

*"INFORMATICA APPLICATA ALL'ODONTOIATRIA:
Applicativi informatici e devices nello studio odontoiatrico*

**FABIO SCAFFIDI
MATTEO TAINO**

MATTEO TAINO

CORSO ANNUALE PER ASSISTENTI DI STUDIO ODONTOIATRICO



ASSOCIAZIONE NAZIONALE DENTISTI ITALIANI
SEZIONE PROVINCIALE DI MILANO LODI MONZA E BRIANZA

- SISTEMA OPERATIVO

Abbreviazione SO o, in inglese, OS (Operating System).

E' l'insieme di programmi di base di un elaboratore che controlla le risorse fisiche hardware e software regolando lo svolgimento delle operazioni elementari del computer (caricamento dei programmi, ingresso dati, emissione dei risultati, gestione dell'hardware, ecc.)

• SISTEMA OPERATIVO

- Senza SO un computer è solo un “macchinario inutile”.
- Il SO rende possibile la gestione, l'elaborazione l'archiviazione dell'INFORMAZIONE
- L'hardware fornisce potenza di calcolo, il SO la rende disponibile agli utenti
- Il SO è alla base dell'esecuzione di tutti gli altri programmi
- Il SO è l'intermediario tra l'utente e la macchina

SISTEMA OPERATIVO

Microsoft	Apple
	OSX Big Sur 11.1
Windows 10	OSX Catalina 10.15
Windows 8.1	OSX Mojave 10.14
	OSX High Sierra 10.13



Per navigare in sicurezza nel web è buona norma ricordare di:

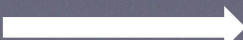
- installare e tenere aggiornato un antivirus
- installare gli aggiornamenti del sistema operativo
- scaricare i programmi necessari solo dai siti ufficiali

SISTEMA OPERATIVO

Sistemi operativi client attualmente utilizzabili:

- Windows 8.1  Fine aggiornamenti: 10 gennaio 2023
- Windows 10  Fine aggiornamenti: 13 ottobre 2026

Sistemi operativi server attualmente utilizzabili:

- Windows Server 2012  Fine aggiornamenti: 10 ottobre 2023
- Windows Server 2016  Fine aggiornamenti: 11 gennaio 2027
- Windows Server 2019  Fine aggiornamenti: 9 gennaio 2029

SISTEMA OPERATIVO

Sistemi operativi client da NON UTILIZZARE in ambito medico:

- Windows XP  Fine aggiornamenti: 8 aprile 2014
- Windows Vista  Fine aggiornamenti: 11 aprile 2017
- Windows 7  Fine aggiornamenti: 14 gennaio 2020

Sistemi operativi server da NON UTILIZZARE in ambito medico:

- Windows Server 2003  Fine aggiornamenti: 14 luglio 2015
- Windows Server 2008  Fine aggiornamenti: 14 gennaio 2020

SICUREZZA DEI DATI

VIRUS: come regola generale si assume che un virus possa danneggiare direttamente solo il software della macchina che lo ospita, anche se esso può indirettamente provocare danni anche all'hardware, ad esempio causando il surriscaldamento della CPU mediante overclocking, oppure fermando la ventola di raffreddamento

SICUREZZA DEI DATI

MALWARE: abbreviazione per **malicious software** (software dannoso), indica un qualsiasi software usato per disturbare le operazioni svolte da un computer, rubare informazioni sensibili, accedere a sistemi informatici privati, o mostrare pubblicità indesiderata.

Il malware non necessariamente è creato per arrecare danni tangibili ad un computer o un sistema informatico, ma va inteso anche come un programma che può rubare di nascosto informazioni di vario tipo, da commerciali a private, senza essere rilevato dall'utente anche per lunghi periodi di tempo.

SICUREZZA DEI DATI

TROJAN: un trojan o trojan horse (in italiano Cavallo di Troia), nell'ambito della sicurezza informatica, indica un tipo di malware.

Il trojan nasconde il suo funzionamento all'interno di un altro programma apparentemente utile e innocuo. L'utente eseguendo o installando quest'ultimo programma installa o esegue di conseguenza anche il codice del trojan nascosto.

I trojan non si diffondono autonomamente come i virus e non sono in grado di replicare se stessi. Quindi richiedono un intervento diretto dell'aggressore per far giungere l'eseguibile maligno alla vittima.

SICUREZZA DEI DATI

RANSOMWARE: è un tipo di malware che limita l'accesso al dispositivo che infetta, richiedendo un riscatto (ransom in inglese). Ad esempio alcune forme di ransomware bloccano il sistema e intimano all'utente di pagare per sbloccare il sistema, altri invece cifrano i file dell'utente chiedendo di pagare per riportare i file cifrati allo stato originale.

ANTIVIRUS

Come si può diffondere un virus?

- File infetto presente su chiavetta usb e trasferito su pc senza antivirus
- Programma scaricato da siti non ufficiali
- Utilizzo di link non sicuri
- Email non controllata da antivirus
- Email falsificata proveniente da mittente “attendibile” che in realtà contiene virus (persone conosciute, enti ufficiali come banche, posta, corrieri, ecc.)

SICUREZZA DEI DATI

PHISHING: tipo di truffa effettuata su Internet attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile. Si tratta di una attività illegale che sfrutta una tecnica di ingegneria sociale: il malintenzionato effettua un invio massivo di messaggi di posta elettronica che imitano, nell'aspetto e nel contenuto, messaggi legittimi di fornitori di servizi; tali messaggi fraudolenti richiedono di fornire informazioni riservate come, ad esempio, il numero della carta di credito o la password per accedere ad un determinato servizio

SICUREZZA DEI DATI

Qualche suggerimento pratico....

- Prestare attenzione al tipo di file allegato al messaggio email. Conoscere le estensioni dei file può aiutare.

.doc / .docx	File di Microsoft Word
.xls / .xlsx	File di Microsoft Excel
.ppt / .pptx	File di Microsoft Powerpoint
.ods / .odt / .odp	Suite OpenOffice
.pdf	File di Adobe Acrobat
.zip / .rar	File compressi
.exe	File eseguibili
.mp3 / .wav / .m4a / .flac / .wma	File audio
.avi / .mp4 / .mkv / .mov / .flv	File video
.jpg / .jpeg / .png / .gif / .bmp	File immagine

SICUREZZA DEI DATI

Qualche suggerimento pratico....

- Password di almeno 8 caratteri, almeno una lettera maiuscola e almeno un numero oltre a un carattere speciale come !, \$, =, @. Non utilizzare nella password termini che possano identificare facilmente l'utente come il proprio nome o cognome o la data di nascita.
- Non utilizzare parole ovvie come ad esempio: password, pippo, pluto, 12345678
- Cercare di avere più password e non usare mai la stessa per tutti i vostri accessi ai siti che richiedono un login

ANTIVIRUS

Qualche suggerimento pratico....

- Quando si crea una email evitare di mettere indirizzi di persone che non si conoscono tra loro nel campo A o CC. E' meglio usare il campo CCN

A:
Cc:
Ccn:
Oggetto:

CASELLA PEC

La Posta Elettronica Certificata (PEC) è il sistema che consente di inviare e-mail con valore legale equiparato ad una raccomandata con ricevuta di ritorno.

Le principali caratteristiche che distinguono una email PEC da una email tradizionale sono:

- medesimo valore legale della raccomandata con ricevuta di ritorno con attestazione dell'orario esatto di spedizione
- il sistema di Posta Certificata, grazie ai protocolli di sicurezza utilizzati, è in grado di garantire la certezza del contenuto non rendendo possibili modifiche al messaggio, sia per quanto riguarda i contenuti che eventuali allegati.

CASELLA PEC

- il termine "Certificata" si riferisce al fatto che il gestore del servizio rilascia al mittente una ricevuta che costituisce prova legale dell'avvenuta spedizione del messaggio ed eventuali allegati. Allo stesso modo, il gestore della casella PEC del destinatario invia al mittente la ricevuta di avvenuta consegna
- nel caso in cui il mittente dovesse smarrire le ricevute, la traccia informatica delle operazioni svolte, conservata dal gestore per 30 mesi, consentirà la riproduzione, con lo stesso valore giuridico, delle ricevute stesse.

EDITOR DI TESTO

Un editor di testo permette di scrivere, memorizzare e stampare un testo di qualsiasi tipo, recuperarlo successivamente, correggerlo o integrarlo e ristamparlo senza bisogno di riscriverlo nuovamente.

FOGLIO DI CALCOLO

È un programma che permette di effettuare calcoli, elaborare dati e tracciare efficaci rappresentazioni grafiche. Il principio su cui si basa il foglio di calcolo è semplice: fornire una tabella, detta anche foglio di lavoro, formata da celle in cui si possono inserire dati, numeri o formule.

GESTIONALE STUDIO ODONTOIATRICO

Vantaggi:

- Gestione appuntamenti e richiami
- Controllo completo situazione clinica, radiografica e amministrativa del paziente
- Eliminazione della documentazione cartacea del paziente
- Gestione del magazzino
- Monitoraggio andamento dello studio

RACCOLTA DATI DI UN NUOVO PAZIENTE

Esistono diversi approcci per effettuare questa operazione apparentemente semplice

1. chiederli a voce
2. copiarli da supporti cartacei
3. raccoglierli con un lettore tramite tessera sanitaria
4. far compilare l'anagrafica e l'anamnesi tramite tablet

VANTAGGI RACCOLTA DATI IN MODO DIGITALE

- Maggiore sicurezza della correttezza dei recapiti telefonici e indirizzo email (ricordare appuntamenti, gestire i richiami, inviare documenti contabili e clinici)
- Certezza di memorizzare negli archivi il codice fiscale corretto per evitare errori in fase di invio delle spese sanitarie al sistema TS
- Risparmio di spazio non più occupato da contenitori per archiviare pagine di anamnesi e consenso informato.

FIRMA DIGITALE

Il nuovo Codice di Amministrazione Digitale (CAD), approvato a fine 2011, disciplina l'utilizzo dei documenti digitali e della firma grafometrica.

Il 21 maggio 2013 sono state pubblicate sulla Gazzetta Ufficiale n° 117 le ultime disposizioni tecniche attuative.

La normativa sancisce l'introduzione in Italia dell'uso della "Firma Elettronica Avanzata".

FIRMA GRAFOMETRICA

La **firma grafometrica** è una definizione comunemente usata per indicare una modalità di **firma elettronica** realizzata con un gesto manuale del tutto analogo alla **firma autografa** su carta. La **firma elettronica avanzata** non consente il **libero scambio** di documenti informatici: il suo uso è limitato al contesto e ha **valore legale** nei limiti previsti dalla normativa



FIRMA DIGITALE

La Firma Digitale è l'equivalente informatico di una tradizionale firma autografa apposta su carta e ha le seguenti caratteristiche:

Autenticità

La firma digitale garantisce l'identità del sottoscrittore

Integrità

La firma digitale assicura che il documento non sia stato modificato dopo la sottoscrizione

Validità legale

La firma digitale attribuisce piena validità legale al documento firmato

La Firma Digitale è costituita da un dispositivo (smart card o chiavetta USB) che contiene un certificato digitale di sottoscrizione, tramite il quale il titolare può firmare digitalmente i propri documenti.



RILASCIO DEL CERTIFICATO E SUA AUTENTICAZIONE

Una volta acquistato il dispositivo di firma, ci sono diverse modalità di autenticazione per ottenere il rilascio del certificato digitale:

- DE VISU presso un Pubblico Ufficiale
- DE VISU tramite app certificata con operatore
 - DE VISU a domicilio

SOFTWARE DI FIRMA E VERIFICA

Una volta attivato il Kit sul computer, attraverso il Software di Firma è possibile selezionare il documento elettronico da sottoporre a Firma Digitale

Al momento della Firma del documento, il software chiederà l'inserimento del PIN e procederà con la creazione del file firmato digitalmente.

È possibile firmare digitalmente qualsiasi tipo di file elettronico, anche file in formato pdf.

In fase di verifica della Firma da parte del destinatario del documento firmato verrà accertato che:

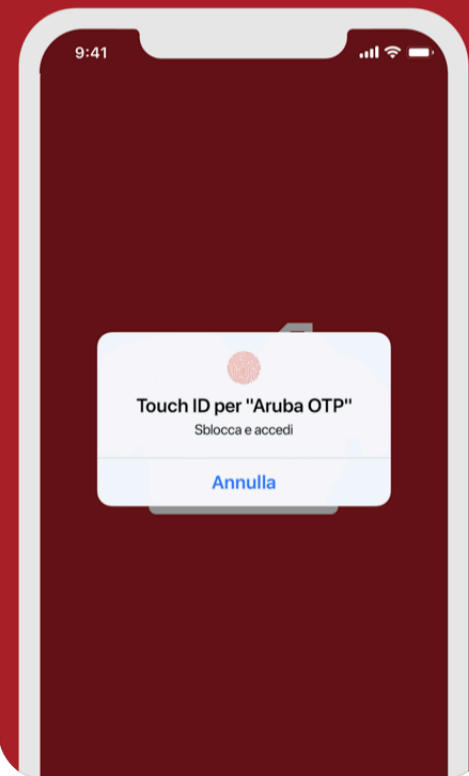
- il documento non sia stato modificato dopo la Firma;
- il Certificato del sottoscrittore sia garantito da una Autorità di Certificazione (CA) inclusa nell'Elenco Pubblico dei Certificatori;
- il Certificato del sottoscrittore non sia scaduto;
- il Certificato del sottoscrittore non sia stato sospeso o revocato.

Se tutte le verifiche daranno esito positivo, il documento sottoscritto digitalmente potrà essere considerato valido a tutti gli effetti di legge.

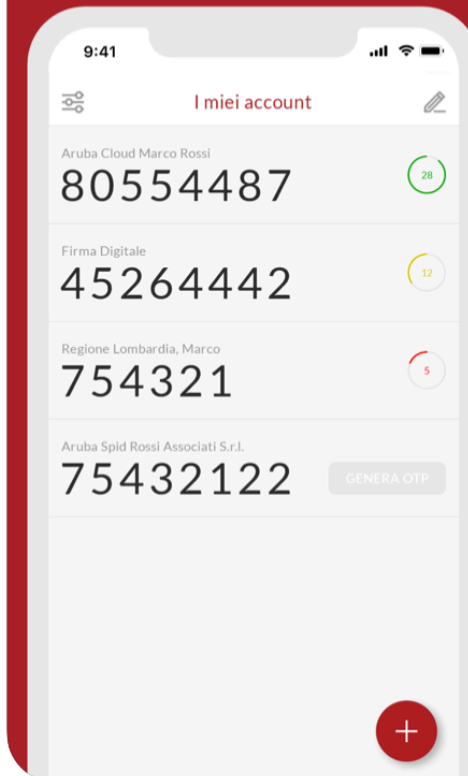
FIRMA DIGITALE REMOTA



Proteggi l'app tramite PIN,
Touch ID o Face ID



Tieni sotto controllo
la validità dell'OTP



SISTEMA TS INVIO SPESE MEDICHE

L'articolo 3, comma 3 del D. Lgs. 175/2014 prevede che il Sistema Tessera Sanitaria, metta a disposizione dell'Agenzia delle Entrate le informazioni concernenti le spese sanitarie sostenute dai cittadini, ai fini della predisposizione della dichiarazione dei redditi precompilata.

Tali informazioni devono essere inviate entro il **31 gennaio** di ogni anno

Il servizio telematico per la trasmissione dei dati è disponibile 24 ore su 24, di conseguenza, fermo restando la possibilità di optare per la frequenza temporale che si ritiene opportuno scegliere (in tempo reale, giornaliera, mensile o altro), la trasmissione dei dati di spesa sanitaria deve essere effettuata entro e non oltre il mese di gennaio dell'anno successivo a quello della spesa effettuata dal cittadino.

COME INVIARE I DATI DI SPESA SANITARIA?

I dati di spesa possono essere trasmessi attraverso 4 canali:

- Data entry di ogni singola spesa sul sito www.sistemats.it
- tramite l'applicazione web messa a disposizione dell'utente (funzionalità on line)
- Invio di ogni singola spesa con web service (SINCRONO).
- Invio di un file Xml con tutte le spese con web service (ASINCRONO)

COME VERIFICARE L'ESITO DELLA TRASMISSIONE DEI DATI DI SPESA SANITARIA?

Il sistema all'atto della ricezione dei dati rilascia un protocollo univoco che attesta esclusivamente la ricezione del file e non il corretto contenuto dei dati che devono essere trasmessi. In caso di mancata accettazione della trasmissione del file dovuta alla non adeguatezza alle regole di trasporto o ad anomalie nella nomenclatura del file o ad irregolarità nella struttura dei dati o ad incongruenze tra i dati comunicati, non si considerano acquisiti dal sistema TS i dati contenuti nei file scartati. Al fine di acquisire e verificare l'esito della corretta trasmissione dei documenti trasmessi, il sistema mette a disposizione dell'utente un'apposita ricevuta che può essere consultata sul sito del sistema ovvero acquisita per via telematica tramite gli appositi web service

PRIMA VISITA

Il paziente, dopo essere stato registrato nei sistemi informatici dello studio, viene sottoposto a prima visita.

- Quali strumenti ha a disposizione il medico per poter capire a fondo lo stato clinico?
- Quali software possono aiutarlo a pianificare il trattamento più adatto?
- Come può spiegare al paziente il piano di cura?

RADIOLOGIA DIGITALE

- E' vietata l'esposizione non giustificata
- Tutte le dosi dovute a esposizioni mediche per scopi radiologici, ad eccezione delle procedure radioterapeutiche, devono essere mantenute al livello più basso ragionevolmente ottenibile e compatibile con il raggiungimento dell'informazione diagnostica richiesta
- Le esposizioni sono vietate nei confronti delle donne con gravidanza in atto
- Le esposizioni mediche sono effettuate dallo specialista su richiesta motivata del prescrittente. La scelta delle metodologie e tecniche idonee ad ottenere il maggior beneficio clinico con il minimo danno individuale e la valutazione sulla possibilità di utilizzare tecniche sostitutive non basate su radiazioni ionizzanti compete allo specialista.

RADIOLOGIA DIGITALE

- Le attività radiodiagnostiche complementari all'esercizio clinico possono essere svolte dal medico chirurgo in possesso della specializzazione nella disciplina in cui rientra l'intervento stesso o dall'odontoiatra nell'ambito della propria attività professionale specifica
- I responsabili dei programmi di formazione assicurano che la partecipazione agli aspetti pratici di coloro che seguono tali programmi avvenga sotto la loro responsabilità, gradualmente secondo le cognizioni acquisite.
- Nelle attività di radioterapia il responsabile dell'impianto radiologico avvalendosi dell'esperto di fisica medica predispone le procedure per la valutazione delle dosi somministrate ai pazienti durante i trattamenti di radioterapia e ne verifica la corretta applicazione.

ESAMI RADIOGRAFICI

Finalità:

- Ricerca ed evidenza di carie, problemi parodontali, lesioni alla radice dei denti, danni all'osso a seguito di traumi o malattia parodontale, cisti, ascessi, terapie precedentemente effettuate, fratture radicolari, corpi estranei
- Nei bambini servono per valutare crescita e sviluppo dei denti e/o eventuale presenza di denti inclusi
- Aiutare l'odontoiatra nei trattamenti ortodontici o protesici
- Aiutare il medico chirurgo nei casi implantari, spesso si richiede una TAC

ORTOPANTOMOGRAMMA

Permette di vedere in un unico esame entrambe le arcate dentarie

Presenta un limite importante:
si rileva sempre un coefficiente di distorsione e ingrandimento rilevante (15-30%)

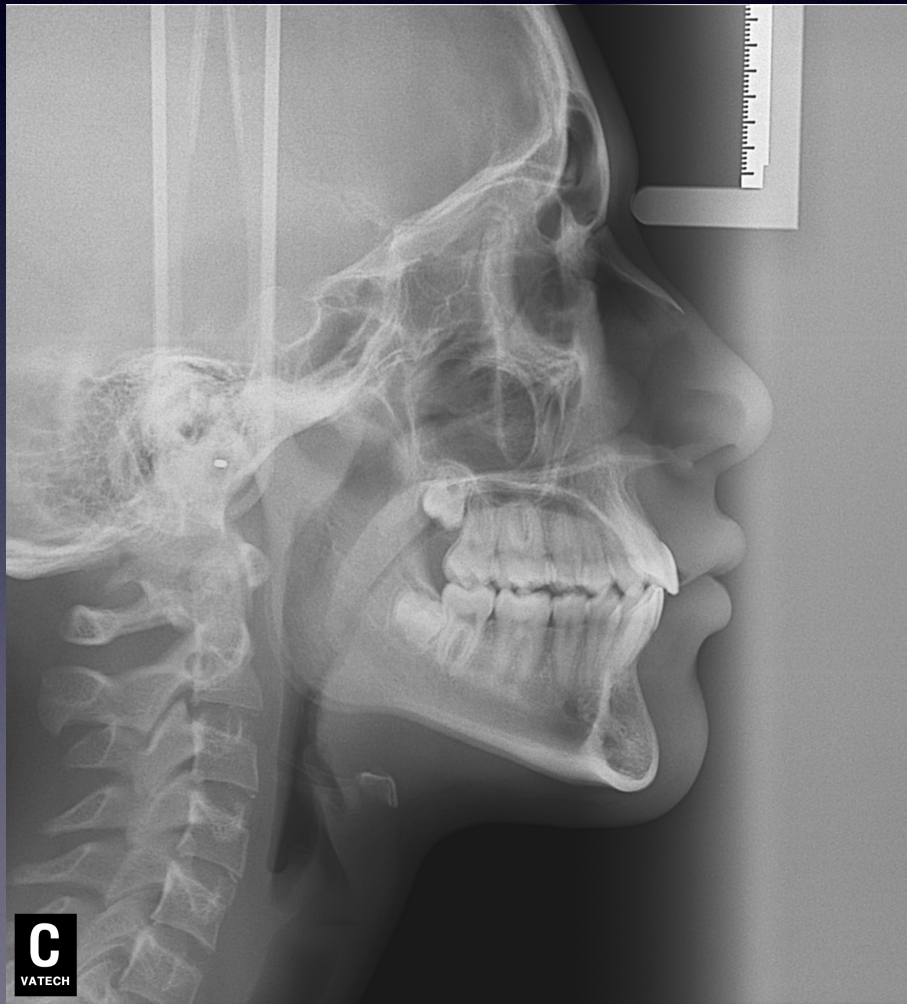


ORTOPANTOMOGRAMFIA

- Dentizione e problemi quali agenesie, denti inclusi come gli ottavi o gli elementi sovranumerari
- Nei bambini può mostrare lo stato di permuta dentaria
- Nei pazienti parodontali evidenzia il grado di progressione della malattia parodontale oltre a indicare le aree che necessitano di trattamento
- Permette di vedere fratture come ad esempio quelle mandibolari, lesioni periapicali, cisti e tumori del cavo orale
- In implantologia permette di analizzare l'area che andrà trattata consentendo di studiare lo spessore dell'osso e lo spazio tra i denti vicini

TELERADIOGRAFIA

Molto utile in ambito ortodontico o in ambito gnatologico



RX ENDORALI

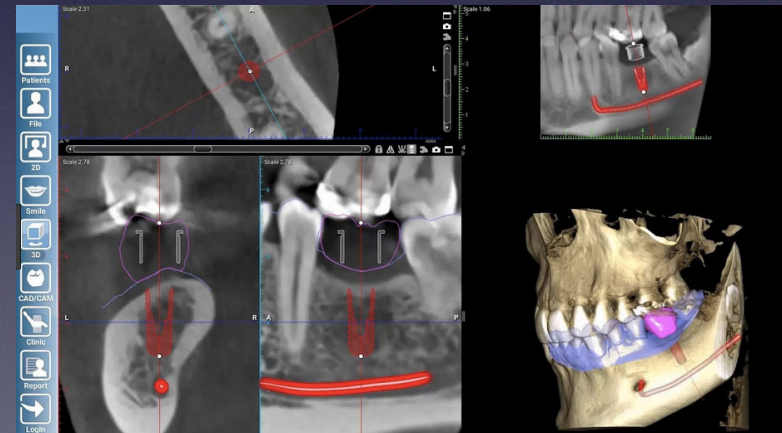
- Presenta il vantaggio di non modificare nella sostanza la metodica di lavoro adottata con le lastre a pellicola
- Esistono diversi formati di lastre adatte ad adulti e ai bambini
- Si posiziona in bocca al paziente utilizzando sempre il centratore
- Tempi di esposizione nettamente inferiori rispetto ad una rx analogica (dose radiogena più bassa fino al 60 %)
- Si continua ad utilizzare lo stesso radiografico già presente in studio
- Si elimina il problema dei liquidi di sviluppo
- Le lastre rx possono essere utilizzate migliaia di volte
- Elaborazione delle immagini attraverso software specifici

ESAME RX 2D / 3D

- Scansioni tridimensionali complete o parziali ad alta risoluzione del cranio del paziente
- I dati acquisiti vengono ricostruiti in un volume 3D da un software specifico
- Si hanno importanti vantaggi nella progettazione chirurgica implantare, nel rialzo del seno mascellare, estrazione di denti inclusi, individuazione del nervo mandibolare in rapporto agli ottavi inclusi

TAC

- Si ottiene un volume reale
- Possibilità di misurare le dimensioni reali delle aree esaminate con software dedicati



SOFTWARE GESTIONE IMMAGINI

- Programma gestione immagini del produttore del dispositivo
- Software gestione immagini integrato nel programma gestionale

PAZIENTE CHIRURGICO

Per pianificare correttamente un intervento chirurgico, attraverso l'analisi digitale di una tac, possiamo ricorrere a software che ci consentono di:

- studiare la zona in cui il medico andrà ad operare (dettagli anatomici, spessore osseo, misurazione gli spazi)
- creare mascherine per la chirurgia guidata (dima custom-made)



IMPRONTA DIGITALE

- Scanner utilizzati sia in studio che nei laboratori
- Impiegati per la scansione di elementi singoli o riabilitazioni più estese
- Tramite software è possibile progettare in forma digitale il manufatto protesico. Il software permette di gestire i margini, la forma, le cuspidi e di simularne l'occlusione
- Maggiore confort per il paziente nel rilevare l'impronta rispetto alle tecniche tradizionali
- Dematerializzazione dei modelli in gesso dei pazienti

COMUNICARE CON IL PAZIENTE

- Trasformare il tempo trascorso in sala d'attesa in un momento di approfondimento delle pratiche base di igiene orale (uso dello spazzolino o del filo interdentale)
- Utilizzare una serie di video per illustrare le specialità odontoiatriche dello studio
- Permettere al paziente di comprendere meglio il preventivo che gli è stato fatto
- La documentazione radiografica ha un'importante funzione di supporto al medico nell'illustrare lo stato clinico al paziente

DOCUMENTAZIONE PAZIENTE

- SOLO l'odontoiatra è abilitato ad eseguire attività radiodiagnostiche
- Le leggi in materia di radioprotezione impongono la conservazione e la circolazione degli esami radiologici al fine di evitare al paziente inutili esposizioni alle radiazioni.
- L'odontoiatra è tenuto all'archiviazione per dieci anni degli esami eseguiti presso il proprio studio (art. 4 comma 3, D.M.14 febbraio 1997)
- Gli esami radiografici devono essere rintracciabili e disponibili per il paziente in qualsiasi momento.
- In alternativa è possibile, per l'odontoiatra, consegnare le radiografie al paziente, documentando con ricevuta.
- Per gli esami radiologici eseguiti presso una struttura esterna e acquisiti dallo studio, subentra l'obbligo di custodia di cosa altrui e risarcimento in caso di perdita o danneggiamento del bene

DOCUMENTAZIONE PAZIENTE

Possibili modalità di consegna:

- Esportare gli esami radiografici e copiarli su chiavetta usb o masterizzarli su dvd
- Esportare gli esami radiografici e inviarli per email (dopo aver anonimizzato le immagini)

SICUREZZA DEI DATI DELLO STUDIO

Backup: processo di creazione di una copia verso un supporto esterno di dati importanti per l'utente al fine di essere in grado di ripristinarli in caso di cancellazione o impossibilità ad accedervi (ad esempio: in caso di rottura dell'hardware)

SICUREZZA DEI DATI DELLO STUDIO

E' molto importante impostare i processi di backup (manuali o automatici) seguendo un criterio:

- backup completo
- backup giornaliero
- backup incrementale

E' altamente consigliato avere backup su dispositivi collocati in luoghi differenti

SICUREZZA DEI DATI DELLO STUDIO

E' fondamentale verificare:

- la perfetta riuscita del backup ed eventualmente capire cosa non è stato copiato e il perché dell'errore
- ricevere un dettaglio (log) del processo di backup (ad esempio via email) per essere sempre aggiornati sui salvataggi dei dati

PROTEZIONE DEI DATI DIGITALI

Il regolamento generale sulla protezione dei dati (GDPR, General Data Protection Regulation-Regolamento UE 2016/679) è un Regolamento con il quale la Commissione europea intende rafforzare e rendere più omogenea la protezione dei dati personali di cittadini dell'Unione Europea e dei residenti nell'Unione Europea, sia all'interno che all'esterno dei confini dell'Unione europea (UE).

Il testo, pubblicato su Gazzetta Ufficiale Europea il 4 maggio 2016 ed entrato in vigore il 25 maggio dello stesso anno, ha iniziato ad avere efficacia il **25 maggio 2018**.

Il regime di protezione dei dati proposto per l'UE estende gli obiettivi della legge europea sulla protezione dei dati a tutte le imprese estere che trattano dati di residenti europei a prescindere dal luogo nel quale le trattano e dalla loro sede legale. Permette di armonizzare le diverse normative sulla protezione dei dati in tutta l'UE, facilitando così l'osservanza delle norme da parte delle imprese non europee; tuttavia, questo è stato ottenuto a costo di un regime che prevede una severa disciplina di protezione dei dati, con rigide sanzioni che possono raggiungere il 4% del volume globale di affari

Secondo la Commissione Europea "i dati personali sono qualunque informazione relativa a un individuo, collegata alla sua vita sia privata, sia professionale o pubblica. Può riguardare qualunque dato personale: nomi, foto, indirizzi email, dettagli bancari, interventi su siti web di social network, informazioni mediche o indirizzi IP di computer.

Un valido consenso deve essere esplicitamente dato per la raccolta dei dati e per i propositi per i quali sono usati (Articolo 7; definito in Articolo 4). Pertanto se la richiesta viene inserita nell'ambito di altre dichiarazioni essa va distinta e formulata con linguaggio semplice e chiaro (Articolo 7). Condizione di validità del consenso è che le finalità per cui viene richiesto siano esplicite, legittime, adeguate e pertinenti (Articolo 5). Nel caso in cui il consenso al trattamento dei propri dati personali per una o più specifiche finalità sia stato espresso da minori esso è valido solo se il minore ha almeno 16 anni.

La sicurezza dei dati raccolti è garantita dal titolare del trattamento e dal responsabile del trattamento chiamati a mettere in atto misure tecniche e organizzative idonee per garantire un livello di sicurezza adeguato al rischio. A tal fine il titolare e il responsabile del trattamento garantiscono che chiunque acceda ai dati raccolti lo faccia nel rispetto dei poteri da loro conferiti e dopo essere stato appositamente istruito.

Il titolare del trattamento dei dati avrà l'obbligo legale di rendere note le fughe di dati all'autorità nazionale e di comunicarle entro 72 ore da quando ne è venuto a conoscenza. I resoconti delle fughe di dati non sono soggetti ad alcuno standard "de minimis" e debbono essere riferite all'autorità sovrintendente non appena se ne viene a conoscenza e comunque entro 72 ore. In alcune situazioni le persone di cui sono stati sottratti i dati dovranno essere avvertite.

- I Device Fissi e Device Mobili, intesi nell'accezione di Strumenti Aziendali, sono uno strumento di lavoro che pertanto deve essere utilizzato esclusivamente per l'attività lavorativa
- Gli Strumenti Aziendali devono essere custoditi con cura, evitando ogni possibile forma di danneggiamento ed essere bloccati (es. log-out di sessione) quando se ne interrompe l'uso, in modo che utenti non autorizzati non abbiano accesso ai dati in esso contenuti salvo che con l'inserimento delle credenziali di sblocco
- Viene espressamente vietato salvo non sia già impedito by default, installare ed utilizzare programmi non espressamente autorizzati dallo Studio

- Divieto di collocare, anche temporaneamente, sugli Strumenti Aziendali o nella Rete Aziendale qualsiasi file che non sia attinente allo svolgimento dell'attività lavorativa
- Si evidenzia che le violazioni della normativa a tutela dei diritti d'autore sul software e su tutte le opere di ingegno (es: film, file musicali, ecc.) - che impone la presenza nel sistema di software regolarmente licenziati o comunque liberi e quindi non protetti dal diritto d'autore - vengono sanzionate anche penalmente
- Sulla Rete Aziendale devono essere configurati strumenti in grado di impedire, nel rispetto del principio di data protection by design e by default, l'accesso a siti non pertinenti con l'attività lavorativa o che offrono contenuti palesemente violativi del diritto d'autore

STRUMENTI FONDAMENTALI PER IL GDPR:

- ANTIVIRUS: aggiornamento automatico almeno una volta al giorno
- FIREWALL: software o hardware
- AGGIORNAMENTI SOFTWARE: ricerca quotidiana automatica almeno una volta al giorno
- CIFRATURA SUPPORTI: strumento di cifratura presente in Windows o in alternativa utilizzare software di terze parti
- INSTALLAZIONE SOFTWARE: deve essere autorizzata dallo studio
- BACKUP: devono essere effettuate copie di sicurezza dei dati almeno una volta a settimana
- VPN: accesso autorizzato e controllato da dispositivi mobili verso lo studio tramite connessione sicura

SUPPORTO REMOTO

Possibilità di accedere attraverso internet ad un pc remoto potendo operare e risolvere problemi come se ci si trovasse davanti alla postazione che presenta il problema software.

SUPPORTO REMOTO

Software più diffusi:

- Teamviewer
- LogMeIn
- Ammy
- Supremo
- AnyDesk