行政院衛生署

100 年度醫院電子病歷檢查案

電子病歷驗證準則(草案)

單位：行政院衛生署

版本：V 1.0

民國　100 年 12 月 8 日

目錄

一、 目的

（一）對不同格式之電子病歷，制定合適的簽章格式及驗章流程，提供醫療機構實施電子病歷管理及衛生署進行電子病歷簽章驗證作業時之依據。

（二）用以辨識及確認電子文件簽署人身分及電子文件之真偽。

二、 法源依據

（一）醫療機構電子病歷製作及管理辦法

（二）電子簽章法

三、 名詞解釋

(一) 病歷

1. 醫療法第 67 條，病歷應包括下列各款之資料：

(1) 醫師依醫師法執行業務所製作之病歷。

(2) 各項檢查、檢驗報告資料。

(3) 其他各類醫事人員執行業務所製作之紀錄。

2. 醫師法第 12 條：

醫師執行業務時，應製作病歷，並簽名或蓋章及加註執行年、月、日。

前項病歷，除應於首頁載明病人姓名、出生年、月、日、性別及住址等基本資料外，其內容至少應載明下列事項：

(1) 就診日期。

(2) 主訴。

(3) 檢查項目及結果。

(4) 診斷或病名。

(5) 治療、處置或用藥等情形。

(6) 其他應記載事項。

病歷由醫師執業之醫療機構依醫療法規定保存。

(二) 電子文件

電子文件是利用光、電、磁等技術所做成之訊息、紀錄，可能以文字、聲音、圖片或影像等等不同方式呈現，但只要足以表示文件製作者之意思，可以電子形式處理，比方說可經由電腦閱讀者，都可稱之為電子文件。

(三) 病歷電子檔

以電子文件方式完成之病歷。

(四) 電子病歷

依「醫療機構電子病歷製作及管理辦法」以電子文件方式製作及貯存之病歷。

(五) 電子簽章

指依附於電子文件並與其相關連，用以辨識及確認電子文件簽署人身分、資格及電子文件真偽者。

(六) 憑證

指載有簽章驗證資料，用以確認簽署人身分、資格之電子形式證明。

(七) 本文

病歷單張之電子形式。

(八) 簽章格式

本文加簽體的封裝模式。

(九) 區塊

指本文中被個別簽章之病歷範圍。一份本文可含有一個以上的區塊。

四、 驗證對象及驗證範圍

(一)驗證對象

醫療機構依據「醫療機構電子病歷製作及管理辦法」製作完成之電子病歷。

(二)驗證範圍

1. 本文檔案
2. 簽章檔案

※補充說明

1. 時戳非「醫療機構電子病歷製作及管理辦法」所要求之必要項目，目前亦未規範醫院簽章時必須包括時戳，因此不納入本準則之驗證範圍。

2. 有關憑證之有效性牽涉文件製作日期，在時戳為非必要之情況下，無法進行憑證效期之驗證，因此不納入本準則之驗證範圍。

五、 本文與簽章之關係模式

(一)本文形式

1. XML 文件

   電子病歷文件內嵌 W3C 簽體。

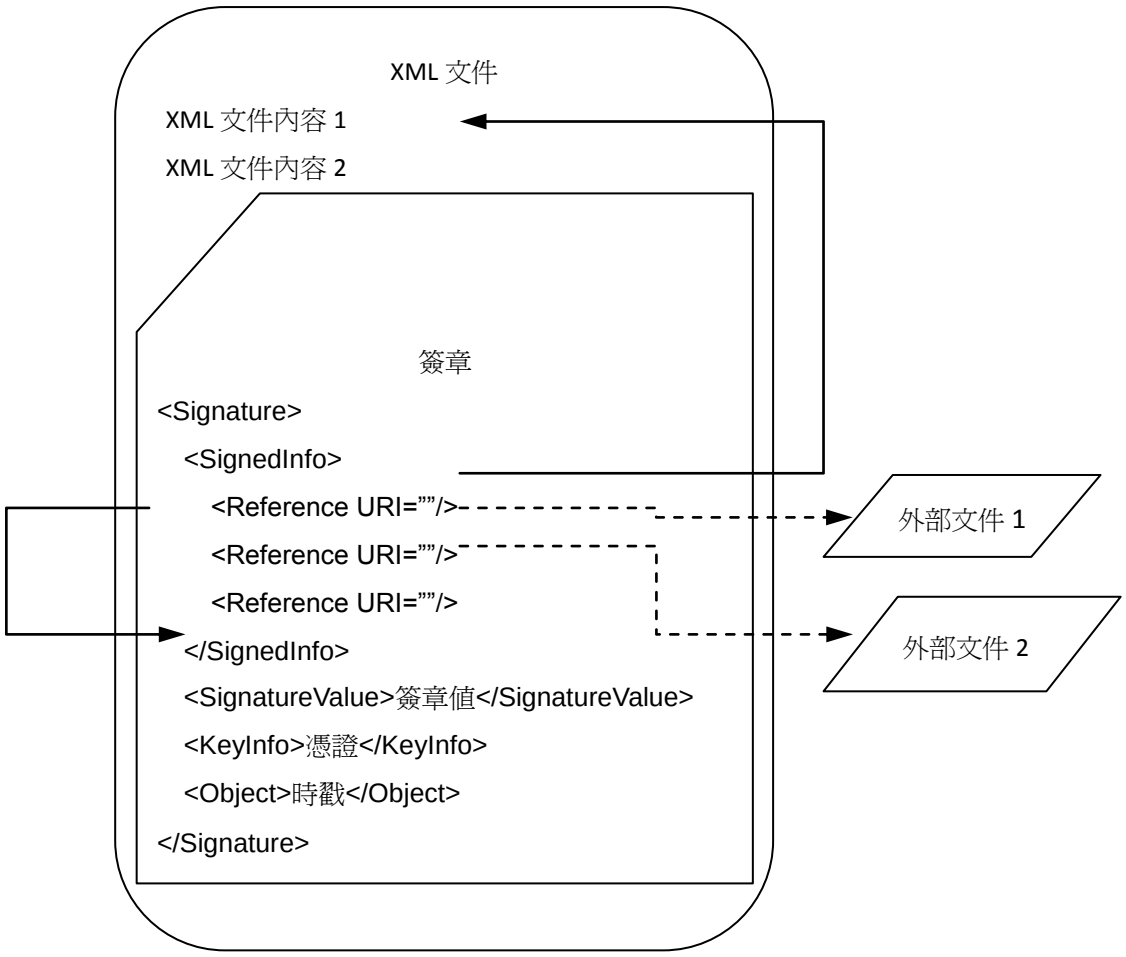
2. 非 XML 文件(ex：JPG、DOC)

   電子病歷文件內嵌或獨立於 W3C 簽體。

(二)簽章格式

1. Enveloped Signature：此種做法在簽署的 XML 文件之根元素包住簽體。
   - W3C Enveloped 簽章 (W3C Enveloped Signature)
   - 說明：適用於 XML 文件之簽章
   - 圖例：

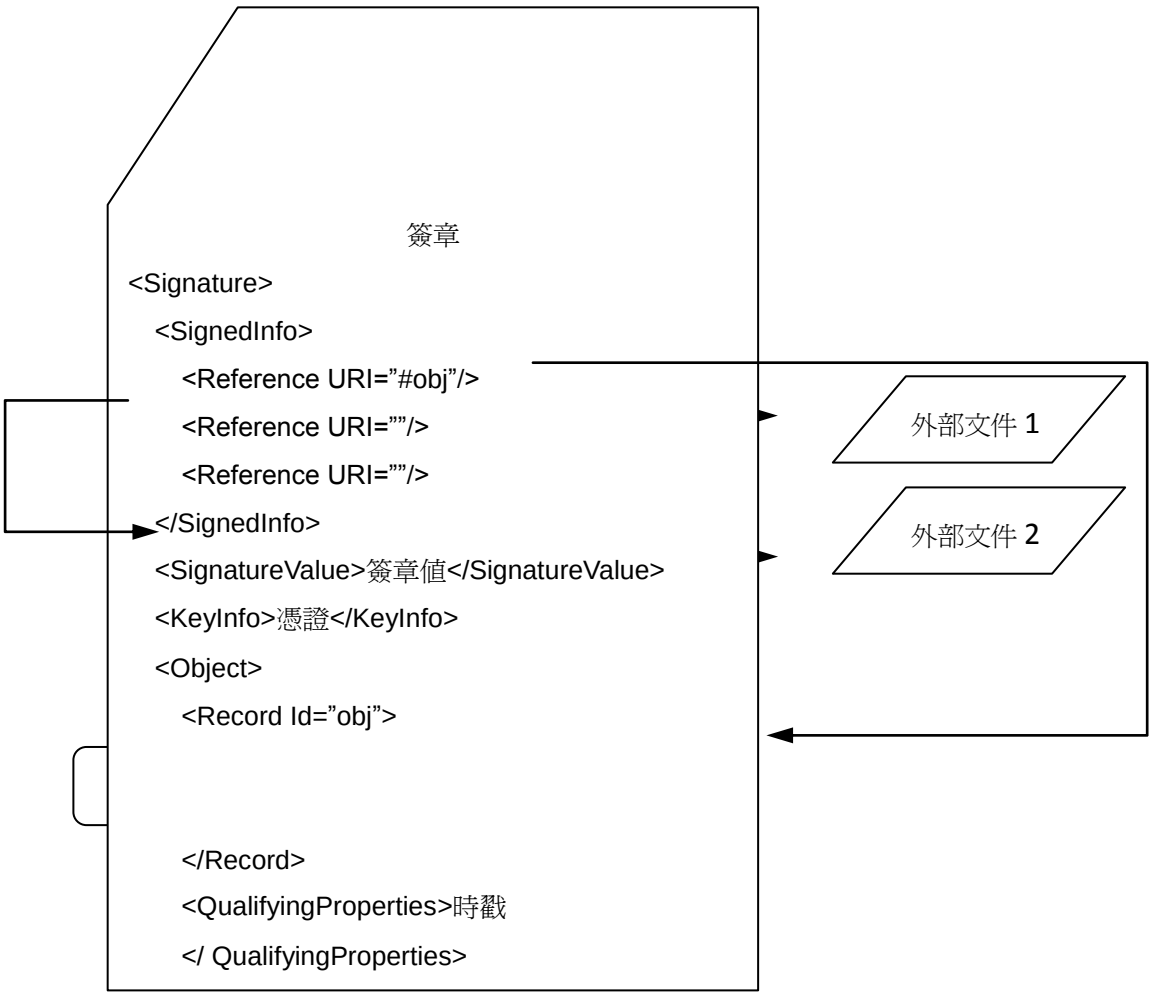
▢	本文 (XML 文件)
⬠	本文 (Binary 文件，例如: WORD)
▢	簽章 (Signature)
▱	外部文件



2. Enveloping Signature：簽體包住被簽署的資料；將本文(可以是 XML 文件或是 Base64 編碼之文件)置於簽體之<Object>標記內。

- W3C Enveloping 簽章 (W3C Enveloping Signature)
- 說明：適用於 XML 文件及非 XML 文件之簽章
- 圖例：

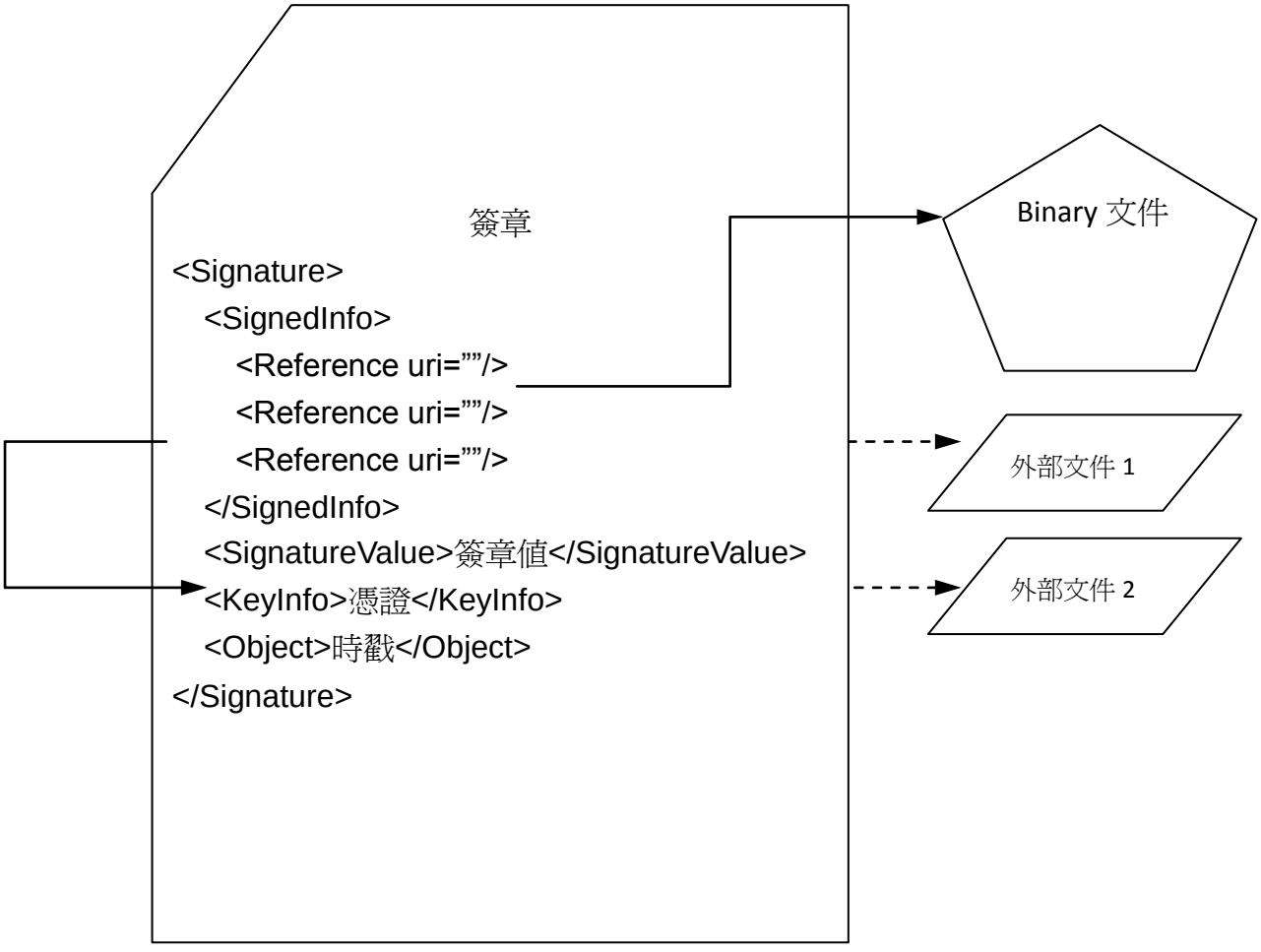
▢	本文 (XML 文件)
⬠	本文 (Binary 文件，例如: PDF)
▢	簽章 (Signature)
▱	外部文件



3. Detached Signature：簽體與被簽署的文件是分離的，在簽體內使用 <Reference URI=”路徑”>標記來參考到外部文件位址

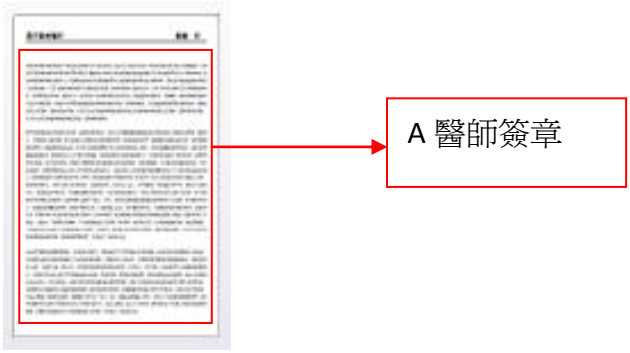
- W3C Detached 簽章 (W3C Detached Signature)
- 說明：適用於 XML 文件及非 XML 文件之簽章
- 圖例：

▢	本文 (XML 文件)
⬠	本文 (Binary 文件，例如: WORD)
▢	簽章 (Signature)
▱	外部文件

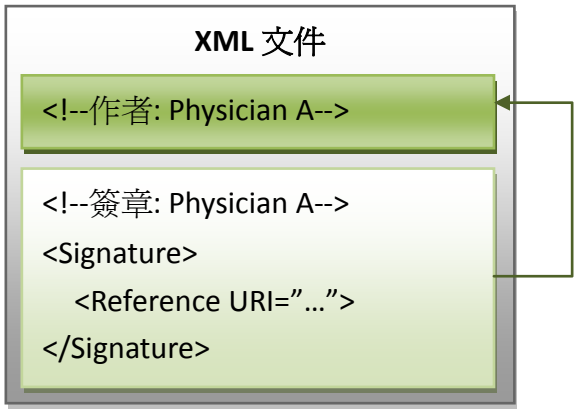


(三)本文與簽章之關係

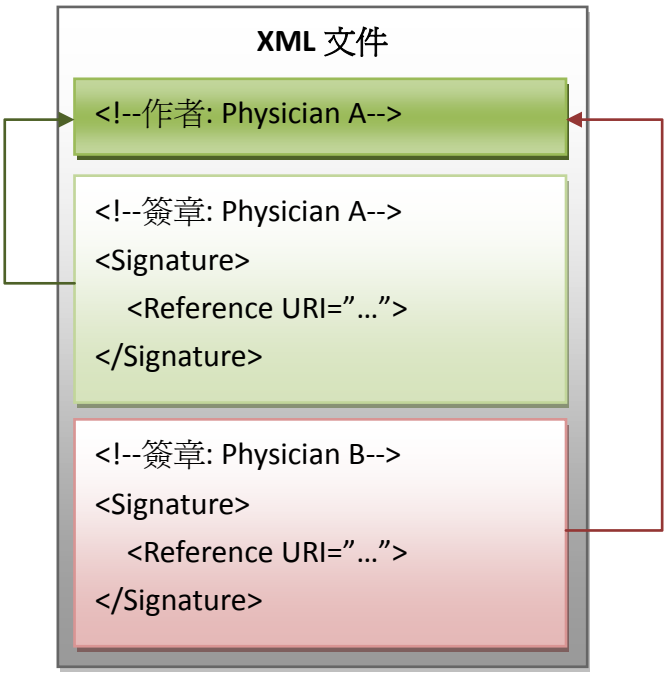
1. 本文僅由單一作者獨立製作。



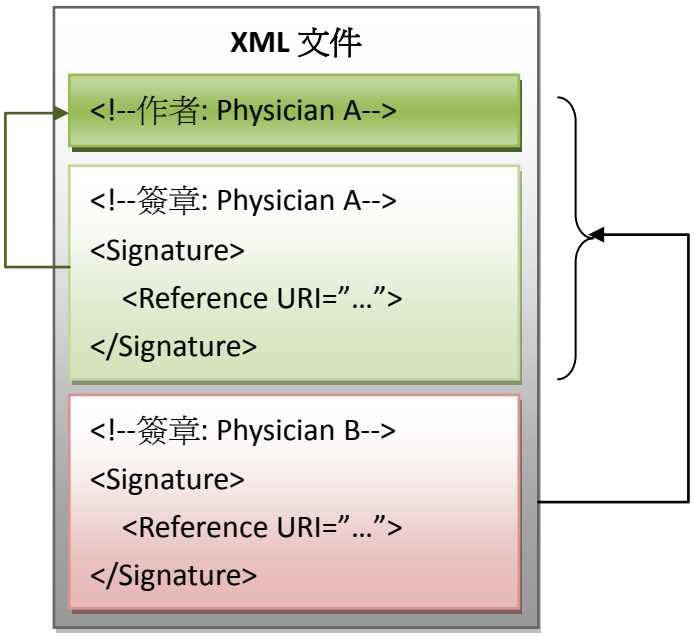
1.1 作者獨立簽章。



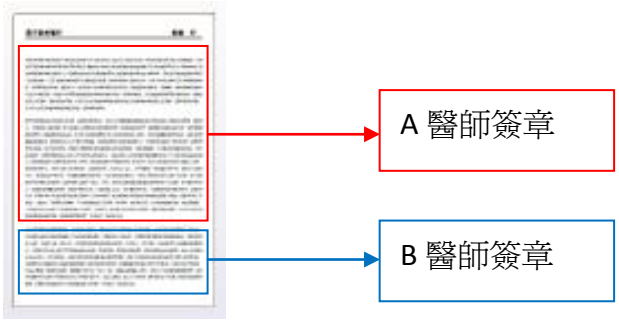
1.2 最後簽章者對前面所有區塊進行簽章。



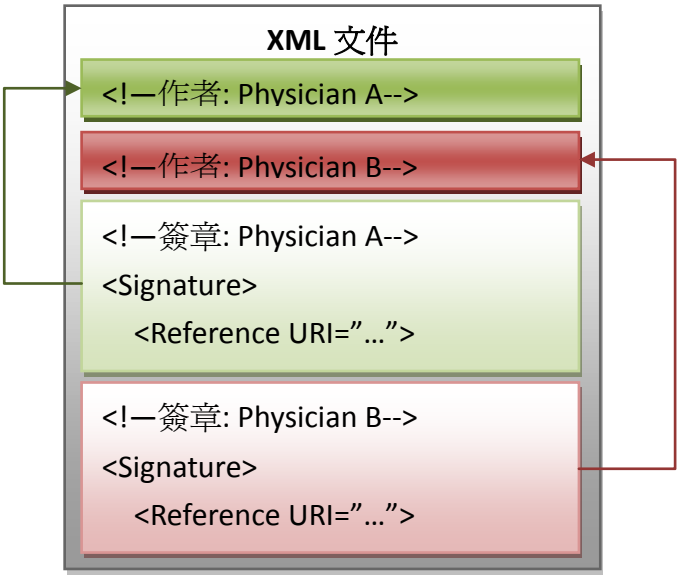
1.3 最後簽章者對前面所有區塊及簽章進行簽章。



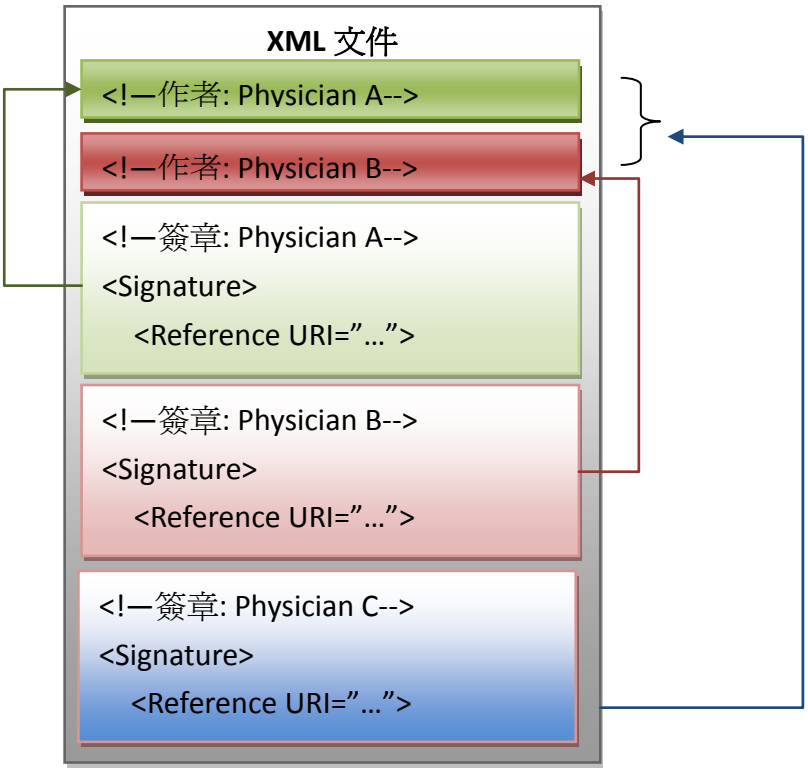
2. 本文由多位作者獨立製作之區塊所合成。



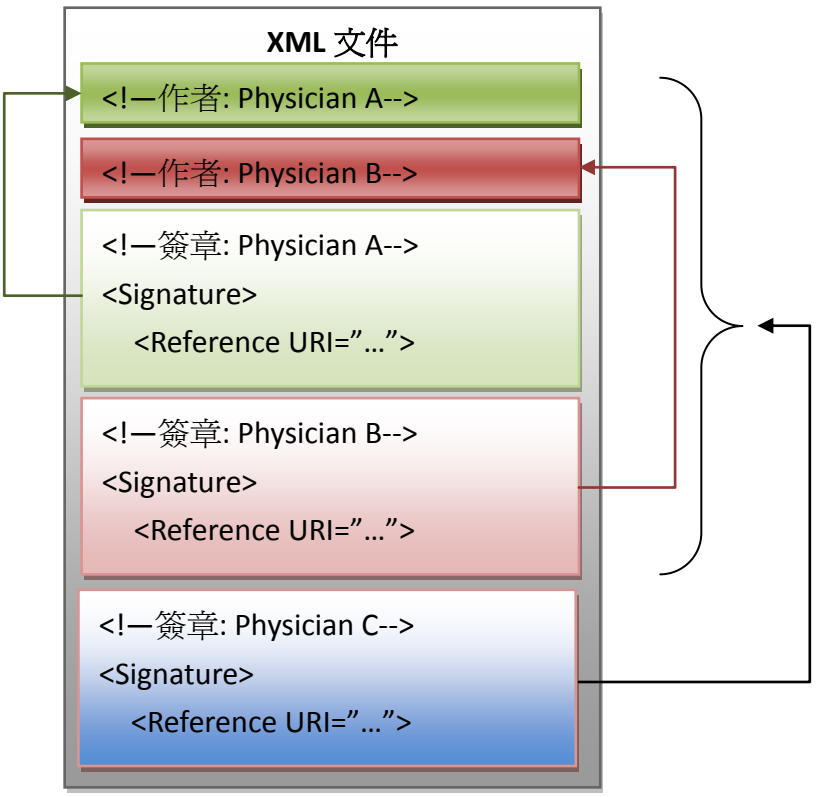
2.1 多位作者對自己獨立製作之區塊進行簽章。



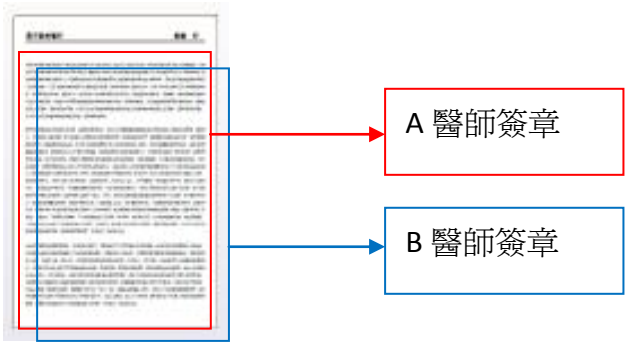
2.2 多位作者對自己獨立製作之區塊進行簽章，而最後簽章者對前面所有區塊進行簽章。



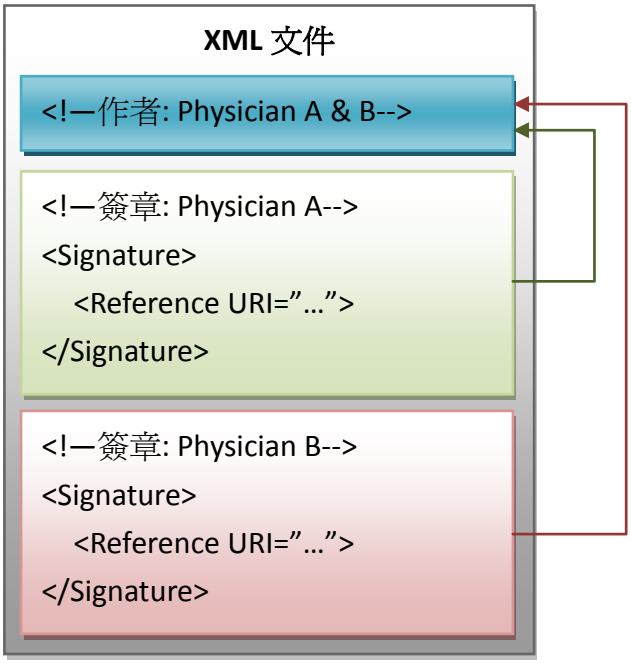
2.3 多位作者對自己獨立製作之區塊進行簽章，而最後簽章者對前面所有區塊及簽章進行簽章。



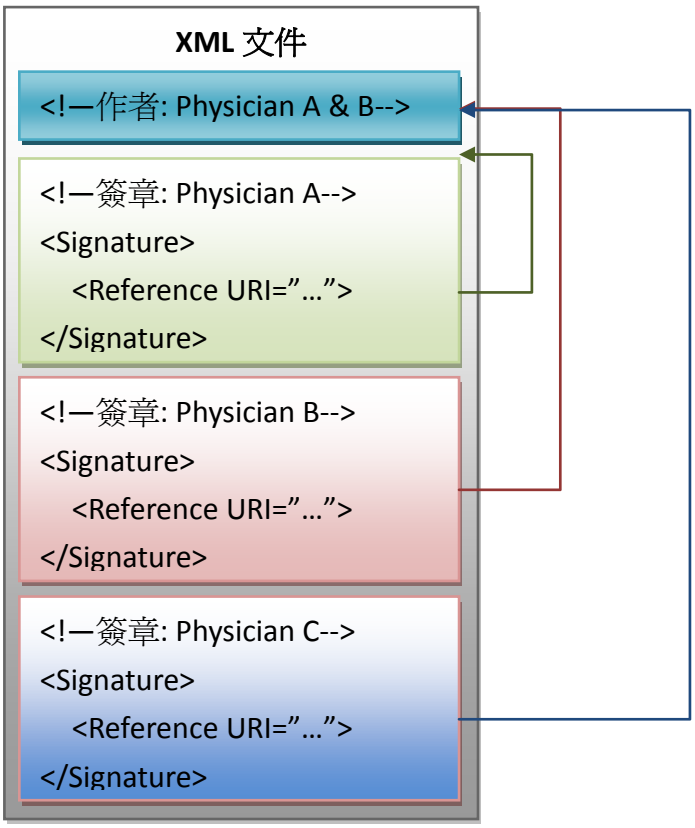
3. 本文由多位作者共同製作之區塊所合成。



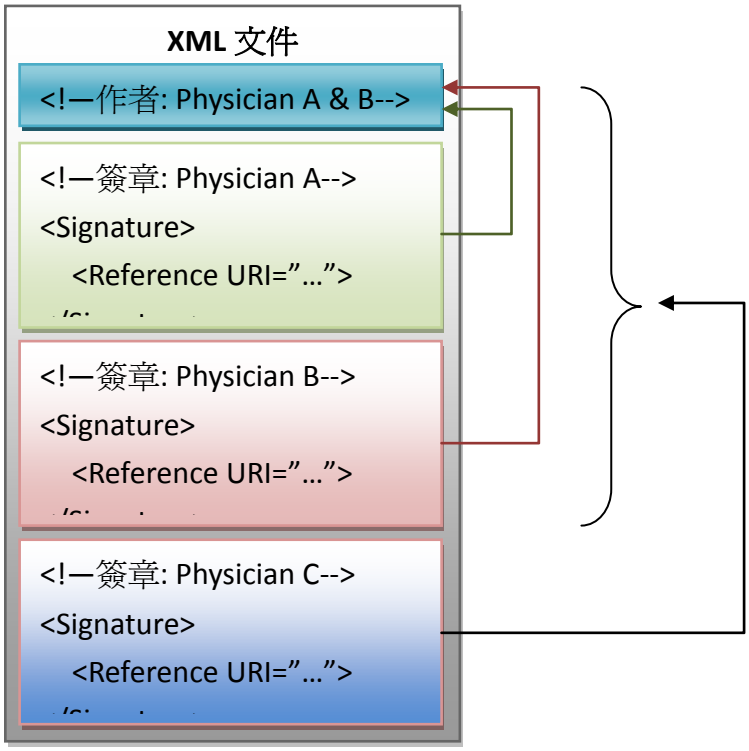
3.1 多位作者對共同製作之區塊共同簽章。



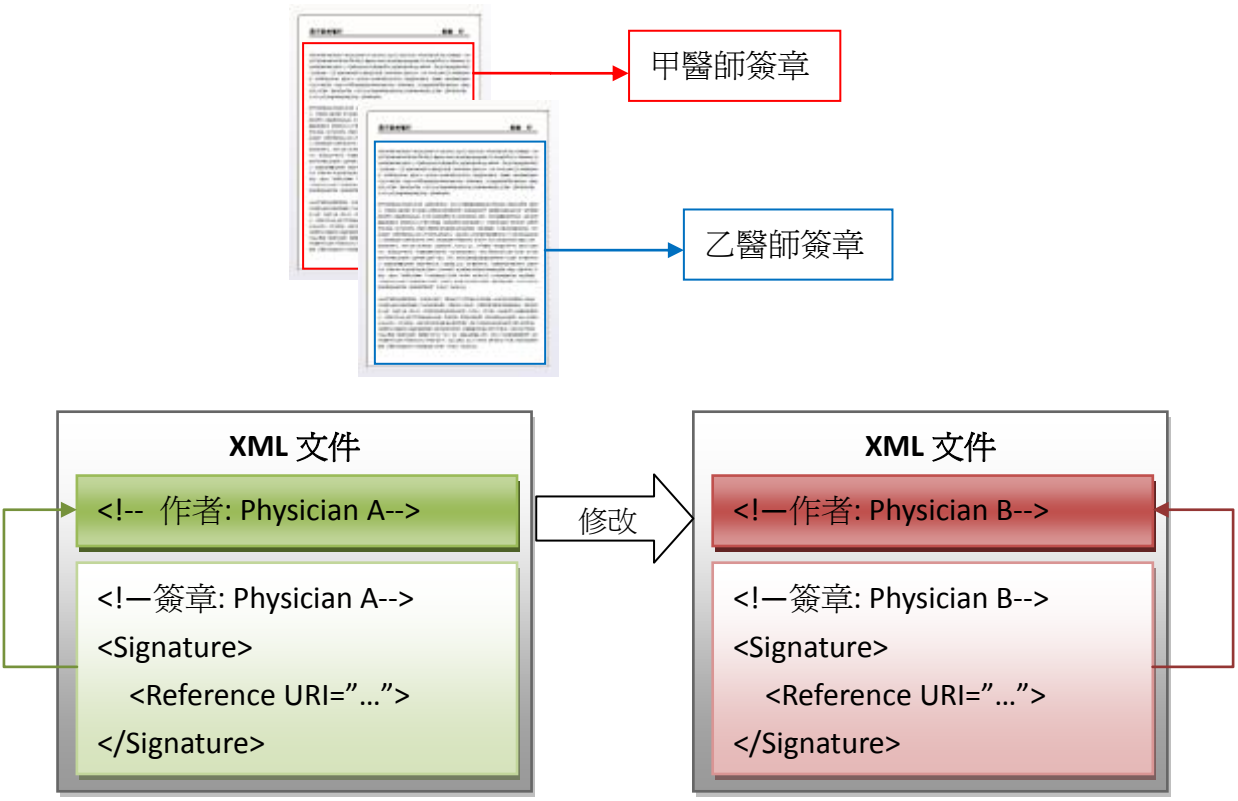
3.2 多位作者對共同製作之區塊共同簽章，而最後簽章者對前面所有區塊進行簽章。



3.3 多位作者對共同製作之區塊共同簽章，而最後簽章者對前面所有區塊及簽章進行簽章。



4. 對先前作者製作之區塊進行修改，則修改者必須另建新本文並對其行簽章。



六、 驗證項目

依電子病歷「本文」與「簽章」之關係，所有簽章被驗證無誤，該電子病歷檔案方視為有效。

(一) 驗證電子病歷「本文」與「簽章」之依存關係，即封裝格式(簽章格式)是否符合 W3C 三種類型(Enveloping Signatures、Enveloped Signatures、Detached Signatures)之一。

(二) 依電子病歷「本文」與「簽章」之關係，驗證「簽體」是否以公鑰對應之私鑰製作。

(三) 依電子病歷「本文」與「簽章」之關係，驗證「本文」是否遭受竄改。

(四) 憑證所屬類別。

七、驗證程序

電子病歷驗證無法以人來進行驗證，因此需仰賴行政院衛生署所提供之軟體依據驗證項目逐項進行檢查。

八、維護流程

「電子病歷驗證準則」由衛生署正式公告後，若「醫療機構電子病歷製作及管理辦法」或相關法規進行修正或接收到增修建議，應配合修正，以維護「電子病歷驗證準則」之正確性。其維護流程如下：

(一) 提案報階段

配合相關法規修訂以及醫療機構對驗證準則有修正建議時，由行政院衛生署蒐集彙整相關資料，醫療機構提出修正建議時應有具體理由說明，並草擬建議修正內容，衛生署收到相關建議應於一個月內提交專家審議，視建議的適切性、重要性及可行性決議是否納入修訂，或若不予修訂則直接函覆復提案報人／或單位。

(二) 起草階段

針對修正之法規及蒐集之修訂建議，由衛生署先行修改，擬定草案。

(三) 初審階段

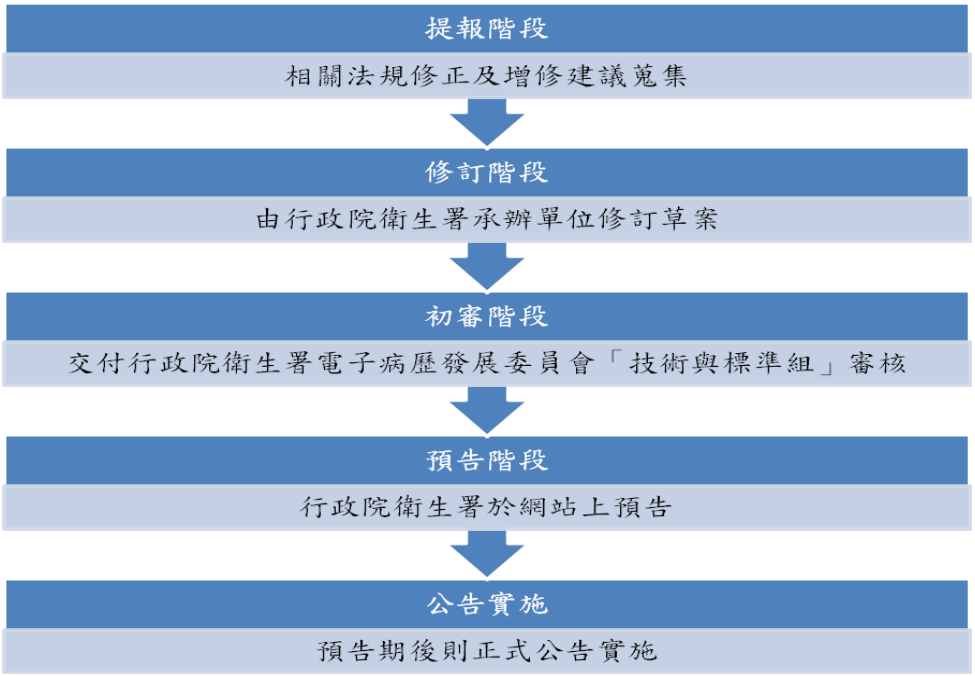
修改後之草案將呈交行政院衛生署電子病歷發展委員會「技術與標準組」，召開委員會進行討論，並依據會議決議進行修改。

(四) 預告階段

修改後之電子病歷驗證準則草案，將在行政院衛生署網站預告，預告期間為期二週，對於本草案內容有任何意見或修正建議，可於預告期間陳述意見。

(五) 公告實施

電子病歷驗證準則草案經預告後，即可正式公告實施。



【電子病歷驗證準則維護流程】

九、參考文獻

1. 醫療法，中華民國九十八年五月二十日總統華總一義字第 09800125131 號令。
2. 醫師法，中華民國九十八年五月十三日總統華總一義字第 09800116281 號令。
3. 電子簽章法，民國 90 年 11 月 14 日。
4. 陳群顯(88)。電子簽章法之研究。碩士論文，台北：東吳大學法律學系。
5. 吳志成(92)。醫療資訊系統導入電子簽章之參考架構與整體解決方案。國碩士論文，花蓮：立東華大學資訊工程學系。
6. W3C(2008)。W3C XML Signature Syntax and Processing。2011 年 12 月 6 日，網址： http://www.w3.org/TR/xmldsig-core/
7. W3C(2008)。Canonical XML Version 1.0。2011 年 12 月 6 日，網址： http://www.w3.org/TR/2001/REC-xml-c14n-20010315
8. Assigned ETSI XML URIs。ETSI TS 101 903 v1.41 - XML Advanced Electronic Signatures。2011 年 12 月 6 日，網址： http://uri.etsi.org/01903/v1.2.2/ts_101903v010401p.pdf

十、附錄

Enveloped 簽章範例

對於電子病歷 XML 文件之簽章格式採用 W3C XMLdsig Enveloped 簽章之標準，簽章的動作對整個 SignedInfo 區段進行 XML 正規化 (XML Canonicalization) 處理後再進行簽章。

範例如下：

```
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#" Id="簽章流水號">
  <SignedInfo>
    <CanonicalizationMethod
Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
    <SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
    <Reference URI="#文件流水號">
    <Transforms>
      <Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
      <Transform
Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
    </Transforms>
    <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
/>
    <DigestValue>base64 編碼之 SHA-1 值</ds:DigestValue>
    </Reference>
  </SignedInfo>
  <SignatureValue>base64 編碼之簽章</SignatureValue>
  <KeyInfo>
    <X509Data>
      <X509Certificate>base64 編碼之憑證</X509Certificate>
```

```
      </X509Data>
    </KeyInfo>
    <Object>
      <QualifyingProperties xmlns="http://uri.etsi.org/01903/v1.4.1#"
Target="#簽章流水號">
        <UnsignedProperties>
          <UnsignedSignatureProperties>
            <SignatureTimeStamp>
              <EncapsulatedTimeStamp>base64 編碼之時戳
</EncapsulatedTimeStamp>
            </SignatureTimeStamp>
          </UnsignedSignatureProperties>
        </UnsignedProperties>
      </QualifyingProperties>
    </Object>
</Signature>
```

注意：

若電子病歷 XML 文件有參考到外部文件，則匯出電子病歷時，連同被參考到的外部文件必須與電子病歷一併存放在同一個資料夾內，以避免不同平台之檔案路徑問題。

Enveloping 簽章範例

對於非 XML 文件則採用 W3C XMLdsig Enveloping 簽章，

格式如下：

```
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#" Id="簽章流水號">
  <SignedInfo>
    <CanonicalizationMethod
Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
    <SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
    <Reference URI="#文件流水號">
    <Transforms>
      <Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
      <Transform
Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
    </Transforms>
    <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
/>
    <DigestValue>base64 編碼之 SHA-1 值</ds:DigestValue>
    </Reference>
  </SignedInfo>
  <SignatureValue>base64 編碼之簽章</SignatureValue>
  <KeyInfo>
    <X509Data>
      <X509Certificate>base64 編碼之憑證</X509Certificate>
    </X509Data>
  </KeyInfo>
  <Object Id="文件流水號">base64 編碼二進位檔案內容</Object>
```

```
  <Object>
    <QualifyingProperties xmlns="http://uri.etsi.org/01903/v1.4.1#"
Target="#簽章流水號">
      <UnsignedProperties>
        <UnsignedSignatureProperties>
          <SignatureTimeStamp>
            <EncapsulatedTimeStamp>base64 編碼之時戳
</EncapsulatedTimeStamp>
          </SignatureTimeStamp>
        </UnsignedSignatureProperties>
      </UnsignedProperties>
    </QualifyingProperties>
  </Object>
</Signature>
```

注意：

若電子病歷 XML 文件有參考到外部文件，則匯出電子病歷時，連同被參考到的外部文件必須與電子病歷一併存放在同一個資料夾內，以避免不同平台之檔案路徑問題。