentirà di dare attuazione di quanto previsto nell'Accordo Quadro.

Una volta dato riscontro positivo alla presente nomina, resta inteso che la mancata esecuzione delle istruzioni ivi contenute, costituisce una violazione del Regolamento UE 2016/679.

IL DIRETTORE GENERALE

Dr. _____

Per ricezione ed integrale accettazione del Responsabile

LA Direzione Generale della Regione

_____

# ALLEGATO 1 – Principi, Diritti e Misure Tecniche e Organizzative

Si chiede di descrivere le modalità per garantire, per quanto di competenza, il rispetto dei seguenti principi di trattamento e diritti degli interessati, secondo le indicazioni del Regolamento UE 679/2016, nell'ambito delle attività svolte per conto del Titolare; in alternativa indicare se siano ritenute non applicabili e darne motivazione o siano state programmate azioni ed eventuali scadenze.

| Req. | Principi e Diritti (riferimenti agli articoli del Reg. UE 679/2016) | Adottata (SI/NO) | Descrizione |
|---|---|---|---|
| A.1 | Art. 5.1.a e Art. 7 – Liceità e Gestione Consenso al Trattamento | | |
| A.2 | Art. 5.1.c minimizzazione dei dati | | |
| A.3 | Art. 5.1.e Limitazione della conservazione (art. 13 del Regolamento) | | |
| A.4 | Art. 15 Diritto di Accesso | | |
| A.5 | Art. 16 – Diritto di Rettifica | | |
| A.6 | Art. 17 – Diritto alla Cancellazione | | |
| A.7 | Art. 18 – Diritto alla Limitazione del Trattamento | | |
| A.8 | Art. 20 – Diritto alla portabilità dei dati | | |

Si chiede di descrivere quali delle seguenti misure tecniche e organizzative siano state adottate nell'ambito dei prodotti e/o servizi forniti alla ASL Titolare o se siano state programmate azioni di implementazione ed eventuali scadenze; in alternativa indicare se siano ritenute non applicabili e darne motivazione.

| Req. | Misura | Dettaglio | Adottata (SI/NO) | Descrizione/Motivazione |
|---|---|---|---|---|
| B.1 | **Politiche per la protezione dei dati** | Politiche per la protezione dei dati personali, sicurezza delle informazioni e conservazione | | |
| B.2 | **Organizzazione per la protezione dei dati** | Articolazione dell'organizzazione per la Protezione dei Dati Personali (DPO, Responsabili, ecc...) | | |
| B.3 | **Gestione della Sicurezza dei Dati da parte delle risorse umane (dipendenti/collaboratori)** | Procedure di ingresso di nuovi dipendenti/collaboratori, cambiamento di mansioni e/o cessazione del rapporto di lavoro.<br>Piano di Formazione periodica sulla Protezione dei Dati Personali | | |
| B.4 | **Gestione degli asset (dati personali e strumenti di supporto)** | Classificazione, Censimento e Definizione delle Responsabilità dei dati personali e dei relativi supporti/strumenti di trattamento utilizzati | | |
| B.5 | **Controllo degli accessi logici e partizionamento dei dati** | Procedure di gestione degli accessi logici degli utenti a sistemi e applicazioni che trattano dati personali | | |
| B.6 | **Pseudonimizzazione** | Misure per garantire la pseudonimizzazione dei dati personali utilizzati nel servizio erogato | | |
| B.7 | **Cifratura** | Procedure e Criteri di utilizzo della cifratura | | |
| B.8 | **Controllo degli accessi fisici** | Procedura di definizione della sicurezza dei locali, delle aree di trattamento di dati personali e di gestione della sicurezza fisica delle apparecchiature (strumenti di supporto) | | |

| Req. | Misura | Dettaglio | Adottata (SI/NO) | Descrizione/Motivazione |
|---|---|---|---|---|
| B.9 | **Sicurezza delle attività operative e manutenzione** | Policies tecnico-organizzative (es.: Utilizzo dei dispositivi portatili, VPN, dispositivi personali, posta elettronica, ecc.)<br>Misure di sicurezza antivirus-antimalware<br>Procedure di Gestione dei Backup<br>Criteri e procedure per la raccolta di Log e Monitoraggio dei sistemi<br>Procedure di controllo dell'integrità degli strumenti di erogazione del servizio<br>Procedure di controllo delle vulnerabilità tecniche<br>Procedure di gestione delle Manutenzioni | |  |
| B.10 | **Sicurezza della rete e delle comunicazioni** | Procedure di gestione della sicurezza della rete<br>Procedure per la gestione del trasferimento di informazioni | | |
| B.11 | **Gestione dei sistemi applicativi** | Criteri per la definizione dei Requisiti di sicurezza dei sistemi utilizzati/da acquisire<br>Procedure operative per le operazioni di acquisizione, sviluppo e di manutenzione dei sistemi | | |
| B.12 | **Relazioni con i sub-fornitori** | Procedure e nomine per garantire la protezione dei dati personali trattati dai sub-fornitori | | |
| B.13 | **Gestione degli incidenti e delle Violazioni di dati personali** | Procedure di gestione degli incidenti sulla Sicurezza delle Informazioni e delle Violazioni di Dati Personali | | |
| B.14 | **Continuità Operativa** | Procedure di Gestione della Continuità Operativa del servizio<br>Misure per garantire la Sicurezza in condizioni di emergenza e degli strumenti atti a garantire la Continuità Operativa. | | |

| Req. | Misura | Dettaglio | Adottata (SI/NO) | Descrizione/Motivazione |
|---|---|---|---|---|
| B.15 | **Conformità e Audit** | Procedure per garantire il tempestivo aggiornamento normativo e l'adeguamento del servizio alle nuove indicazioni<br>Procedure di Audit interne per assicurare la sicurezza dei trattamenti sui sistemi in uso per la ASL Titolare (test, verifica e valutazione dell'efficacia delle misure tecniche e organizzative) | |  |
| B.16 | **Misure per il rispetto della Privacy by Design** | Ved. Reg. UE 679/2016 art. 25 | | |
| B.17 | **Misure per il rispetto della Privacy by Default** | Ved. Reg. UE 679/2016 art. 25 | | |
| B.18 | **DPO – Data Protection Officer (Responsabile della Protezione dei Dati)** | Si richiede di dare comunicazione, se nominato, degli estremi e dei riferimenti di contatto del Responsabile della Protezione Dati dell'organizzazione (RPD – DPO/Data Protection Officer) | | |
| B.19 | **Presenza di Polizza Cyber Risk** | Si richiede se la Vostra azienda sia dotata di **polizza cyber-risk e l'eventuale dettaglio della stessa** | | |
| B.20 | **Gestione del Cambiamento** | Si richiede se esista una **procedura di gestione dei cambiamenti (Change Management)** nelle modalità di erogazione del servizio (es.: cambiamenti infrastrutturali, cambiamenti organizzativi, ecc...). Si richiede di fornirne copia. | | |

# ALLEGATO 2 – Ambito del Trattamento

Sulla scorta degli atti d'ufficio risulta che le categorie di attività (art. 30.2 del Regolamento) svolte dal Responsabile, nell'ambito dei servizi erogati per conto della ASL Titolare, siano di supporto ai seguenti trattamenti censiti:

| Cod. | Sub. | Requisito | Descrizione |
|---|---|---|---|
| 1 | | **Trattamento 1** | Distribuzione di Farmaci del PHT tramite le Farmacie convenzionate con la modalità in nome e per conto (DPC) del SSR. |
| | 1.1 | Categorie di interessati | Pazienti |
| | 1.2 | Tipi di Dati Personali oggetto di trattamento (indicare se dati comuni, categorie particolari, dati relativi a condanne penali e reati | - Dati comuni<br>- Categorie particolari di dati personali (dati relativi alla salute) |
| | 1.3 | Finalità del trattamento | - Attività amministrative correlate a quelle di prevenzione, diagnosi, cura e riabilitazione<br>- Programmazione, gestione, controllo e valutazione dell'assistenza sanitaria |
| | 1.4 | Durata del trattamento | Fino alla cessazione per qualunque motivo del Accordo Quadro e/o, comunque, dei Servizi ovvero fino alla revoca anticipata per qualsiasi motivo da parte del Titolare |
| | 1.5 | Tempo di Conservazione | 5 anni salvo diverse istruzioni comunicate successivamente |

# ALLEGATO 3 – Categorie di attività di trattamento (30.2) e relativi impatti

In linea con l'approccio basato sul rischio previsto dal GDPR, il Titolare ha individuato per le seguenti categorie di attività relative al trattamento (operazioni di trattamento), secondo quanto previsto dall'Art. 30.2 del GDPR, il livello d'impatto potenziale (quindi considerato **prima dell'applicazione delle misure di sicurezza** adottate dal Titolare che del Responsabile) sui diritti e le libertà degli interessati ed il livello di impatto reale **dopo l'adozione delle misure di sicurezza** come di seguito indicato:

| ID | Trattamento (rif. Trattamenti Allegato 2) | Categorie di attività relative al trattamento (Operazioni di trattamento) | Appl. | Livello di Impatto Potenziale del Trattamento | Livello di Impatto Residuo del Trattamento (calcolato tenendo conto delle misure – All. 1) |
|---|---|---|---|---|---|
| 1 | Distribuzione di Farmaci del PHT tramite le Farmacie convenzionate con la modalità in nome e per conto (DPC) del SSR. | Raccolta | X | **Impatto Massimo** | **Impatto Trascurabile** |
| | | Registrazione | X | | |
| | | Organizzazione | X | | |
| | | Strutturazione | X | | |
| | | Conservazione | | | |
| | | Adattamento o Modifica | X | | |
| | | Estrazione | X | | |
| | | Consultazione | X | | |
| | | Uso | X | | |
| | | Comunicazione mediante trasmissione o qualsiasi altra forma di messa a disposizione | X | | |
| | | Raffronto o Interconnessione | | | |
| | | Limitazione | X | | |
| | | Cancellazione o Distruzione | | | |


Il livello di impatto indicato nella precedente tabella è relativo al valore valutato sia prima dell'adozione delle misure di sicurezza (colonna *"Livello di Impatto Potenziale"*), previste dall'Allegato 1, che successivamente all'implementazione delle stesse (colonna *"Livello di Impatto residuo"*).

I criteri di classificazione dei livelli di impatto adottati dal Titolare sono i seguenti:

- **Impatto trascurabile**: gli interessati coinvolti dal trattamento non saranno affetti da inconvenienti oppure possono incontrare alcuni inconvenienti che possono superare senza alcun problema (es. perdita di tempo per ripetere formalità, etc.);
- **Impatto limitato**: gli interessati coinvolti dal trattamento possono incontrare disagi significativi che però possono superare nonostante alcune difficoltà (es. interruzione temporanea del servizio fino a 8 ore);
- **Impatto significativo**: gli interessati coinvolti dal trattamento possono avere conseguenze significative che dovrebbero essere in grado di superare seppure con gravi difficoltà (es. interruzione temporanea del servizio oltre le 8 ore e fino e non oltre le 24 ore);
- **Impatto massimo**: gli interessati coinvolti dal trattamento possono incontrare conseguenze significative, o addirittura irreversibili, che non possono superare (es.: Interruzione del servizio oltre le 24 ore, impossibilità o perdita della possibilità di accesso ai servizi, mancato rispetto dei diritti dell'interessato – es.: diritto alla salute)

MMG / PLS

Allegato 4: d

# (INSERIRE LOGO)

## IL DIRETTORE GENERALE

Regione Abruzzo Dipartimento per la Salute e il Welfare

Prot. n. _____/ _____, lì _____

Preg.mo Dr._____

_____

**Oggetto: Accordo per la Nomina a Responsabile del Trattamento dei Dati Personali del Dr _____, in qualità di Medico di Medicina Generale / Pediatra di Libera Scelta. *Data Processing Agreement* (DPA) ai sensi dell'Art. 28 del Regolamento Generale sulla Protezione dei Dati n. 679/2016 (GDPR – General Data Protection Regulation) e delle vigenti normative in materia di Protezione dei Dati Personali. In applicazione della Delibera ASL PE n. 353 del 19 aprile 2017 e della Delibera G.R.A.n. 780 del 20 dicembre 2017.**

Il presente accordo integra e specifica gli obblighi di protezione dei dati gravanti sulla ASL di _____(di seguito ASL Titolare o Titolare) e il Dr. _____ (di seguito anche Responsabile) derivanti dall'esecuzione::

a) dell'Accordo Quadro recepito con Delibera G.R.A. n. 780 del 20 dicembre 2017, avente ad oggetto "Modifica e integrazione Decreto del Commissario ad Acta n. 114 del 28.09.2016 recante "Distribuzione di farmaci del PHT tramite le farmacie convenzionate con la modalità in nome e per conto (DPC) del SSR e attivazione del servizio Farmacup – Approvazione dell'Accordo Quadro Regionale con le associazioni delle farmacie pubbliche e private"- Provvedimenti" (di seguito "Accordo Quadro");

b) della Delibera ASL PE n. 353 del 19 aprile 2017 avente ad oggetto "Approvazione degli esiti della procedura negoziata volta alla aggiudicazione della fornitura – in licenza d'uso – del software per la gestione di una piattaforma web per la realizzazione della distribuzione per conto di farmaci PHT"- o, in ogni caso, derivanti dall'esecuzione, a qualunque titolo, da parte del Responsabile a favore della ASL PE di fornitura di un applicativo Web-DPC per garantire gli ordini dei farmaci oggetto dell'Accordo Quadro, e relativa installazione, manutenzione e/o l'assistenza tecnica, con particolare riferimento ai dati del Titolare e dei Terzi Interessati, ai sensi del Regolamento europeo n. 679 del 27 aprile 2016 **("GDPR")** e delle vigenti norme in materia di protezione dei dati personali;

Il Responsabile e la ASL Titolare di seguito congiuntamente le **"Parti"** e ciascuna singolarmente la **"Parte".**

## Articolo 1 – Oggetto, natura, finalità e durata del trattamento

Il presente DPA si applica al trattamento dei dati personali svolto dal Responsabile del trattamento ("Responsabile del Trattamento" o "Responsabile") per conto della ASL Titolare del trattamento ("Titolare del Trattamento" o "Titolare"), ai sensi dell'Accordo Quadro e definisce gli obblighi delle Parti in materia di tutela dei dati personali.

Natura e finalità del trattamento: il Responsabile tratta i dati personali nella misura necessaria a fornire i servizi di cui all'Accordo Quadro. I servizi che possono essere svolti dal Responsabile sono indicati nell'Accordo Quadro e nella Delibera ASL PE n. 353/ 2017. I trattamenti autorizzati, ai sensi del presente DPA, sono indicati nell'Allegato 2.

Ciascuna Parte è esclusivamente responsabile per il proprio rispetto delle disposizioni di legge applicabili in materia di protezione dei dati personali.

La durata del trattamento dei dati personali dei Terzi Interessati da parte del Responsabile corrisponde alla durata dell'Accordo Quadro.

## Articolo 2 – Tipologie di dati personali e categorie di interessati

I soggetti i cui dati personali sono oggetto del trattamento da parte del Responsabile ai sensi del presente DPA possono essere, a titolo esemplificativo e non esaustivo, dipendenti e collaboratori della ASL Titolare, terzi incaricati, a qualunque titolo, dalla ASL Titolare, pazienti, controparti contrattuali della ASL Titolare e, in generale, terze parti rispetto alle quali la ASL Titolare agisce come titolare del trattamento dei dati personali ai sensi del GDPR (congiuntamente i "Terzi Interessati"). I dati personali trattati possono consistere, a titolo esemplificativo, in recapiti, dati identificativi, informazioni relative allo stato di salute, prescrizioni mediche, piani terapeutici.

## Articolo 3 – Istruzioni

Il Responsabile effettua il trattamento dei dati personali esclusivamente sulla base delle istruzioni ricevute dalla ASL Titolare in forma scritta: il dettaglio delle operazioni consentite è indicato nell'Allegato 3 al presente DPA. Il presente DPA e l'Accordo Quadro costituiscono parte delle istruzioni della ASL Titolare per il trattamento dei dati personali da parte del Responsabile e potranno essere integrate, in qualunque momento, da eventuali specifiche disposizioni, conformi alla legge applicabile in materia di Protezione dei Dati, ove ritenuto necessario da parte del Titolare.

Qualsiasi istruzione aggiuntiva o diversa rispetto a quanto previsto nell'Accordo Quadro e nel presente DPA dovrà essere trasmessa dalla ASL Titolare al Responsabile per iscritto e comunicata via PEC e/o raccomandata a/r. Tale istruzione aggiuntiva diverrà efficace entro 30 giorni dalla data di comunicazione.

## Articolo 4 – Riservatezza

Il Responsabile garantisce che i soggetti autorizzati al trattamento dei dati personali per proprio conto si siano impegnati contrattualmente a mantenere la riservatezza dei dati e siano soggetti a tale obbligo.

## Articolo 5 – Sicurezza del trattamento

Il Responsabile si impegna ad adottare le misure richieste dall'Art. 32 del GDPR.

In particolare - in considerazione dello stato dell'arte, dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché dei rischi derivanti, in particolare, dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trattati, il Responsabile si impegna a mettere in atto le misure tecniche e organizzative indicate nell'Allegato 1 al presente DPA di cui si richiede la compilazione per la descrizione delle modalità di implementazione.

Qualora il Responsabile intendesse apportare modifiche alle misure tecniche e organizzative descritte nell'Allegato 1, in considerazione del progresso e sviluppo tecnologico, effettuerà una preventiva comunicazione alla ASL Titolare, fermo restando che tali modifiche non potranno comportare l'approntamento di un livello di protezione inferiore rispetto a quanto previsto nell'Allegato 1.

## Articolo 6 – Assistenza

Tenendo conto della natura del trattamento dei dati personali svolto dal Responsabile, come descritto nell'Accordo Quadro, il Responsabile si impegna ad assistere il Titolare, approntando le adeguate misure tecniche e organizzative, nella misura in cui ciò sia possibile, per consentire al Titolare di permettere ai Terzi Interessati l'esercizio dei diritti di cui agli Artt. da 12 a 23 del GDPR.

Il Responsabile dovrà informare il Titolare, senza ingiustificato ritardo, qualora un Terzo Interessato eserciti nei suoi confronti uno dei diritti di cui agli Artt. da 12 a 23 del GDPR.

Tenendo conto della natura del trattamento, come descritto nell'Accordo Quadro e nel presente DPA, e delle informazioni di volta in volta messe a disposizione, il Responsabile si impegna ad assistere il Titolare a garantire il rispetto degli obblighi di cui agli Artt. da 32 a 36 del GDPR

## Articolo 7 – Cancellazione

I dati personali di proprietà del Titolare che siano oggetto di trattamento da parte del Responsabile, nell'ambito dell'esecuzione delle attività previste dall'Accordo Quadro, in base ai termini di conservazione di tali trattamenti, opportunamente previsti nei registri di trattamento, devono essere periodicamente cancellati ove ne ricorra il termine. Alla cessazione dell'Accordo Quadro, ove applicabile, i dati oggetto di Trattamento da parte del Responsabile devono essere restituiti al Titolare, entro un termine di 30 giorni dalla cessazione da parte del Responsabile dei servizi in relazione ai quali viene eseguito il trattamento dei dati personali.

In mancanza di diverse istruzioni successive, il Titolare chiede sin d'ora al Responsabile, (e questi agli eventuali sub-responsabili) di procedere con la cancellazione di tutte le copie di dati personali in proprio possesso a seguito della cessazione, da parte del Responsabile, dei servizi in relazione ai quali esegue il trattamento dei dati personali, salvo che la legge applicabile obblighi il Responsabile alla conservazione dei dati personali trattati.

## Articolo 8 – Violazioni di Dati Personali (cd. "Data Breach")

Il Responsabile si impegna ad informare il Titolare, senza ingiustificato ritardo e comunque entro 12 ore dal momento in cui ne sia venuto a conoscenza, di ogni violazione della sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati Personali trasmessi, conservati o comunque trattati.

Il Responsabile si impegna inoltre, ai sensi dell'art. 28.3, lett. f), tenuto conto della natura del trattamento e delle informazioni a sua disposizione, a prestare ogni necessaria collaborazione al Titolare in relazione all'adempimento degli obblighi sullo stesso gravanti di notifica delle suddette violazioni all'Autorità ai sensi dell'art. 33 del GDPR o di comunicazione della stessa agli interessati ai sensi dell'art. 34 del GDPR.
La comunicazione dovrà avvenire a mezzo PEC/mail rispettivamente agli indirizzi _____ e _____.

## Articolo 9 – Valutazione D'impatto (CD. "DATA PROTECTION IMPACT ASSESSMENT")

Il Responsabile, ai sensi dell'art. 28.3, lett. f), s'impegna fin da ora, tenuto conto della natura del trattamento e delle informazioni a sua disposizione, a fornire al Titolare ogni elemento utile all'effettuazione, da parte di quest'ultimo, della valutazione di impatto sulla protezione dei dati, qualora il Titolare sia tenuto ad effettuarla

ai sensi dell'art. 35 del Regolamento, nonché ogni collaborazione nell'effettuazione della eventuale consultazione preventiva al Garante da parte di quest'ultimo ai sensi dell'art. 36 del Regolamento stesso.

## Articolo 10 – Soggetti Autorizzati al Trattamento

Fatto salvo quanto previsto all'articolo 11, il Responsabile, garantisce che l'accesso ai Dati Personali sarà limitato esclusivamente ai propri dipendenti e collaboratori, previamente identificati per iscritto, il cui accesso ai Dati Personali sia necessario per l'esecuzione dei Servizi.

Il Responsabile si impegna a fornire ai propri dipendenti e collaboratori, deputati a trattare i Dati Personali del Titolare, le istruzioni necessarie per garantire un corretto, lecito e sicuro trattamento, curarne la formazione, vigilare sul loro operato, vincolarli alla riservatezza su tutte le informazioni acquisite nello svolgimento della loro attività, anche per il periodo successivo alla cessazione del rapporto di lavoro, e a comunicare al Titolare, su specifica richiesta, l'elenco aggiornato degli stessi.

## Articolo 11 – Sub-responsabili del Trattamento

Per l'esecuzione di specifiche attività per conto della ASL Titolare, il Responsabile, potrà avvalersi di sub-responsabili del trattamento (ciascuno un "Sub-responsabile del Trattamento") ai sensi del GDPR. I Sub-responsabili del Trattamento sono autorizzati a trattare dati personali dei Terzi Interessati esclusivamente allo scopo di eseguire le attività per le quali tali dati personali siano stati forniti al Responsabile ed è fatto loro divieto di trattare tali dati personali per altre finalità. Se il Responsabile, ricorrerà a Sub-responsabili del Trattamento, essi saranno vincolati, per iscritto, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, agli stessi obblighi in materia di protezione dei dati contenuti nel presente DPA tra il Titolare del trattamento e il Responsabile,, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del regolamento. Qualora il sub-responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile, conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi del Sub-responsabile.

L'elenco completo dei Sub-responsabili del Trattamento che verranno eventualmente incaricati dal Responsabile, per l'esecuzione di attività di trattamento dei dati di cui all'Accordo Quadro dovrà essere previamente fornito alla ASL Titolare per la necessaria autorizzazione; tale autorizzazione dovrà essere richiesta dal Responsabile anche in caso di eventuali aggiornamenti a tale elenco.

Il Responsabile si impegna a informare anticipatamente il Titolare, anche con mezzi elettronici (indirizzi e-mail e/o PEC indicati all'art. 8 del presente DPA), laddove intenda includere un nuovo Sub-responsabile del Trattamento nell'elenco, intenda sostituire o cessare il rapporto con un Sub-responsabile del Trattamento esistente. La modifica si intenderà accettata dal Titolare laddove quest'ultimo non sollevi obiezioni per iscritto entro 3 (tre) mesi dalla ricezione della comunicazione da parte del Responsabile.

Qualora la ASL Titolare sollevi obiezioni su uno o più sub-responsabili del Trattamento, il Titolare darà indicazioni al Responsabile sulle relative motivazioni. In tal caso, il Responsabile potrà:

1. proporre altro Sub-responsabile del Trattamento in sostituzione del Sub-responsabile del Trattamento per il quale la ASL Titolare abbia sollevato obiezioni; o
2. adottare misure tese a superare le obiezioni della ASL Titolare (qualora le obiezioni fossero superabili).

Il Responsabile risponde nei confronti della ASL Titolare per l'adempimento del Sub-responsabile del Trattamento ai propri obblighi.

Nel caso in cui il Responsabile abbia necessità di ricorrere a un Sub-responsabile del Trattamento situato in un Paese terzo (extra UE), il Responsabile dovrà darne preventiva comunicazione al Titolare per l'approvazione e, eventualmente, per definire e concordare le modalità di trasferimento dei dati personali conformi a quanto previsto dagli Artt. 44 e seguenti del GDPR. Il Responsabile dovrà garantire inoltre che siano adottate adeguate misure tecniche e organizzative affinché il trattamento soddisfi i requisiti del GDPR,

sia assicurata la protezione dei diritti dei Terzi Interessati e le opportune misure di sicurezza siano documentate.

## Articolo 12 – Amministratori di Sistema

Il Responsabile si impegna a conformarsi al Provvedimento generale del Garante per la protezione dei dati personali del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", così come modificato dal Provvedimento del Garante del 25 giugno 2009, e ad ogni altro pertinente provvedimento dell'Autorità.

In riferimento ai sistemi informatici di trattamento dei dati del Titolare per i quali il Responsabile eserciti attività di Amministrazione di Sistema, egli si impegna a:

1. designare quali amministratori di sistema le figure professionali dedicate alla gestione e alla manutenzione di impianti di elaborazione o di loro componenti con cui vengono effettuati trattamenti di Dati personali, fornendo al Titolare, su richiesta, informazioni sulle valutazioni effettuate per le designazioni;
2. effettuare un'elencazione analitica degli ambiti di operatività consentiti a ciascuno in base al relativo profilo di autorizzazione assegnato e fornendo, su richiesta, informazioni relative alle valutazioni alla base delle designazioni;
3. predisporre e conservare l'elenco contenente gli estremi identificativi delle persone fisiche qualificate quali amministratori di sistema e le funzioni ad essi attribuite;
4. comunicare periodicamente al Titolare l'elenco aggiornato degli amministratori di sistema, specificandone l'ambito di responsabilità (sistemi, database, reti, applicativi, etc.);
5. verificare annualmente l'operato degli amministratori di sistema, informando il Titolare circa le risultanze di tale verifica;
6. mantenere i file di log in conformità a quanto previsto nel suddetto provvedimento (qualora i sistemi siano installati presso le strutture del Responsabile o di suoi sub-Responsabili);
7. garantire una rigida separazione tra chi autorizza e/o assegna i privilegi di accesso e chi effettua le attività tecnico-sistemistiche.

## Articolo 13 – Rapporti con le Autorità

Il Responsabile, su richiesta del Titolare, si impegna a coadiuvare quest'ultimo nella difesa in caso di procedimenti dinanzi all'autorità di controllo o all'autorità giudiziaria che riguardino il trattamento dei Dati Personali di propria competenza.

## Articolo 14 – Ulteriori Obblighi e Responsabilità

Il Responsabile mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui alla normativa in materia di protezione dei dati personali e/o delle istruzioni del Titolare di cui al presente atto di designazione e consente al Titolare del trattamento l'esercizio del potere di controllo e ispezione, prestando ogni ragionevole collaborazione alle attività di audit effettuate dal Titolare stesso o da un altro soggetto da questi incaricato o autorizzato, con lo scopo di controllare l'adempimento degli obblighi e delle istruzioni di cui al presente atto.

Il Titolare darà comunicazione al Responsabile della propria intenzione di svolgere un Audit comunicandone l'oggetto, la tempistica, la data, e la durata dell'Audit.

Il Titolare fornirà al Responsabile una relazione scritta di natura confidenziale contenente il riepilogo dell'oggetto e dei risultati dell'Audit.

Il Responsabile si impegna altresì a:

1. effettuare almeno annualmente un rendiconto in ordine all'esecuzione delle istruzioni ricevute dal Titolare (e agli adempimenti eseguiti) ed alle conseguenti risultanze;

2. collaborare, se richiesto dalla ASL Titolare, con gli altri Responsabili del trattamento, al fine di armonizzare e coordinare l'intero processo di trattamento dei Dati Personali;
3. realizzare quant'altro sia ragionevolmente utile e/o necessario al fine di garantire l'adempimento degli obblighi previsti dalla normativa applicabile in materia di protezione dei dati, nei limiti dei compiti affidati con il presente atto di designazione;
4. informare prontamente il Titolare di ogni questione rilevante ai fini di legge, in particolar modo, a titolo esemplificativo e non esaustivo, nei casi in cui abbia notizia, in qualsiasi modo, che il trattamento dei Dati Personali violi la normativa in materia di protezione dei dati personali o presenti comunque rischi specifici per i diritti, le libertà fondamentali e/o la dignità dell'interessato o qualora, a suo parere, un'istruzione violi la normativa, nazionale o comunitaria, relativa alla protezione dei dati oppure qualora il Responsabile sia soggetto ad obblighi di legge che gli rendono illecito o impossibile agire secondo le istruzioni ricevute dalla ASL Titolare e/o conformarsi alla normativa o a provvedimenti dell'Autorità di Controllo.

Resta inteso che qualora il Responsabile (o eventuali suoi Sub-responsabili) determini autonomamente le finalità e i mezzi di trattamento in violazione delle istruzioni impartite dal Titolare, sarà considerato, a sua volta, Titolare del trattamento, assumendo i conseguenti oneri, rischi e responsabilità.

## Articolo 15 – Disposizioni Finali

Resta inteso che la presente designazione non comporta alcun diritto per il Responsabile ad uno specifico compenso o indennità o rimborso per l'attività svolta, né ad un incremento del compenso spettante allo stesso in virtù del Contratto con la ASL Titolare.

Gli allegati alla presente designazione fanno parte integrante della stessa.

Per tutto quanto non previsto dal presente atto di designazione si rinvia alle disposizioni generali vigenti ed applicabili in materia di protezione dei dati personali.

Il mancato riscontro alle presenti istruzioni non consentirà di dare attuazione di quanto previsto nell'Accordo Quadro.

Una volta dato riscontro positivo alla presente nomina, resta inteso che la mancata esecuzione delle istruzioni ivi contenute, costituisce una violazione del Regolamento UE 2016/679.

IL DIRETTORE GENERALE

Dr. _____

Per ricezione ed integrale accettazione del Responsabile

Il Dr.

_____

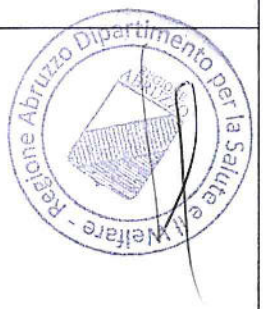

# ALLEGATO 1 – Principi, Diritti e Misure Tecniche e Organizzative

Si chiede di descrivere le modalità per garantire, per quanto di competenza, il rispetto dei seguenti principi di trattamento e diritti degli interessati, secondo le indicazioni del Regolamento UE 679/2016, nell'ambito delle attività svolte per conto del Titolare; in alternativa indicare se siano ritenute non applicabili e darne motivazione o siano state programmate azioni ed eventuali scadenze.

| Req. | Principi e Diritti (riferimenti agli articoli del Reg. UE 679/2016) | Adottata (SI/NO) | Descrizione |
|---|---|---|---|
| A.1 | Art. 5.1.a e Art. 7 – Liceità e Gestione Consenso al Trattamento | | |
| A.2 | Art. 5.1.c minimizzazione dei dati | | |
| A.3 | Art. 5.1.e Limitazione della conservazione (art. 13 del Regolamento) | | |
| A.4 | Art. 15 Diritto di Accesso | | |
| A.5 | Art. 16 – Diritto di Rettifica | | |
| A.6 | Art. 17 – Diritto alla Cancellazione | | |
| A.7 | Art. 18 – Diritto alla Limitazione del Trattamento | | |
| A.8 | Art. 20 – Diritto alla portabilità dei dati | | |

Si chiede di descrivere quali delle seguenti misure tecniche e organizzative siano state adottate nell'ambito dei prodotti e/o servizi forniti alla ASL Titolare o se siano state programmate azioni di implementazione ed eventuali scadenze; in alternativa indicare se siano ritenute non applicabili e darne motivazione.

| Req. | Misura | Dettaglio | Adottata (SI/NO) | Descrizione/Motivazione |
|---|---|---|---|---|
| B.1 | **Politiche per la protezione dei dati** | Politiche per la protezione dei dati personali, sicurezza delle informazioni e conservazione | | |
| B.2 | **Organizzazione per la protezione dei dati** | Articolazione dell'organizzazione per la Protezione dei Dati Personali (DPO, Responsabili, ecc...) | | |
| B.3 | **Gestione della Sicurezza dei Dati da parte delle risorse umane (dipendenti/collaboratori)** | Procedure di ingresso di nuovi dipendenti/collaboratori, cambiamento di mansioni e/o cessazione del rapporto di lavoro.<br>Piano di Formazione periodica sulla Protezione dei Dati Personali | | |
| B.4 | **Gestione degli asset (dati personali e strumenti di supporto)** | Classificazione, Censimento e Definizione delle Responsabilità dei dati personali e dei relativi supporti/strumenti di trattamento utilizzati | | |
| B.5 | **Controllo degli accessi logici e partizionamento dei dati** | Procedure di gestione degli accessi logici degli utenti a sistemi e applicazioni che trattano dati personali | | |
| B.6 | **Pseudonimizzazione** | Misure per garantire la pseudonimizzazione dei dati personali utilizzati nel servizio erogato | | |
| B.7 | **Cifratura** | Procedure e Criteri di utilizzo della cifratura | | |
| B.8 | **Controllo degli accessi fisici** | Procedura di definizione della sicurezza dei locali, delle aree di trattamento di dati personali e di gestione della sicurezza fisica delle apparecchiature (strumenti di supporto) | | |

| Req. | Misura | Dettaglio | Adottata (SI/NO) | Descrizione/Motivazione |
|---|---|---|---|---|
| B.9 | **Sicurezza delle attività operative e manutenzione** | Policies tecnico-organizzative (es.: Utilizzo dei dispositivi portatili, VPN, dispositivi personali, posta elettronica, ecc.)<br>Misure di sicurezza antivirus-antimalware<br>Procedure di Gestione dei Backup<br>Criteri e procedure per la raccolta di Log e Monitoraggio dei sistemi<br>Procedure di controllo dell'integrità degli strumenti di erogazione del servizio<br>Procedure di controllo delle vulnerabilità tecniche<br>Procedure di gestione delle Manutenzioni | |  |
| B.10 | **Sicurezza della rete e delle comunicazioni** | Procedure di gestione della sicurezza della rete<br>Procedure per la gestione del trasferimento di informazioni | | |
| B.11 | **Gestione dei sistemi applicativi** | Criteri per la definizione dei Requisiti di sicurezza dei sistemi utilizzati/da acquisire<br>Procedure operative per le operazioni di acquisizione, sviluppo e di manutenzione dei sistemi | | |
| B.12 | **Relazioni con i sub-fornitori** | Procedure e nomine per garantire la protezione dei dati personali trattati dai sub-fornitori | | |
| B.13 | **Gestione degli incidenti e delle Violazioni di dati personali** | Procedure di gestione degli incidenti sulla Sicurezza delle Informazioni e delle Violazioni di Dati Personali | | |
| B.14 | **Continuità Operativa** | Procedure di Gestione della Continuità Operativa del servizio<br>Misure per garantire la Sicurezza in condizioni di emergenza e degli strumenti atti a garantire la Continuità Operativa. | | |

| Req. | Misura | Dettaglio | Adottata (SI/NO) | Descrizione/Motivazione |
|---|---|---|---|---|
| B.15 | **Conformità e Audit** | Procedure per garantire il tempestivo aggiornamento normativo e l'adeguamento del servizio alle nuove indicazioni<br>Procedure di Audit interne per assicurare la sicurezza dei trattamenti sui sistemi in uso per la ASL Titolare (test, verifica e valutazione dell'efficacia delle misure tecniche e organizzative) | | |
| B.16 | **Misure per il rispetto della Privacy by Design** | Ved. Reg. UE 679/2016 art. 25 | | |
| B.17 | **Misure per il rispetto della Privacy by Default** | Ved. Reg. UE 679/2016 art. 25 | | |
| B.18 | **DPO – Data Protection Officer (Responsabile della Protezione dei Dati)** | Si richiede di dare comunicazione, se nominato, degli estremi e dei riferimenti di contatto del Responsabile della Protezione Dati dell'organizzazione (RPD – DPO/Data Protection Officer) | | |
| B.19 | **Presenza di Polizza Cyber Risk** | Si richiede se la Vostra azienda sia dotata di **polizza cyber-risk e l'eventuale dettaglio della stessa** | | |
| B.20 | **Gestione del Cambiamento** | Si richiede se esista una **procedura di gestione dei cambiamenti (Change Management)** nelle modalità di erogazione del servizio (es.: cambiamenti infrastrutturali, cambiamenti organizzativi, ecc...). Si richiede di fornirne copia. | | |

# ALLEGATO 2 – Ambito del Trattamento

Sulla scorta degli atti d'ufficio risulta che le categorie di attività (art. 30.2 del Regolamento) svolte dal Responsabile, nell'ambito dei servizi erogati per conto della ASL Titolare, siano di supporto ai seguenti trattamenti censiti:

| Cod. | Sub. | Requisito | Descrizione |
|---|---|---|---|
| 1 | | **Trattamento 1** | Prescrizione Farmaci e Piani Terapeutici propedeutici alla Distribuzione di Farmaci del PHT tramite le Farmacie convenzionate con la modalità in nome e per conto (DPC) del SSR, previa prescrizione medica e Piano Terapeutico.. |
| | 1.1 | Categorie di interessati | Pazienti |
| | 1.2 | Tipi di Dati Personali oggetto di trattamento (indicare se dati comuni, categorie particolari, dati relativi a condanne penali e reati | - Dati comuni<br>- Categorie particolari di dati personali (dati relativi alla salute) |
| | 1.3 | Finalità del trattamento | - Attività amministrative correlate a quelle di prevenzione, diagnosi, cura e riabilitazione;<br>- Attività sanitarie correlate a quelle di prevenzione, diagnosi, cura e riabilitazione;<br>- Programmazione, gestione, controllo e valutazione dell'assistenza sanitaria;<br>- Attività certificatorie; |
| | 1.4 | Durata del trattamento | Se non diversamente stabilito da normativa di settore, fino alla cessazione per qualunque motivo del Contratto e/o, comunque, dei Servizi ovvero fino alla revoca anticipata per qualsiasi motivo da parte del Titolare |
| | 1.5 | Tempo di Conservazione | Se non diversamente stabilito da normativa di settore , 5 anni salvo diverse istruzioni comunicate successivamente |

# ALLEGATO 3 – Categorie di attività di trattamento (30.2) e relativi impatti

In linea con l'approccio basato sul rischio previsto dal GDPR, il Titolare ha individuato per le seguenti categorie di attività relative al trattamento (operazioni di trattamento), secondo quanto previsto dall'Art. 30.2 del GDPR, il livello d'impatto potenziale (quindi considerato **prima dell'applicazione delle misure di sicurezza** adottate dal Titolare che del Responsabile) sui diritti e le libertà degli interessati ed il livello di impatto reale **dopo l'adozione delle misure di sicurezza** come di seguito indicato:

| ID | Trattamento (rif. Trattamenti Allegato 2) | Categorie di attività relative al trattamento (Operazioni di trattamento) | Appl. | Livello di Impatto Potenziale del Trattamento | Livello di Impatto Residuo del Trattamento (calcolato tenendo conto delle misure – All. 1) |
|---|---|---|---|---|---|
| 1 | Prescrizione Farmaci e Piani Terapeutici propedeutici alla Distribuzione di Farmaci del PHT tramite le Farmacie convenzionate con la modalità in nome e per conto (DPC) del SSR. | Raccolta | X | **Impatto Massimo** | **Impatto Trascurabile** |
| | | Registrazione | X | | |
| | | Organizzazione | X | | |
| | | Strutturazione | X | | |
| | | Conservazione | X | | |
| | | Adattamento o Modifica | X | | |
| | | Estrazione | X | | |
| | | Consultazione | X | | |
| | | Uso | X | | |
| | | Comunicazione mediante trasmissione o qualsiasi altra forma di messa a disposizione | X | | |
| | | Raffronto o Interconnessione | | | |
| | | Limitazione | X | | |
| | | Cancellazione o Distruzione | | | |

Il livello di impatto indicato nella precedente tabella è relativo al valore valutato sia prima dell'adozione delle misure di sicurezza (colonna *"Livello di Impatto Potenziale"*), previste dall'Allegato 1, che successivamente all'implementazione delle stesse (colonna *"Livello di Impatto residuo"*).

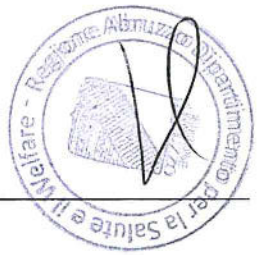
I criteri di classificazione dei livelli di impatto adottati dal Titolare sono i seguenti:

- **Impatto trascurabile**: gli interessati coinvolti dal trattamento non saranno affetti da inconvenienti oppure possono incontrare alcuni inconvenienti che possono superare senza alcun problema (es. perdita di tempo per ripetere formalità, etc.);
- **Impatto limitato**: gli interessati coinvolti dal trattamento possono incontrare disagi significativi che però possono superare nonostante alcune difficoltà (es. interruzione temporanea del servizio fino a 8 ore);
- **Impatto significativo**: gli interessati coinvolti dal trattamento possono avere conseguenze significative che dovrebbero essere in grado di superare seppure con gravi difficoltà (es. interruzione temporanea del servizio oltre le 8 ore e fino e non oltre le 24 ore);
- **Impatto massimo**: gli interessati coinvolti dal trattamento possono incontrare conseguenze significative, o addirittura irreversibili, che non possono superare (es.: Interruzione del servizio oltre le 24 ore, impossibilità o perdita della possibilità di accesso ai servizi, mancato rispetto dei diritti dell'interessato – es.: diritto alla salute)

Allegato 4 a

# (INSERIRE LOGO)

## IL DIRETTORE GENERALE



Prot. n. _____/ _____ _____, lì _____

Spett.le ASL PESCARA
Via Renato Paolini, 45
65124 Pescara
P.I. 01397530982

**Oggetto: Accordo per la Nomina a Responsabile del Trattamento dei Dati Personali della Asl Pescara. *Data Processing Agreement* (DPA) ai sensi dell'Art. 28 del Regolamento Generale sulla Protezione dei Dati n. 679/2016 (GDPR – General Data Protection Regulation) e delle vigenti normative in materia di Protezione dei Dati Personali. In applicazione della Delibera ASL PE n. 353 del 19 aprile 2017 e della Delibera G.R.A.n. 780 del 20 dicembre 2017.**

Il presente accordo integra e specifica gli obblighi di protezione dei dati gravanti sulla ASL di _____ (di seguito ASL Titolare o Titolare) e la Asl Pescara (di seguito anche Responsabile o ASL Responsabile) derivanti dall'esecuzione:

a) dell'Accordo Quadro recepito con Delibera G.R.A. n. 780 del 20 dicembre 2017, avente ad oggetto "Modifica e integrazione Decreto del Commissario ad Acta n. 114 del 28.09.2016 recante "Distribuzione di farmaci del PHT tramite le farmacie convenzionate con la modalità in nome e per conto (DPC) del SSR e attivazione del servizio Farmacup – Approvazione dell'Accordo Quadro Regionale con le associazioni delle farmacie pubbliche e private" – Provvedimenti (di seguito "Accordo Quadro");

b) della Delibera ASL PE n. 353 del 19 aprile 2017 avente ad oggetto "Approvazione degli esiti della procedura negoziata volta alla aggiudicazione della fornitura – in licenza d'uso – del software per la gestione di una piattaforma web per la realizzazione della distribuzione per conto di farmaci PHT"- o, in ogni caso, derivanti dall'esecuzione, a qualunque titolo, da parte del Responsabile a favore della ASL PE di fornitura di un applicativo Web-DPC per garantire gli ordini dei farmaci oggetto dell'Accordo Quadro, e relativa installazione, manutenzione e/o l'assistenza tecnica, con particolare riferimento ai dati del Titolare e dei Terzi Interessati, ai sensi del Regolamento europeo n. 679 del 27 aprile 2016 **("GDPR")** e delle vigenti norme in materia di protezione dei dati personali;

Il Responsabile e la ASL Titolare di seguito congiuntamente le **"Parti"** e ciascuna singolarmente la **"Parte".**

## Articolo 1 – Oggetto, natura, finalità e durata del trattamento

Il presente DPA si applica al trattamento dei dati personali svolto dal Responsabile ("Responsabile del Trattamento") per conto della ASL Titolare del trattamento ("Titolare del Trattamento"), ai sensi dell'Accordo Quadro e definisce gli obblighi delle Parti in materia di tutela dei dati personali.

Natura e finalità del trattamento: il Responsabile tratta i dati personali nella misura necessaria a fornire i servizi di cui all'Accordo Quadro. I servizi che possono essere svolti dal Responsabile sono indicati nell'Accordo Quadro e nella Delibera ASL PE n. 353/ 2017. I trattamenti autorizzati, ai sensi del presente DPA, sono indicati nell'Allegato 2.

Ciascuna Parte è esclusivamente responsabile per il proprio rispetto delle disposizioni di legge applicabili in materia di protezione dei dati personali.

La durata del trattamento dei dati personali dei Terzi Interessati da parte del Responsabile corrisponde alla durata dell'Accordo Quadro.

## Articolo 2 – Tipologie di dati personali e categorie di interessati

I soggetti i cui dati personali sono oggetto del trattamento da parte del Responsabile ai sensi del presente DPA possono essere, a titolo esemplificativo e non esaustivo, dipendenti e collaboratori della ASL Titolare, terzi incaricati, a qualunque titolo, dalla ASL Titolare, pazienti, controparti contrattuali della ASL Titolare e, in generale, terze parti rispetto alle quali la ASL Titolare agisce come titolare del trattamento dei dati personali ai sensi del GDPR (congiuntamente i "Terzi Interessati"). I dati personali trattati possono consistere, a titolo esemplificativo, in recapiti, dati identificativi, informazioni relative allo stato di salute, prescrizioni mediche, piani terapeutici.

## Articolo 3 – Istruzioni

Il Responsabile effettua il trattamento dei dati personali esclusivamente sulla base delle istruzioni ricevute dalla ASL Titolare in forma scritta: il dettaglio delle operazioni consentite è indicato nell'Allegato 3 al presente DPA. Il presente DPA e l'Accordo Quadro costituiscono parte delle istruzioni della ASL Titolare per il trattamento dei dati personali da parte del Responsabile e potranno essere integrate, in qualunque momento, da eventuali specifiche disposizioni, conformi alla legge applicabile in materia di Protezione dei Dati, ove ritenuto necessario da parte del Titolare.

Qualsiasi istruzione aggiuntiva o diversa rispetto a quanto previsto nell'Accordo Quadro e nel presente DPA dovrà essere trasmessa dalla ASL Titolare al Responsabile per iscritto e comunicata via PEC e/o raccomandata a/r. Tale istruzione aggiuntiva diverrà efficace entro 30 giorni dalla data di comunicazione.

## Articolo 4 – Riservatezza

Il Responsabile garantisce che i soggetti autorizzati al trattamento dei dati personali per proprio conto si siano impegnati contrattualmente a mantenere la riservatezza dei dati e siano soggetti a tale obbligo.

## Articolo 5 – Sicurezza del trattamento

Il Responsabile si impegna ad adottare le misure richieste dall'Art. 32 del GDPR.

In particolare - in considerazione dello stato dell'arte, dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché dei rischi derivanti, in particolare, dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trattati, il Responsabile si impegna a mettere in atto le misure tecniche e organizzative indicate nell'Allegato 1 al presente DPA di cui si richiede la compilazione per la descrizione delle modalità di implementazione.

Qualora il Responsabile intendesse apportare modifiche alle misure tecniche e organizzative descritte nell'Allegato 1, in considerazione del progresso e sviluppo tecnologico, effettuerà una preventiva

comunicazione alla ASL Titolare, fermo restando che tali modifiche non potranno comportare l'approntamento di un livello di protezione inferiore rispetto a quanto previsto nell'Allegato 1.


## Articolo 6 – Assistenza

Tenendo conto della natura del trattamento dei dati personali svolto dal Responsabile, come descritto nell'Accordo Quadro, il Responsabile si impegna ad assistere il Titolare, approntando le adeguate misure tecniche e organizzative, nella misura in cui ciò sia possibile, per consentire al Titolare di permettere ai Terzi Interessati l'esercizio dei diritti di cui agli Artt. da 12 a 23 del GDPR.

Il Responsabile dovrà informare il Titolare, senza ingiustificato ritardo, qualora un Terzo Interessato eserciti nei suoi confronti uno dei diritti di cui agli Artt. da 12 a 23 del GDPR.

Tenendo conto della natura del trattamento, come descritto nell'Accordo Quadro e nel presente DPA, e delle informazioni di volta in volta messe a disposizione, il Responsabile si impegna ad assistere il Titolare a garantire il rispetto degli obblighi di cui agli Artt. da 32 a 36 del GDPR

## Articolo 7 – Cancellazione

I dati personali di proprietà del Titolare che siano oggetto di trattamento da parte del Responsabile, nell'ambito dell'esecuzione delle attività previste dall'Accordo Quadro, in base ai termini di conservazione di tali trattamenti, opportunamente previsti nei registri di trattamento, devono essere periodicamente cancellati ove ne ricorra il termine. Alla cessazione dell'Accordo Quadro, ove applicabile, i dati oggetto di Trattamento da parte del Responsabile devono essere restituiti al Titolare, entro un termine di 30 giorni dalla cessazione da parte del Responsabile dei servizi in relazione ai quali viene eseguito il trattamento dei dati personali.

In mancanza di diverse istruzioni successive, il Titolare chiede sin d'ora al Responsabile, (e questi agli eventuali sub-responsabili) di procedere con la cancellazione di tutte le copie di dati personali in proprio possesso a seguito della cessazione, da parte del Responsabile, dei servizi in relazione ai quali esegue il trattamento dei dati personali, salvo che la legge applicabile obblighi il Responsabile alla conservazione dei dati personali trattati.

## Articolo 8 – Violazioni di Dati Personali (cd. "Data Breach")

Il Responsabile si impegna ad informare il Titolare, senza ingiustificato ritardo e comunque entro 12 ore dal momento in cui ne sia venuto a conoscenza, di ogni violazione della sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati Personali trasmessi, conservati o comunque trattati.

Il Responsabile si impegna inoltre, ai sensi dell'art. 28.3, lett. f), tenuto conto della natura del trattamento e delle informazioni a sua disposizione, a prestare ogni necessaria collaborazione al Titolare in relazione all'adempimento degli obblighi sullo stesso gravanti di notifica delle suddette violazioni all'Autorità ai sensi dell'art. 33 del GDPR o di comunicazione della stessa agli interessati ai sensi dell'art. 34 del GDPR.
La comunicazione dovrà avvenire a mezzo PEC/mail rispettivamente agli indirizzi _____ e _____.

## Articolo 9 – Valutazione D'impatto (CD. "DATA PROTECTION IMPACT ASSESSMENT")

Il Responsabile, ai sensi dell'art. 28.3, lett. f), s'impegna fin da ora, tenuto conto della natura del trattamento e delle informazioni a sua disposizione, a fornire al Titolare ogni elemento utile all'effettuazione, da parte di quest'ultimo, della valutazione di impatto sulla protezione dei dati, qualora il Titolare sia tenuto ad effettuarla ai sensi dell'art. 35 del Regolamento, nonché ogni collaborazione nell'effettuazione della eventuale consultazione preventiva al Garante da parte di quest'ultimo ai sensi dell'art. 36 del Regolamento stesso.


## Articolo 10 – Soggetti Autorizzati al Trattamento

Fatto salvo quanto previsto all'articolo 12, il Responsabile, garantisce che l'accesso ai Dati Personali sarà limitato esclusivamente ai propri dipendenti e collaboratori, previamente identificati per iscritto, il cui accesso ai Dati Personali sia necessario per l'esecuzione dei Servizi.

Il Responsabile si impegna a fornire ai propri dipendenti e collaboratori, deputati a trattare i Dati Personali del Titolare, le istruzioni necessarie per garantire un corretto, lecito e sicuro trattamento, curarne la formazione, vigilare sul loro operato, vincolarli alla riservatezza su tutte le informazioni acquisite nello svolgimento della loro attività, anche per il periodo successivo alla cessazione del rapporto di lavoro, e a comunicare al Titolare, su specifica richiesta, l'elenco aggiornato degli stessi.

## Articolo 11 – Nomina della ASL Pescara anche in qualità di Sub-responsabile del Trattamento

Per l'esecuzione delle attività previste dall'Accordo Quadro, la ASL Titolare, in qualità di Responsabile del Trattamento, per conto delle altre ASL abruzzesi, nomina la Asl Pescara anche Sub-responsabile del Trattamento.

## Articolo 12 – Sub-responsabili del Trattamento

Per l'esecuzione di specifiche attività per conto della ASL Titolare, il Responsabile, potrà avvalersi di sub-responsabili del trattamento (ciascuno un "Sub-responsabile del Trattamento") ai sensi del GDPR. I Sub-responsabili del Trattamento sono autorizzati a trattare dati personali dei Terzi Interessati esclusivamente allo scopo di eseguire le attività per le quali tali dati personali siano stati forniti al Responsabile ed è fatto loro divieto di trattare tali dati personali per altre finalità. Se il Responsabile, ricorrerà a Sub-responsabili del Trattamento, essi saranno vincolati, per iscritto, mediante un Accordo Quadro o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, agli stessi obblighi in materia di protezione dei dati contenuti nel presente DPA tra il Titolare del trattamento e il Responsabile, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del regolamento. Qualora il sub-responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile, conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi del Sub-responsabile.

L'elenco completo dei Sub-responsabili del Trattamento che verranno eventualmente incaricati dal Responsabile, per l'esecuzione di attività di trattamento dei dati di cui all'Accordo Quadro dovrà essere previamente fornito alla ASL Titolare per la necessaria autorizzazione; tale autorizzazione dovrà essere richiesta dal Responsabile anche in caso di eventuali aggiornamenti a tale elenco.

Il Responsabile si impegna a informare anticipatamente il Titolare, anche con mezzi elettronici (indirizzi e-mail e/o PEC indicati all'art. 8 del presente DPA), laddove intenda includere un nuovo Sub-responsabile del Trattamento nell'elenco, intenda sostituire o cessare il rapporto con un Sub-responsabile del Trattamento esistente. La modifica si intenderà accettata dal Titolare laddove quest'ultimo non sollevi obiezioni per iscritto entro 3 (tre) mesi dalla ricezione della comunicazione da parte del Responsabile.

Qualora la ASL Titolare sollevi obiezioni su uno o più sub-responsabili del Trattamento, il Titolare darà indicazioni al Responsabile sulle relative motivazioni. In tal caso, il Responsabile potrà:

1. proporre altro Sub-responsabile del Trattamento in sostituzione del Sub-responsabile del Trattamento per il quale la ASL Titolare abbia sollevato obiezioni; o
2. adottare misure tese a superare le obiezioni della ASL Titolare (qualora le obiezioni fossero superabili).

Il Responsabile risponde nei confronti della ASL Titolare per l'adempimento del Sub-responsabile del Trattamento ai propri obblighi.

Nel caso in cui il Responsabile abbia necessità di ricorrere a un Sub-responsabile del Trattamento situato in un Paese terzo (extra UE), il Responsabile dovrà darne preventiva comunicazione al Titolare per

l'approvazione e, eventualmente, per definire e concordare le modalità di trasferimento dei dati personali conformi a quanto previsto dagli Artt. 44 e seguenti del GDPR. Il Responsabile dovrà garantire inoltre che siano adottate adeguate misure tecniche e organizzative affinché il trattamento soddisfi i requisiti del GDPR, sia assicurata la protezione dei diritti dei Terzi Interessati e le opportune misure di sicurezza siano documentate.

## Articolo 13 – Amministratori di Sistema

Il Responsabile si impegna a conformarsi al Provvedimento generale del Garante per la protezione dei dati personali del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", così come modificato dal Provvedimento del Garante del 25 giugno 2009, e ad ogni altro pertinente provvedimento dell'Autorità.

In riferimento ai sistemi informatici di trattamento dei dati del Titolare per i quali il Responsabile eserciti attività di Amministrazione di Sistema, egli si impegna a:

1. designare quali amministratori di sistema le figure professionali dedicate alla gestione e alla manutenzione di impianti di elaborazione o di loro componenti con cui vengono effettuati trattamenti di Dati personali, fornendo al Titolare, su richiesta, informazioni sulle valutazioni effettuate per le designazioni;
2. effettuare un'elencazione analitica degli ambiti di operatività consentiti a ciascuno in base al relativo profilo di autorizzazione assegnato e fornendo, su richiesta, informazioni relative alle valutazioni alla base delle designazioni;
3. predisporre e conservare l'elenco contenente gli estremi identificativi delle persone fisiche qualificate quali amministratori di sistema e le funzioni ad essi attribuite;
4. comunicare periodicamente al Titolare l'elenco aggiornato degli amministratori di sistema, specificandone l'ambito di responsabilità (sistemi, database, reti, applicativi, etc.);
5. verificare annualmente l'operato degli amministratori di sistema, informando il Titolare circa le risultanze di tale verifica;
6. mantenere i file di log in conformità a quanto previsto nel suddetto provvedimento (qualora i sistemi siano installati presso le strutture del Responsabile o di suoi sub-Responsabili);
7. garantire una rigida separazione tra chi autorizza e/o assegna i privilegi di accesso e chi effettua le attività tecnico-sistemistiche.

## Articolo 14 – Rapporti con le Autorità

Il Responsabile, su richiesta del Titolare, si impegna a coadiuvare quest'ultimo nella difesa in caso di procedimenti dinanzi all'autorità di controllo o all'autorità giudiziaria che riguardino il trattamento dei Dati Personali di propria competenza.

## Articolo 15 – Ulteriori Obblighi e Responsabilità

Il Responsabile mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui alla normativa in materia di protezione dei dati personali e/o delle istruzioni del Titolare di cui al presente atto di designazione e consente al Titolare del trattamento l'esercizio del potere di controllo e ispezione, prestando ogni ragionevole collaborazione alle attività di audit effettuate dal Titolare stesso o da un altro soggetto da questi incaricato o autorizzato, con lo scopo di controllare l'adempimento degli obblighi e delle istruzioni di cui al presente atto.

Il Titolare darà comunicazione al Responsabile della propria intenzione di svolgere un Audit comunicandone l'oggetto, la tempistica, la data, e la durata dell'Audit.

Il Titolare fornirà al Responsabile una relazione scritta di natura confidenziale contenente il riepilogo dell'oggetto e dei risultati dell'Audit.

Il Responsabile si impegna altresì a:

1. effettuare almeno annualmente un rendiconto in ordine all'esecuzione delle istruzioni ricevute dal Titolare (e agli adempimenti eseguiti) ed alle conseguenti risultanze;
2. collaborare, se richiesto dalla ASL Titolare, con gli altri Responsabili del trattamento, al fine di armonizzare e coordinare l'intero processo di trattamento dei Dati Personali;
3. realizzare quant'altro sia ragionevolmente utile e/o necessario al fine di garantire l'adempimento degli obblighi previsti dalla normativa applicabile in materia di protezione dei dati, nei limiti dei compiti affidati con il presente atto di designazione;
4. informare prontamente il Titolare di ogni questione rilevante ai fini di legge, in particolar modo, a titolo esemplificativo e non esaustivo, nei casi in cui abbia notizia, in qualsiasi modo, che il trattamento dei Dati Personali violi la normativa in materia di protezione dei dati personali o presenti comunque rischi specifici per i diritti, le libertà fondamentali e/o la dignità dell'interessato o qualora, a suo parere, un'istruzione violi la normativa, nazionale o comunitaria, relativa alla protezione dei dati oppure qualora il Responsabile sia soggetto ad obblighi di legge che gli rendono illecito o impossibile agire secondo le istruzioni ricevute dalla ASL Titolare e/o conformarsi alla normativa o a provvedimenti dell'Autorità di Controllo.

Resta inteso che qualora il Responsabile (o eventuali suoi Sub-responsabili) determini autonomamente le finalità e i mezzi di trattamento in violazione delle istruzioni impartite dal Titolare, sarà considerato, a sua volta, Titolare del trattamento, assumendo i conseguenti oneri, rischi e responsabilità.

## Articolo 16 – Disposizioni Finali

Resta inteso che la presente designazione non comporta alcun diritto per il Responsabile ad uno specifico compenso o indennità o rimborso per l'attività svolta, né ad un incremento del compenso spettante allo stesso in virtù del Accordo Quadro con la ASL Titolare.

Gli allegati alla presente designazione fanno parte integrante della stessa.

Per tutto quanto non previsto dal presente atto di designazione si rinvia alle disposizioni generali vigenti ed applicabili in materia di protezione dei dati personali.

Il mancato riscontro alle presenti istruzioni non consentirà di dare attuazione di quanto previsto nell'Accordo Quadro.

Una volta dato riscontro positivo alla presente nomina, resta inteso che la mancata esecuzione delle istruzioni ivi contenute, costituisce una violazione del Regolamento UE 2016/679.

IL DIRETTORE GENERALE

Dr. _____

Per ricezione ed integrale accettazione
del Responsabile

ASL PESCARA

Dr. Armando Mancini


# ALLEGATO 1 – Principi, Diritti e Misure Tecniche e Organizzative

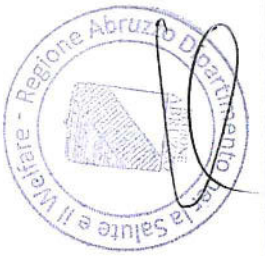
Si chiede di descrivere le modalità per garantire, per quanto di competenza, il rispetto dei seguenti principi di trattamento e diritti degli interessati, secondo le indicazioni del Regolamento UE 679/2016, nell'ambito delle attività svolte per conto del Titolare; in alternativa indicare se siano ritenute non applicabili e darne motivazione o siano state programmate azioni ed eventuali scadenze.

| Req. | Principi e Diritti (riferimenti agli articoli del Reg. UE 679/2016) | Adottata (SI/NO) | Descrizione |
|---|---|---|---|
| A.1 | Art. 5.1.a e Art. 7 – Liceità e Gestione Consenso al Trattamento | | |
| A.2 | Art. 5.1.c minimizzazione dei dati | | |
| A.3 | Art. 5.1.e Limitazione della conservazione (art. 13 del Regolamento) | | |
| A.4 | Art. 15 Diritto di Accesso | | |
| A.5 | Art. 16 – Diritto di Rettifica | | |
| A.6 | Art. 17 – Diritto alla Cancellazione | | |
| A.7 | Art. 18 – Diritto alla Limitazione del Trattamento | | |
| A.8 | Art. 20 – Diritto alla portabilità dei dati | | |

Si chiede di descrivere quali delle seguenti misure tecniche e organizzative siano state adottate nell'ambito dei prodotti e/o servizi forniti alla ASL Titolare o se siano state programmate azioni di implementazione ed eventuali scadenze; in alternativa indicare se siano ritenute non applicabili e darne motivazione.

| Req. | Misura | Dettaglio | Adottata (SI/NO) | Descrizione/Motivazione |
|---|---|---|---|---|
| B.1 | **Politiche per la protezione dei dati** | Politiche per la protezione dei dati personali, sicurezza delle informazioni e conservazione | | |
| B.2 | **Organizzazione per la protezione dei dati** | Articolazione dell'organizzazione per la Protezione dei Dati Personali (DPO, Responsabili, ecc...) | | |
| B.3 | **Gestione della Sicurezza dei Dati da parte delle risorse umane (dipendenti/collaboratori)** | Procedure di ingresso di nuovi dipendenti/collaboratori, cambiamento di mansioni e/o cessazione del rapporto di lavoro.<br>Piano di Formazione periodica sulla Protezione dei Dati Personali | | |
| B.4 | **Gestione degli asset (dati personali e strumenti di supporto)** | Classificazione, Censimento e Definizione delle Responsabilità dei dati personali e dei relativi supporti/strumenti di trattamento utilizzati | | |
| B.5 | **Controllo degli accessi logici e partizionamento dei dati** | Procedure di gestione degli accessi logici degli utenti a sistemi e applicazioni che trattano dati personali | | |
| B.6 | **Pseudonimizzazione** | Misure per garantire la pseudonimizzazione dei dati personali utilizzati nel servizio erogato | | |
| B.7 | **Cifratura** | Procedure e Criteri di utilizzo della cifratura | | |
| B.8 | **Controllo degli accessi fisici** | Procedura di definizione della sicurezza dei locali, delle aree di trattamento di dati personali e di gestione della sicurezza fisica delle apparecchiature (strumenti di supporto) | | |

| Req. | Misura | Dettaglio | Adottata (SI/NO) | Descrizione/Motivazione |
|---|---|---|---|---|
| B.9 | **Sicurezza delle attività operative e manutenzione** | Policies tecnico-organizzative (es.: Utilizzo dei dispositivi portatili, VPN, dispositivi personali, posta elettronica, ecc.)<br>Misure di sicurezza antivirus-antimalware<br>Procedure di Gestione dei Backup<br>Criteri e procedure per la raccolta di Log e Monitoraggio dei sistemi<br>Procedure di controllo dell'integrità degli strumenti di erogazione del servizio<br>Procedure di controllo delle vulnerabilità tecniche<br>Procedure di gestione delle Manutenzioni | | |
| B.10 | **Sicurezza della rete e delle comunicazioni** | Procedure di gestione della sicurezza della rete<br>Procedure per la gestione del trasferimento di informazioni | | |
| B.11 | **Gestione dei sistemi applicativi** | Criteri per la definizione dei Requisiti di sicurezza dei sistemi utilizzati/da acquisire<br>Procedure operative per le operazioni di acquisizione, sviluppo e di manutenzione dei sistemi | | |
| B.12 | **Relazioni con i sub-fornitori** | Procedure e nomine per garantire la protezione dei dati personali trattati dai sub-fornitori | | |
| B.13 | **Gestione degli incidenti e delle Violazioni di dati personali** | Procedure di gestione degli incidenti sulla Sicurezza delle Informazioni e delle Violazioni di Dati Personali | | |
| B.14 | **Continuità Operativa** | Procedure di Gestione della Continuità Operativa del servizio<br>Misure per garantire la Sicurezza in condizioni di emergenza e degli strumenti atti a garantire la Continuità Operativa. | | |

| Req. | Misura | Dettaglio | Adottata (SI/NO) | Descrizione/Motivazione |
|---|---|---|---|---|
| **B.15** | **Conformità e Audit** | Procedure per garantire il tempestivo aggiornamento normativo e l'adeguamento del servizio alle nuove indicazioni<br><br>Procedure di Audit interne per assicurare la sicurezza dei trattamenti sui sistemi in uso per la ASL Titolare (test, verifica e valutazione dell'efficacia delle misure tecniche e organizzative) | |  |
| **B.16** | **Misure per il rispetto della Privacy by Design** | Ved. Reg. UE 679/2016 art. 25 | | |
| **B.17** | **Misure per il rispetto della Privacy by Default** | Ved. Reg. UE 679/2016 art. 25 | | |
| **B.18** | **DPO – Data Protection Officer (Responsabile della Protezione dei Dati)** | Si richiede di dare comunicazione, se nominato, degli estremi e dei riferimenti di contatto del Responsabile della Protezione Dati dell'organizzazione (RPD – DPO/Data Protection Officer) | | |
| **B.19** | **Presenza di Polizza Cyber Risk** | Si richiede se la Vostra azienda sia dotata di **polizza cyber-risk e l'eventuale dettaglio della stessa** | | |
| **B.20** | **Gestione del Cambiamento** | Si richiede se esista una **procedura di gestione dei cambiamenti (Change Management)** nelle modalità di erogazione del servizio (es.: cambiamenti infrastrutturali, cambiamenti organizzativi, ecc…). Si richiede di fornirne copia. | | |

# ALLEGATO 2 – Ambito del Trattamento

Sulla scorta degli atti d'ufficio risulta che le categorie di attività (art. 30.2 del Regolamento) svolte dal Responsabile, nell'ambito dei servizi erogati per conto della ASL Titolare, siano di supporto ai seguenti trattamenti censiti:

| Cod. | Sub. | Requisito | Descrizione |
|---|---|---|---|
| 1 | | **Trattamento 1** | Distribuzione di Farmaci del PHT tramite le Farmacie convenzionate con la modalità in nome e per conto (DPC) del SSR. |
| | 1.1 | Categorie di interessati | Pazienti |
| | 1.2 | Tipi di Dati Personali oggetto di trattamento (indicare se dati comuni, categorie particolari, dati relativi a condanne penali e reati | - Dati comuni<br>- Categorie particolari di dati personali (dati relativi alla salute) |
| | 1.3 | Finalità del trattamento | - Attività amministrative correlate a quelle di prevenzione, diagnosi, cura e riabilitazione<br>- Programmazione, gestione, controllo e valutazione dell'assistenza sanitaria |
| | 1.4 | Durata del trattamento | Fino alla cessazione per qualunque motivo del Accordo Quadro e/o, comunque, dei Servizi ovvero fino alla revoca anticipata per qualsiasi motivo da parte del Titolare |
| | 1.5 | Tempo di Conservazione | 5 anni salvo diverse istruzioni comunicate successivamente |
| 2 | | **Trattamento 2** (descrizione del Trattamento) | Gestione utenze per l'accesso al sistema informatico per la DPC e relative registrazioni di attività |
| | 2.1 | Categorie di interessati | Dipendenti e collaboratori delle strutture coinvolte (Farmacie, MMG, Distributori, ASL) |
| | 2.2 | Tipo di Dati Personali oggetto di trattamento (indicare se dati comuni, categorie particolari, dati relativi a condanne penali e reati | - Dati comuni (dati anagrafici degli utenti) |
| | 2.3 | Finalità del trattamento | - Gestione delle utenze per il raggiungimento delle finalità di cui al punto 1.3 del presente allegato |
| | 2.4 | Durata del trattamento | Fino alla cessazione per qualunque motivo del Contratto e/o, comunque, dei Servizi ovvero fino alla revoca anticipata per qualsiasi motivo da parte del Titolare |
| | 2.5 | Tempo di Conservazione | 5 anni salvo diverse istruzioni comunicate successivamente |

# ALLEGATO 3 – Categorie di attività di trattamento (30.2) e relativi impatti

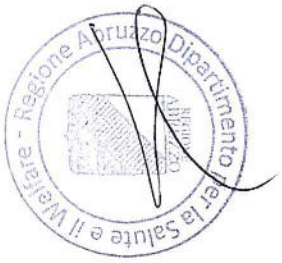
In linea con l'approccio basato sul rischio previsto dal GDPR, il Titolare ha individuato per le seguenti categorie di attività relative al trattamento (operazioni di trattamento), secondo quanto previsto dall'Art. 30.2 del GDPR, il livello d'impatto potenziale (quindi considerato **prima dell'applicazione delle misure di sicurezza** adottate dal Titolare che del Responsabile) sui diritti e le libertà degli interessati ed il livello di impatto reale **dopo l'adozione delle misure di sicurezza** come di seguito indicato:

| ID | Trattamento (rif. Trattamenti Allegato 2) | Categorie di attività relative al trattamento (Operazioni di trattamento) | Appl. | Livello di Impatto Potenziale del Trattamento | Livello di Impatto Residuo del Trattamento (calcolato tenendo conto delle misure – All. 1) |
|---|---|---|---|---|---|
| 1 | Distribuzione di Farmaci del PHT tramite le Farmacie convenzionate con la modalità in nome e per conto (DPC) del SSR. | Raccolta | | **Impatto Massimo** | **Impatto Trascurabile** |
| | | Registrazione | X | | |
| | | Organizzazione | X | | |
| | | Strutturazione | X | | |
| | | Conservazione | X | | |
| | | Adattamento o Modifica | | | |
| | | Estrazione | X | | |
| | | Consultazione | | | |
| | | Uso | | | |
| | | Comunicazione mediante trasmissione o qualsiasi altra forma di messa a disposizione | | | |
| | | Raffronto o Interconnessione | | | |
| | | Limitazione | X | | |
| | | Cancellazione o Distruzione | X | | |
| 2 | Gestione utenze per l'accesso al sistema informatico per la DPC e relative registrazioni di attività | Raccolta | X | **Impatto Massimo** | **Impatto Trascurabile** |
| | | Registrazione | X | | |
| | | Organizzazione | X | | |
| | | Strutturazione | X | | |
| | | Conservazione | X | | |
| | | Adattamento o Modifica | X | | |
| | | Estrazione | X | | |
| | | Consultazione (solo delle utenze) | X | | |
| | | Uso | | | |
| | | Comunicazione mediante trasmissione o qualsiasi altra forma di messa a disposizione | | | |
| | | Raffronto o Interconnessione | | | |
| | | Limitazione | X | | |
| | | Cancellazione o Distruzione | X | | |

Il livello di impatto indicato nella precedente tabella è relativo al valore valutato sia prima dell'adozione delle misure di sicurezza (colonna *"Livello di Impatto Potenziale"*), previste dall'Allegato 1, che successivamente all'implementazione delle stesse (colonna *"Livello di Impatto residuo"*).

I criteri di classificazione dei livelli di impatto adottati dal Titolare sono i seguenti:

- **Impatto trascurabile**: gli interessati coinvolti dal trattamento non saranno affetti da inconvenienti oppure possono incontrare alcuni inconvenienti che possono superare senza alcun problema (es. perdita di tempo per ripetere formalità, etc.);
- **Impatto limitato**: gli interessati coinvolti dal trattamento possono incontrare disagi significativi che però possono superare nonostante alcune difficoltà (es. interruzione temporanea del servizio fino a 8 ore);
- **Impatto significativo**: gli interessati coinvolti dal trattamento possono avere conseguenze significative che dovrebbero essere in grado di superare seppure con gravi difficoltà (es. interruzione temporanea del servizio oltre le 8 ore e fino e non oltre le 24 ore);
- **Impatto massimo**: gli interessati coinvolti dal trattamento possono incontrare conseguenze significative, o addirittura irreversibili, che non possono superare (es.: Interruzione del servizio oltre le 24 ore, impossibilità o perdita della possibilità di accesso ai servizi, mancato rispetto dei diritti dell'interessato – es.: diritto alla salute)



Allegato 4

# AZIENDA SANITARIA LOCALE DI PESCARA

Azienda Pubblica

Sede Legale:
Via Renato Paolini, 45
65124 Pescara
P. IVA 01397530982

## IL DIRETTORE GENERALE

Prot. n. _____/ Pescara, lì _____

Spett.le ASL_____

_____

**Oggetto: Accordo per la Nomina a Responsabile del Trattamento dei Dati Personali della Asl _____.. *Data Processing Agreement* (DPA) ai sensi dell'Art. 28 del Regolamento Generale sulla Protezione dei Dati n. 679/2016 (GDPR – General Data Protection Regulation) e delle vigenti normative in materia di Protezione dei Dati Personali. In applicazione della Delibera ASL PE n. 353 del 19 aprile 2017 e della Delibera G.R.A.n. 780 del 20 dicembre 2017.**

Il presente accordo integra e specifica gli obblighi di protezione dei dati gravanti sulla ASL di Pescara (di seguito ASL PE o ASL Titolare) e la Asl _____ (di seguito anche Responsabile o ASL Responsabile) derivanti dall'esecuzione:

a) dell'Accordo Quadro recepito con Delibera G.R.A. n. 780 del 20 dicembre 2017, avente ad oggetto "Modifica e integrazione Decreto del Commissario ad Acta n. 114 del 28.09.2016 recante "Distribuzione di farmaci del PHT tramite le farmacie convenzionate con la modalità in nome e per conto (DPC) del SSR e attivazione del servizio Farmacup – Approvazione dell'Accordo Quadro Regionale con le associazioni delle farmacie pubbliche e private"- Provvedimenti" (di seguito "Accordo Quadro");

b) della Delibera ASL PE n. 353 del 19 aprile 2017 avente ad oggetto "Approvazione degli esiti della procedura negoziata volta alla aggiudicazione della fornitura – in licenza d'uso – del software per la gestione di una piattaforma web per la realizzazione della distribuzione per conto di farmaci PHT"- o, in ogni caso, derivanti dall'esecuzione, a qualunque titolo, da parte del Responsabile a favore della ASL PE di fornitura di un applicativo Web-DPC per garantire gli ordini dei farmaci oggetto dell'Accordo Quadro, e relativa installazione, manutenzione e/o l'assistenza tecnica, con particolare riferimento ai dati del Titolare e dei Terzi Interessati, ai sensi del Regolamento europeo n. 679 del 27 aprile 2016 **("GDPR")** e delle vigenti norme in materia di protezione dei dati personali;

Il Responsabile e la ASL Titolare di seguito congiuntamente le **"Parti"** e ciascuna singolarmente la **"Parte".**

## Articolo 1 – Oggetto, natura, finalità e durata del trattamento

Il presente DPA si applica al trattamento dei dati personali svolto dal Responsabile ("Responsabile del Trattamento") per conto della ASL Titolare del trattamento ("Titolare del Trattamento"), ai sensi dell'Accordo Quadro e definisce gli obblighi delle Parti in materia di tutela dei dati personali.

Natura e finalità del trattamento: il Responsabile tratta i dati personali nella misura necessaria a fornire i servizi di cui all'Accordo Quadro. I servizi che possono essere svolti dal Responsabile sono indicati nell'Accordo Quadro e nella Delibera ASL PE n. 353/ 2017. I trattamenti autorizzati, ai sensi del presente DPA, sono indicati nell'Allegato 2.

Ciascuna Parte è esclusivamente responsabile per il proprio rispetto delle disposizioni di legge applicabili in materia di protezione dei dati personali.

La durata del trattamento dei dati personali dei Terzi Interessati da parte del Responsabile corrisponde alla durata dell'Accordo Quadro.

## Articolo 2 – Tipologie di dati personali e categorie di interessati

I soggetti i cui dati personali sono oggetto del trattamento da parte del Responsabile ai sensi del presente DPA possono essere, a titolo esemplificativo e non esaustivo, dipendenti e collaboratori della ASL Titolare, terzi incaricati, a qualunque titolo, dalla ASL Titolare, pazienti, controparti contrattuali della ASL Titolare e, in generale, terze parti rispetto alle quali la ASL Titolare agisce come titolare del trattamento dei dati personali ai sensi del GDPR (congiuntamente i "Terzi Interessati"). I dati personali trattati possono consistere, a titolo esemplificativo, in recapiti, dati identificativi, informazioni relative allo stato di salute, prescrizioni mediche, piani terapeutici.

## Articolo 3 – Istruzioni

Il Responsabile effettua il trattamento dei dati personali esclusivamente sulla base delle istruzioni ricevute dalla ASL Titolare in forma scritta: il dettaglio delle operazioni consentite è indicato nell'Allegato 3 al presente DPA. Il presente DPA e l'Accordo Quadro costituiscono parte delle istruzioni della ASL Titolare per il trattamento dei dati personali da parte del Responsabile e potranno essere integrate, in qualunque momento, da eventuali specifiche disposizioni, conformi alla legge applicabile in materia di Protezione dei Dati, ove ritenuto necessario da parte del Titolare.

Qualsiasi istruzione aggiuntiva o diversa rispetto a quanto previsto nell'Accordo Quadro e nel presente DPA dovrà essere trasmessa dalla ASL Titolare al Responsabile per iscritto e comunicata via PEC e/o raccomandata a/r. Tale istruzione aggiuntiva diverrà efficace entro 30 giorni dalla data di comunicazione.

## Articolo 4 – Riservatezza

Il Responsabile garantisce che i soggetti autorizzati al trattamento dei dati personali per proprio conto si siano impegnati contrattualmente a mantenere la riservatezza dei dati e siano soggetti a tale obbligo.

## Articolo 5 – Sicurezza del trattamento

Il Responsabile si impegna ad adottare le misure richieste dall'Art. 32 del GDPR.

In particolare - in considerazione dello stato dell'arte, dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché dei rischi derivanti, in particolare, dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trattati, il Responsabile si impegna a mettere in atto le misure tecniche e organizzative indicate nell'Allegato 1 al presente DPA di cui si richiede la compilazione per la descrizione delle modalità di implementazione.

Qualora il Responsabile intendesse apportare modifiche alle misure tecniche e organizzative descritte nell'Allegato 1, in considerazione del progresso e sviluppo tecnologico, effettuerà una preventiva comunicazione alla ASL Titolare, fermo restando che tali modifiche non potranno comportare l'approntamento di un livello di protezione inferiore rispetto a quanto previsto nell'Allegato 1.

## Articolo 6 – Assistenza

Tenendo conto della natura del trattamento dei dati personali svolto dal Responsabile, come descritto nell'Accordo Quadro, il Responsabile si impegna ad assistere il Titolare, approntando le adeguate misure tecniche e organizzative, nella misura in cui ciò sia possibile, per consentire al Titolare di permettere ai Terzi Interessati l'esercizio dei diritti di cui agli Artt. da 12 a 23 del GDPR.

Il Responsabile dovrà informare il Titolare, senza ingiustificato ritardo, qualora un Terzo Interessato eserciti nei suoi confronti uno dei diritti di cui agli Artt. da 12 a 23 del GDPR.

Tenendo conto della natura del trattamento, come descritto nell'Accordo Quadro e nel presente DPA, e delle informazioni di volta in volta messe a disposizione, il Responsabile si impegna ad assistere il Titolare a garantire il rispetto degli obblighi di cui agli Artt. da 32 a 36 del GDPR

## Articolo 7 – Cancellazione

I dati personali di proprietà del Titolare che siano oggetto di trattamento da parte del Responsabile, nell'ambito dell'esecuzione delle attività previste dall'Accordo Quadro, in base ai termini di conservazione di tali trattamenti, opportunamente previsti nei registri di trattamento, devono essere periodicamente cancellati ove ne ricorra il termine. Alla cessazione dell'Accordo Quadro, ove applicabile, i dati oggetto di Trattamento da parte del Responsabile devono essere restituiti al Titolare, entro un termine di 30 giorni dalla cessazione da parte del Responsabile dei servizi in relazione ai quali viene eseguito il trattamento dei dati personali.

In mancanza di diverse istruzioni successive, il Titolare chiede sin d'ora al Responsabile, (e questi agli eventuali sub-responsabili) di procedere con la cancellazione di tutte le copie di dati personali in proprio possesso a seguito della cessazione, da parte del Responsabile, dei servizi in relazione ai quali esegue il trattamento dei dati personali, salvo che la legge applicabile obblighi il Responsabile alla conservazione dei dati personali trattati.

## Articolo 8 – Violazioni di Dati Personali (cd. "Data Breach")

Il Responsabile si impegna ad informare il Titolare, senza ingiustificato ritardo e comunque entro 12 ore dal momento in cui ne sia venuto a conoscenza, di ogni violazione della sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati Personali trasmessi, conservati o comunque trattati.

Il Responsabile si impegna inoltre, ai sensi dell'art. 28.3, lett. f), tenuto conto della natura del trattamento e delle informazioni a sua disposizione, a prestare ogni necessaria collaborazione al Titolare in relazione all'adempimento degli obblighi sullo stesso gravanti di notifica delle suddette violazioni all'Autorità ai sensi dell'art. 33 del GDPR o di comunicazione della stessa agli interessati ai sensi dell'art. 34 del GDPR.
La comunicazione dovrà avvenire a mezzo PEC/mail rispettivamente agli indirizzi protocollo.aslpe@pec.it e info.urp@ausl.pe.it

## Articolo 9 – Valutazione D'impatto (CD. "DATA PROTECTION IMPACT ASSESSMENT")

Il Responsabile, ai sensi dell'art. 28.3, lett. f), s'impegna fin da ora, tenuto conto della natura del trattamento e delle informazioni a sua disposizione, a fornire al Titolare ogni elemento utile all'effettuazione, da parte di quest'ultimo, della valutazione di impatto sulla protezione dei dati, qualora il Titolare sia tenuto ad effettuarla ai sensi dell'art. 35 del Regolamento, nonché ogni collaborazione nell'effettuazione della eventuale consultazione preventiva al Garante da parte di quest'ultimo ai sensi dell'art. 36 del Regolamento stesso.

## Articolo 10 – Soggetti Autorizzati al Trattamento

Fatto salvo quanto previsto all'articolo 11, il Responsabile, garantisce che l'accesso ai Dati Personali sarà limitato esclusivamente ai propri dipendenti e collaboratori, previamente identificati per iscritto, il cui accesso ai Dati Personali sia necessario per l'esecuzione dei Servizi.

Il Responsabile si impegna a fornire ai propri dipendenti e collaboratori, deputati a trattare i Dati Personali del Titolare, le istruzioni necessarie per garantire un corretto, lecito e sicuro trattamento, curarne la formazione, vigilare sul loro operato, vincolarli alla riservatezza su tutte le informazioni acquisite nello svolgimento della loro attività, anche per il periodo successivo alla cessazione del rapporto di lavoro, e a comunicare al Titolare, su specifica richiesta, l'elenco aggiornato degli stessi.

## Articolo 11 – Sub-responsabili del Trattamento

Per l'esecuzione di specifiche attività per conto della ASL Titolare, il Responsabile, potrà avvalersi di sub-responsabili del trattamento (ciascuno un "Sub-responsabile del Trattamento") ai sensi del GDPR. I Sub-responsabili del Trattamento sono autorizzati a trattare dati personali dei Terzi Interessati esclusivamente allo scopo di eseguire le attività per le quali tali dati personali siano stati forniti al Responsabile ed è fatto loro divieto di trattare tali dati personali per altre finalità. Se il Responsabile, ricorrerà a Sub-responsabili del Trattamento, essi saranno vincolati, per iscritto, mediante un Accordo Quadro o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, agli stessi obblighi in materia di protezione dei dati contenuti nel presente DPA tra il Titolare del trattamento e il Responsabile,, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del regolamento. Qualora il sub-responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile, conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi del Sub-responsabile.

L'elenco completo dei Sub-responsabili del Trattamento che verranno eventualmente incaricati dal Responsabile, per l'esecuzione di attività di trattamento dei dati di cui all'Accordo Quadro dovrà essere previamente fornito alla ASL Titolare per la necessaria autorizzazione; tale autorizzazione dovrà essere richiesta dal Responsabile anche in caso di eventuali aggiornamenti a tale elenco.

Il Responsabile si impegna a informare anticipatamente il Titolare, anche con mezzi elettronici (indirizzi e-mail e/o PEC indicati all'art. 8 del presente DPA), laddove intenda includere un nuovo Sub-responsabile del Trattamento nell'elenco, intenda sostituire o cessare il rapporto con un Sub-responsabile del Trattamento esistente. La modifica si intenderà accettata dal Titolare laddove quest'ultimo non sollevi obiezioni per iscritto entro 3 (tre) mesi dalla ricezione della comunicazione da parte del Responsabile.

Qualora la ASL Titolare sollevi obiezioni su uno o più sub-responsabili del Trattamento, il Titolare darà indicazioni al Responsabile sulle relative motivazioni. In tal caso, il Responsabile potrà:

1. proporre altro Sub-responsabile del Trattamento in sostituzione del Sub-responsabile del Trattamento per il quale la ASL Titolare abbia sollevato obiezioni; o
2. adottare misure tese a superare le obiezioni della ASL Titolare (qualora le obiezioni fossero superabili).

Il Responsabile risponde nei confronti della ASL Titolare per l'adempimento del Sub-responsabile del Trattamento ai propri obblighi.

Nel caso in cui il Responsabile abbia necessità di ricorrere a un Sub-responsabile del Trattamento situato in un Paese terzo (extra UE), il Responsabile dovrà darne preventiva comunicazione al Titolare per l'approvazione e, eventualmente, per definire e concordare le modalità di trasferimento dei dati personali conformi a quanto previsto dagli Artt. 44 e seguenti del GDPR. Il Responsabile dovrà garantire inoltre che siano adottate adeguate misure tecniche e organizzative affinché il trattamento soddisfi i requisiti del GDPR, sia assicurata la protezione dei diritti dei Terzi Interessati e le opportune misure di sicurezza siano documentate.

## Articolo 12 – Amministratori di Sistema

Se applicabile, il Responsabile si impegna a conformarsi al Provvedimento generale del Garante per la protezione dei dati personali del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", così come modificato dal Provvedimento del Garante del 25 giugno 2009, e ad ogni altro pertinente provvedimento dell'Autorità.

In riferimento ai sistemi informatici di trattamento dei dati del Titolare per i quali il Responsabile eserciti attività di Amministrazione di Sistema, egli si impegna a:

1. designare quali amministratori di sistema le figure professionali dedicate alla gestione e alla manutenzione di impianti di elaborazione o di loro componenti con cui vengono effettuati trattamenti di Dati personali, fornendo al Titolare, su richiesta, informazioni sulle valutazioni effettuate per le designazioni;
2. effettuare un'elencazione analitica degli ambiti di operatività consentiti a ciascuno in base al relativo profilo di autorizzazione assegnato e fornendo, su richiesta, informazioni relative alle valutazioni alla base delle designazioni;
3. predisporre e conservare l'elenco contenente gli estremi identificativi delle persone fisiche qualificate quali amministratori di sistema e le funzioni ad essi attribuite;
4. comunicare periodicamente al Titolare l'elenco aggiornato degli amministratori di sistema, specificandone l'ambito di responsabilità (sistemi, database, reti, applicativi, etc.);
5. verificare annualmente l'operato degli amministratori di sistema, informando il Titolare circa le risultanze di tale verifica;
6. mantenere i file di log in conformità a quanto previsto nel suddetto provvedimento (qualora i sistemi siano installati presso le strutture del Responsabile o di suoi sub-Responsabili);
7. garantire una rigida separazione tra chi autorizza e/o assegna i privilegi di accesso e chi effettua le attività tecnico-sistemistiche.

## Articolo 13 – Rapporti con le Autorità

Il Responsabile, su richiesta del Titolare, si impegna a coadiuvare quest'ultimo nella difesa in caso di procedimenti dinanzi all'autorità di controllo o all'autorità giudiziaria che riguardino il trattamento dei Dati Personali di propria competenza.

## Articolo 14 – Ulteriori Obblighi e Responsabilità

Il Responsabile mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui alla normativa in materia di protezione dei dati personali e/o delle istruzioni del Titolare di cui al presente atto di designazione e consente al Titolare del trattamento l'esercizio del potere di controllo e ispezione, prestando ogni ragionevole collaborazione alle attività di audit effettuate dal Titolare stesso o da un altro soggetto da questi incaricato o autorizzato, con lo scopo di controllare l'adempimento degli obblighi e delle istruzioni di cui al presente atto.

Il Titolare darà comunicazione al Responsabile della propria intenzione di svolgere un Audit comunicandone l'oggetto, la tempistica, la data, e la durata dell'Audit.

Il Titolare fornirà al Responsabile una relazione scritta di natura confidenziale contenente il riepilogo dell'oggetto e dei risultati dell'Audit.

Il Responsabile si impegna altresì a:

1. effettuare almeno annualmente un rendiconto in ordine all'esecuzione delle istruzioni ricevute dal Titolare (e agli adempimenti eseguiti) ed alle conseguenti risultanze;
2. collaborare, se richiesto dalla ASL Titolare, con gli altri Responsabili del trattamento, al fine di armonizzare e coordinare l'intero processo di trattamento dei Dati Personali;

3. realizzare quant'altro sia ragionevolmente utile e/o necessario al fine di garantire l'adempimento degli obblighi previsti dalla normativa applicabile in materia di protezione dei dati, nei limiti dei compiti affidati con il presente atto di designazione;
4. informare prontamente il Titolare di ogni questione rilevante ai fini di legge, in particolar modo, a titolo esemplificativo e non esaustivo, nei casi in cui abbia notizia, in qualsiasi modo, che il trattamento dei Dati Personali violi la normativa in materia di protezione dei dati personali o presenti comunque rischi specifici per i diritti, le libertà fondamentali e/o la dignità dell'interessato o qualora, a suo parere, un'istruzione violi la normativa, nazionale o comunitaria, relativa alla protezione dei dati oppure qualora il Responsabile sia soggetto ad obblighi di legge che gli rendono illecito o impossibile agire secondo le istruzioni ricevute dalla ASL Titolare e/o conformarsi alla normativa o a provvedimenti dell'Autorità di Controllo.

Resta inteso che qualora il Responsabile (o eventuali suoi Sub-responsabili) determini autonomamente le finalità e i mezzi di trattamento in violazione delle istruzioni impartite dal Titolare, sarà considerato, a sua volta, Titolare del trattamento, assumendo i conseguenti oneri, rischi e responsabilità.

## Articolo 15 – Disposizioni Finali

Resta inteso che la presente designazione non comporta alcun diritto per il Responsabile ad uno specifico compenso o indennità o rimborso per l'attività svolta, né ad un incremento del compenso spettante allo stesso in virtù del Accordo Quadro con la ASL Titolare.

Gli allegati alla presente designazione fanno parte integrante della stessa.

Per tutto quanto non previsto dal presente atto di designazione si rinvia alle disposizioni generali vigenti ed applicabili in materia di protezione dei dati personali.

Il mancato riscontro alle presenti istruzioni non consentirà di dare attuazione di quanto previsto nell'Accordo Quadro.

Una volta dato riscontro positivo alla presente nomina, resta inteso che la mancata esecuzione delle istruzioni ivi contenute, costituisce una violazione del Regolamento UE 2016/679.

IL DIRETTORE GENERALE

Dr. Armando Mancini

Per ricezione ed integrale accettazione del Responsabile

LA ASL

# ALLEGATO 1 – Principi, Diritti e Misure Tecniche e Organizzative

Si chiede di descrivere le modalità per garantire, per quanto di competenza, il rispetto dei seguenti principi di trattamento e diritti degli interessati, secondo le indicazioni del Regolamento UE 679/2016, nell'ambito delle attività svolte per conto del Titolare; in alternativa indicare se siano ritenute non applicabili e darne motivazione o siano state programmate azioni ed eventuali scadenze.

| Req. | Principi e Diritti (riferimenti agli articoli del Reg. UE 679/2016) | Adottata (SI/NO) | Descrizione |
|---|---|---|---|
| A.1 | Art. 5.1.a e Art. 7 – Liceità e Gestione Consenso al Trattamento | | |
| A.2 | Art. 5.1.c minimizzazione dei dati | | |
| A.3 | Art. 5.1.e Limitazione della conservazione (art. 13 del Regolamento) | | |
| A.4 | Art. 15 Diritto di Accesso | | |
| A.5 | Art. 16 – Diritto di Rettifica | | |
| A.6 | Art. 17 – Diritto alla Cancellazione | | |
| A.7 | Art. 18 – Diritto alla Limitazione del Trattamento | | |
| A.8 | Art. 20 – Diritto alla portabilità dei dati | | |

Si chiede di descrivere quali delle seguenti misure tecniche e organizzative siano state adottate nell'ambito dei prodotti e/o servizi forniti alla ASL Titolare o se siano state programmate azioni di implementazione ed eventuali scadenze; in alternativa indicare se siano ritenute non applicabili e darne motivazione.

| Req. | Misura | Dettaglio | Adottata (SI/NO) | Descrizione/Motivazione |
|---|---|---|---|---|
| B.1 | **Politiche per la protezione dei dati** | Politiche per la protezione dei dati personali, sicurezza delle informazioni e conservazione | | |
| B.2 | **Organizzazione per la protezione dei dati** | Articolazione dell'organizzazione per la Protezione dei Dati Personali (DPO, Responsabili, ecc...) | | |
| B.3 | **Gestione della Sicurezza dei Dati da parte delle risorse umane (dipendenti/collaboratori)** | Procedure di ingresso di nuovi dipendenti/collaboratori, cambiamento di mansioni e/o cessazione del rapporto di lavoro.<br>Piano di Formazione periodica sulla Protezione dei Dati Personali | | |
| B.4 | **Gestione degli asset (dati personali e strumenti di supporto)** | Classificazione, Censimento e Definizione delle Responsabilità dei dati personali e dei relativi supporti/strumenti di trattamento utilizzati | | |
| B.5 | **Controllo degli accessi logici e partizionamento dei dati** | Procedure di gestione degli accessi logici degli utenti a sistemi e applicazioni che trattano dati personali | | |
| B.6 | **Pseudonimizzazione** | Misure per garantire la pseudonimizzazione dei dati personali utilizzati nel servizio erogato | | |
| B.7 | **Cifratura** | Procedure e Criteri di utilizzo della cifratura | | |
| B.8 | **Controllo degli accessi fisici** | Procedura di definizione della sicurezza dei locali, delle aree di trattamento di dati personali e di gestione della sicurezza fisica delle apparecchiature (strumenti di supporto) | | |

| Req. | Misura | Dettaglio | Adottata (SI/NO) | Descrizione/Motivazione |
|---|---|---|---|---|
| B.9 | **Sicurezza delle attività operative e manutenzione** | Policies tecnico-organizzative (es.: Utilizzo dei dispositivi portatili, VPN, dispositivi personali, posta elettronica, ecc.)<br>Misure di sicurezza antivirus-antimalware<br>Procedure di Gestione dei Backup<br>Criteri e procedure per la raccolta di Log e Monitoraggio dei sistemi<br>Procedure di controllo dell'integrità degli strumenti di erogazione del servizio<br>Procedure di controllo delle vulnerabilità tecniche<br>Procedure di gestione delle Manutenzioni | | |
| B.10 | **Sicurezza della rete e delle comunicazioni** | Procedure di gestione della sicurezza della rete<br>Procedure per la gestione del trasferimento di informazioni | | |
| B.11 | **Gestione dei sistemi applicativi** | Criteri per la definizione dei Requisiti di sicurezza dei sistemi utilizzati/da acquisire<br>Procedure operative per le operazioni di acquisizione, sviluppo e di manutenzione dei sistemi | | |
| B.12 | **Relazioni con i sub-fornitori** | Procedure e nomine per garantire la protezione dei dati personali trattati dai sub-fornitori | | |
| B.13 | **Gestione degli incidenti e delle Violazioni di dati personali** | Procedure di gestione degli incidenti sulla Sicurezza delle Informazioni e delle Violazioni di Dati Personali | | |
| B.14 | **Continuità Operativa** | Procedure di Gestione della Continuità Operativa del servizio<br>Misure per garantire la Sicurezza in condizioni di emergenza e degli strumenti atti a garantire la Continuità Operativa. | | |

| Req. | Misura | Dettaglio | Adottata (SI/NO) | Descrizione/Motivazione |
|---|---|---|---|---|
| **B.15** | **Conformità e Audit** | Procedure per garantire il tempestivo aggiornamento normativo e l'adeguamento del servizio alle nuove indicazioni<br>Procedure di Audit interne per assicurare la sicurezza dei trattamenti sui sistemi in uso per la ASL Titolare (test, verifica e valutazione dell'efficacia delle misure tecniche e organizzative) | | |
| **B.16** | **Misure per il rispetto della Privacy by Design** | Ved. Reg. UE 679/2016 art. 25 | | |
| **B.17** | **Misure per il rispetto della Privacy by Default** | Ved. Reg. UE 679/2016 art. 25 | | |
| **B.18** | **DPO – Data Protection Officer (Responsabile della Protezione dei Dati)** | Si richiede di dare comunicazione, se nominato, degli estremi e dei riferimenti di contatto del Responsabile della Protezione Dati dell'organizzazione (RPD – DPO/Data Protection Officer) | | |
| **B.19** | **Presenza di Polizza Cyber Risk** | Si richiede se la Vostra azienda sia dotata di **polizza cyber-risk e l'eventuale dettaglio della stessa** | | |
| **B.20** | **Gestione del Cambiamento** | Si richiede se esista una **procedura di gestione dei cambiamenti (Change Management)** nelle modalità di erogazione del servizio (es.: cambiamenti infrastrutturali, cambiamenti organizzativi, ecc...). Si richiede di fornirne copia. | | |

# ALLEGATO 2 – Ambito del Trattamento

Sulla scorta degli atti d'ufficio risulta che le categorie di attività (art. 30.2 del Regolamento) svolte dal Responsabile, nell'ambito dei servizi erogati per conto della ASL Titolare, siano di supporto ai seguenti trattamenti censiti:

| Cod. | Sub. | Requisito | Descrizione |
|---|---|---|---|
| 1 | | **Trattamento 1** | Distribuzione di Farmaci del PHT tramite le Farmacie convenzionate con la modalità in nome e per conto (DPC) del SSR. |
| | 1.1 | Categorie di interessati | Pazienti |
| | 1.2 | Tipi di Dati Personali oggetto di trattamento (indicare se dati comuni, categorie particolari, dati relativi a condanne penali e reati | - Dati comuni<br>- Categorie particolari di dati personali (dati relativi alla salute) |
| | 1.3 | Finalità del trattamento | - Attività amministrative correlate a quelle di prevenzione, diagnosi, cura e riabilitazione<br>- Programmazione, gestione, controllo e valutazione dell'assistenza sanitaria |
| | 1.4 | Durata del trattamento | Fino alla cessazione per qualunque motivo del Accordo Quadro e/o, comunque, dei Servizi ovvero fino alla revoca anticipata per qualsiasi motivo da parte del Titolare |
| | 1.5 | Tempo di Conservazione | 5 anni salvo diverse istruzioni comunicate successivamente |

# ALLEGATO 3 – Categorie di attività di trattamento (30.2) e relativi impatti

In linea con l'approccio basato sul rischio previsto dal GDPR, il Titolare ha individuato per le seguenti categorie di attività relative al trattamento (operazioni di trattamento), secondo quanto previsto dall'Art. 30.2 del GDPR, il livello d'impatto potenziale (quindi considerato **prima dell'applicazione delle misure di sicurezza** adottate dal Titolare che del Responsabile) sui diritti e le libertà degli interessati ed il livello di impatto reale **dopo l'adozione delle misure di sicurezza** come di seguito indicato:

| ID | Trattamento (rif. Trattamenti Allegato 2) | Categorie di attività relative al trattamento (Operazioni di trattamento) | Appl. | Livello di Impatto Potenziale del Trattamento | Livello di Impatto Residuo del Trattamento (calcolato tenendo conto delle misure – All. 1) |
|---|---|---|---|---|---|
| 1 | Distribuzione di Farmaci del PHT tramite le Farmacie convenzionate con la modalità in nome e per conto (DPC) del SSR. | Raccolta | X | **Impatto Massimo** | **Impatto Trascurabile** |
| | | Registrazione | X | | |
| | | Organizzazione | X | | |
| | | Strutturazione | X | | |
| | | Conservazione | | | |
| | | Adattamento o Modifica | X | | |
| | | Estrazione | X | | |
| | | Consultazione | X | | |
| | | Uso | X | | |
| | | Comunicazione mediante trasmissione o qualsiasi altra forma di messa a disposizione | X | | |
| | | Raffronto o Interconnessione | | | |
| | | Limitazione | X | | |
| | | Cancellazione o Distruzione | | | |

Il livello di impatto indicato nella precedente tabella è relativo al valore valutato sia prima dell'adozione delle misure di sicurezza (colonna *"Livello di Impatto Potenziale"*), previste dall'Allegato 1, che successivamente all'implementazione delle stesse (colonna *"Livello di Impatto residuo"*).

I criteri di classificazione dei livelli di impatto adottati dal Titolare sono i seguenti:

- **Impatto trascurabile**: gli interessati coinvolti dal trattamento non saranno affetti da inconvenienti oppure possono incontrare alcuni inconvenienti che possono superare senza alcun problema (es. perdita di tempo per ripetere formalità, etc.);
- **Impatto limitato**: gli interessati coinvolti dal trattamento possono incontrare disagi significativi che però possono superare nonostante alcune difficoltà (es. interruzione temporanea del servizio fino a 8 ore);
- **Impatto significativo**: gli interessati coinvolti dal trattamento possono avere conseguenze significative che dovrebbero essere in grado di superare seppure con gravi difficoltà (es. interruzione temporanea del servizio oltre le 8 ore e fino e non oltre le 24 ore);
- **Impatto massimo**: gli interessati coinvolti dal trattamento possono incontrare conseguenze significative, o addirittura irreversibili, che non possono superare (es.: Interruzione del servizio oltre le 24 ore, impossibilità o perdita della possibilità di accesso ai servizi, mancato rispetto dei diritti dell'interessato – es.: diritto alla salute)

REGIONE
ABRUZZO

GIUNTA REGIONALE

Allegato 5

*Dipartimento per la Salute e il Welfare*
*Servizio Assistenza farmaceutica e trasfusionale - Innovazione ed Appropriatezza - DPF003*
*Ufficio HTA, appropriatezza, monitoraggio spesa e prescrizioni farmaceutiche*
*Via Conte di Ruvo, 74 - 65127 PESCARA*

Prot. n. 0195580/18

Pescara 10 LUG. 2018

Ai Responsabili dei Servizi Farmaceutici
AA.SS.LL. della Regione Abruzzo

A Federfarma Abruzzo
ffabruzz@tin.it; ur.abruzzo@pec.federfarma.it

Ad A.S.SO.FARM. (sede nazionale)
assofarm@assofarm.it
assofarmsegreteria@assofarm.postecert.it

e p. c.

Ai Direttori Generali
Ai Direttori Amministrativi
AA.SS.LL. della Regione Abruzzo

Al Dirigente del Servizio DPF012 - Servizio Programmazione economico-finanziaria e Finanziamento dei SSR

A Record Data S.r.l.
mail@recorddata.it

*Oggetto: Fatturato farmacie convenzionate SSN.*

Con la presente si forniscono le seguenti indicazioni inerenti alla composizione del Fatturato delle farmacie convenzionate del Servizio Sanitario Nazionale.

Il fatturato SSN risulta composto dai seguenti elementi:
- farmaci ceduti in regime convenzionale al netto dell'IVA e degli sconti di legge;
- prestazioni di assistenza integrativa e protesica.

Sono invece escluse le seguenti voci:
- quota compartecipazione (ticket);
- quota pagata dall'assistito quale differenza di prezzo tra farmaci equivalenti e branded;
- remunerazione della DPC.

Si resta a disposizione per qualsiasi chiarimento.
Cordiali saluti.

Il Responsabile dell'Ufficio
Dott. Ulisse Martegiani
Ulisse Martegiani

Il Dirigente del Servizio
Dott.ssa Emanuela Grimaldi